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
№ 8

Communication, informatization and cybersecurity systems and technologies
№ 8

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 імені Героїв Крут. – 2025. – № 8. – 300 с. – DOI: 10.58254/viti.8.2025.

ISSN 2786-6610

Усі 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 № 1 від 25.11.2025).

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. № 287. Друк. арк. 37,5. Ум.-друк. арк. 34,87. Обл.-вид. арк. 32,43.
Формат паперу 60×84/8. Тираж 60 прим.
Адреса друкарні ВІТІ ім. Героїв Крут: 01011, м. Київ, вул. Князів Острозьких, 45/1

З М І С Т

C O N T E N T S

DOI: 10.58254/viti.8.2025.01.05

УДК 621.3:623.4:629.07-044.4

Ph.D Бернацький А. П. ORCID: 0000-0003-0379-075X (ВІТІ ім. Героїв Крут)
канд. техн. наук, професор Радзівілов Г. Д. ORCID: 0000-0002-6047-1897 (ВІТІ ім. Героїв Крут)
Ph.D Фесенко О. Д. ORCID: 0000-0002-2114-5327 (ВІТІ ім. Героїв Крут)

МЕТОД АДАПТИВНОГО КЕРУВАННЯ БОЙОВИМ СЕРЕДОВИЩЕМ З КІБЕРНЕТИЧНИМ КОНТУРОМ ПРОГНОЗУВАННЯ

У роботі представлено концепцію та результати дослідження архітектури адаптивного керування бойовим середовищем із використанням кібернетичного контуру прогнозування. Класичні підходи до формування систем людино-машинного інтерфейсу демонструють обмежену стійкість у стресових умовах, тоді як сучасні технології цифрових двійників і штучного інтелекту відкривають можливості нових підходів для створення архітектур управління, здатних адаптивно балансувати між втручанням оператора й автоматизацією алгоритмів керування роботизованими системами.

Метою дослідження є розробка методу адаптивного керування нового покоління, яка забезпечує зменшення невизначеності, підвищення довіри до автоматизованих рішень і захист від небезпечних сценаріїв. Для досягнення цієї мети було використано цифрові двійники оператора та роботизованої системи, AI-помічник як інтеграційний вузол і кібернетичний контур прогнозування для багатосценарного моделювання можливих дій. Математична модель включає ентропійні показники як міру невизначеності, матрицю зв'язності для відображення узгодженості двійників і функцію довіри τ, яка визначає ступінь делегування контролю від людини до виконавчої роботизованої системи. Запропоновано і доведено теорему монотонності довіри, що формалізує тенденцію до підвищення рівня довіри в процесі навчання системи.

Експериментальна оцінка ефективності показала, що запропонована архітектура забезпечує 30–40 % зменшення ентропії прогнозу, зростання довіри на 30 % порівняно з базовими моделями, зниження участі оператора на 25–40 % й стабільне проходження безпекових фільтрів навіть у складних екстремальних умовах.

Наукова новизна дослідження полягає у введенні механізму кібернетичного контуру прогнозування до архітектури адаптивного керування, у формалізації теореми монотонності довіри та у використанні ансамблевих симуляцій для оцінки майбутніх сценаріїв. Практичне значення полягає у можливості підвищення ефективності та безпеки екстремальних роботизованих комплексів, у тому числі й бойових, зменшенні когнітивного навантаження на оператора та створенні передумов для впровадження нових стандартів взаємодії людина – машина у miltech-галузі.

Разом із тим, робота виявила низку обмежень, серед яких підвищені обчислювальні витрати, залежність від точності моделей цифрових двійників і потреба у захисті архітектури від кібервтручань.

Отримані результати створюють науково-технічне підґрунтя для переходу від концептуального рівня до експериментально-випробувальної стадії й інтеграції розробленої архітектури у реальні бойові системи наступного покоління.

Ключові слова: *автономні бойові платформи, адаптивне управління, архітектура ЛМІ, цифрові двійники, AI-помічник, кібернетичний контур прогнозування, довіра людина – машина, ентропія прогнозу, бойове середовище, роботизовані системи, miltech.*

A. Bernatskyi, H. Radzivilov, O. Fesenko. Adaptive control architecture for battlefield environments with a cybernetic prediction contour

The paper presents the concept and results of research into the architecture of adaptive combat environment control using a cybernetic prediction loop. Classic approaches to the formation of human-machine interface systems demonstrate limited stability in stressful conditions, while modern technologies of digital twins and artificial intelligence open up opportunities for new approaches to the creation of control architectures capable of adaptively balancing operator intervention and automation of robotic system control algorithms.

The aim of the study is to develop a new generation of adaptive control architecture that reduces uncertainty, increases confidence in automated decisions, and protects against dangerous scenarios. To achieve this goal, digital twins of the operator and the robotic system, an AI assistant as an integration node, and a cybernetic prediction circuit for multi-scenario modeling of possible actions were used. The mathematical model includes entropy indicators as a measure of uncertainty, a connectivity matrix to reflect the consistency of twins, and a trust function τ, which determines the degree of control delegation from human to machine. A monotonicity theorem of trust has been proposed and proven, formalizing the tendency to increase the level of trust in the process of system training.

The experimental results showed that the proposed architecture provides a 30–40% reduction in prediction entropy, a 30% increase in confidence compared to baseline models, a 25–40% reduction in operator involvement, and stable passage through safety filters even in complex extreme conditions.

The scientific novelty of the research lies in the introduction of a cybernetic prediction loop mechanism into the adaptive control architecture, the formalization of the monotonicity theorem of confidence, and the use of ensemble simulations to evaluate future scenarios. The practical significance lies in the possibility of increasing the efficiency and safety of extreme robotic complexes, including combat ones, reducing the cognitive load on the operator, and creating the preconditions for the introduction of new standards of human-machine interaction in the miltech industry.

At the same time, the work revealed a number of limitations, including increased computational costs, dependence on the accuracy of digital twin models, and the need to protect the architecture from cyber interference.

The results obtained provide a scientific and technical basis for moving from the conceptual level to the experimental and testing stage and integrating the developed architecture into real next-generation combat systems.

Keywords: *autonomous combat platforms, adaptive control, HMI architecture, digital twins, AI assistant, cybernetic prediction loop, human – machine trust, prediction entropy, battlefield environment, robotic systems, miltech.*

1. Постановка проблеми

Сучасне бойове середовище характеризується високою динамікою, багатофакторністю та невизначеністю [1]. Тенденція зростання кількості змінних, що впливають на процес прийняття рішень, у поєднанні з високою швидкістю перебігу подій ускладнює застосування класичних моделей управління та їх модифікацій. Ключовим недоліком традиційних людино-машинних інтерфейсів (ЛМІ), що базуються на парадигмі прямого керування, є їхня нездатність до адаптації. Ігнорування динамічних змін у когнітивному та психофізіологічному стані оператора неминуче призводить до когнітивного перевантаження і, як наслідок, до значного зростання ймовірності людської помилки, особливо в умовах високої відповідальності та дефіциту часу.

Крім того, сучасний розвиток засобів радіоелектронної боротьби та кібервпливу підвищує вразливість таких систем, роблячи їх ненадійними саме тоді, коли від них вимагається максимальна стійкість. Фундаментальним недоліком традиційних інтерфейсів є їхня реактивна парадигма функціонування, що змушує систему діяти у відповідь на події, які вже відбулися. Такий підхід не відповідає вимогам сучасних бойових систем, які потребують переходу до проактивного управління, заснованого на прогнозуванні та моделюванні потенційних сценаріїв для ухвалення та прийняття випереджувальних рішень.

У цьому контексті особливої уваги набуває поєднання цифрового двійника (ЦД), AI-помічника та кібернетичного контуру прогнозування. ЦД дозволяє створити віртуальне відображення оператора і технічної системи, забезпечуючи їхнє інтегроване представлення у цифровому середовищі. AI-помічник виступає аналітичним ядром, здатним знімати інформаційне навантаження з оператора і пропонувати оптимальні рішення на основі багатофакторного аналізу. Тоді як кібернетичний контур прогнозування формує додатковий рівень безпеки, переводячи управління з реактивної у проактивну площину, де ризики і потенційно негативні наслідки відсіюються ще на етапі цифрового моделювання.

Таким чином, актуальність дослідження визначається не лише потребою підвищення ефективності ЛМІ у екстремальних і військових системах, але й постає об'єктивними викликами бойового середовища, яке вимагає переходу до нової архітектури адаптивного керування.

2. Аналіз останніх досліджень і публікацій

У сучасних військово-технічних дослідженнях спостерігається стійка тенденція уваги до концепції цифрових двійників та їхньої інтеграції в людино-машинні системи. У рамках європейських та американських оборонних програм цифрове моделювання застосовується для вирішення широкого спектра завдань, таких як: моніторинг стану бойових платформ, інфраструктури та оптимізації логістичних ланцюгів. Окремим напрямом є створення антропоморфних цифрових моделей, що відтворюють фізіологічний стан військовослужбовців. Такі технології доповнюються системами аналізу даних на основі штучного інтелекту, призначеними для підтримки прийняття командних рішень у реальному часі. Зазначені напрями досліджень свідчать про значні перспективи використання ЦД як засобу підвищення загальної стійкості та бойової ефективності військових систем.

Так, група дослідників у роботі [2] провела огляд технології ЦД у сфері оборони, включаючи фронтові додатки, стандартизацію та інтеграцію між різними доменами й умовами застосування. До основних слабких місць вони відносять технологічні обмеження, дефіцит фахівців, бюджетні труднощі, а також недостатню інтеграцію між галузями та відсутність стратегічної координації. Інше дослідження [3] групи військових дослідників – Paul O. Kwon, Gary P. Zientara та інші для Special Warfare Journal – представляє гуманоїдного ЦД з анатомією, фізіологією і біомеханікою для військової підготовки. Наведена система дозволяє симулювати екстремальні умови, температуру, висоту тощо без ризику для людини. Однак фокусування на фізичній симуляції без інтеграції когнітивних або ЛМІ-аспектів не дозволяє застосовувати як комплексне рішення задачі.

У науковій статті [4] розглянуто концепт ЦД, який в режимі реального часу аналізує дані з бойових зон, здійснює прогнози, виявляє аномалії та надає командні рекомендації із застосуванням алгоритмів штучного інтелекту. Однак важливо зазначити, що сфера застосування цього підходу обмежується аналітикою управління активами (*asset management*) і не включає модель оператора та його когнітивні параметри.

У роботі [5] автор Yun Zhou розглядає використання цифрових двійників для модернізації мереж DoD та адаптивного управління ресурсами в межах концепції Combined Joint All-Domain Command and Control (CJADC2). Недоліком цього підходу, подібно до інших згаданих робіт, є його орієнтованість на інфраструктуру, а не на оператора, що залишає людський фактор поза рамками дослідження.

Огляд [6] за авторством Usman Asad та ін. присвячений тенденції людино-орієнтованих цифрових двійників (HCDT) в Industry 5.0, де основна увага приділяється технологіям інтерфейсу сенсорів, когнітивних систем, VR/AR. Ключовим висновком дослідження є те, що в рамках цієї концепції оператори не розглядаються як об’єкти моделювання. Їхня роль залишається другорядною, оскільки вони виступають лише користувачами ЦД, а не його інтегрованою складовою.

На конференції I/ITSEC у квітні 2024 року група дослідників на чолі з A. M. Mohammed представила роботу [7], де було запропоновано архітектуру людино-цифрового двійника. Запропонована модель інтегрує LLM як діалоговий інтерфейс та емоційне моделювання для покращення взаємодії людини й автономних систем. Ключовим внеском є пріоритезація когнітивного зв’язку з оператором. Разом із тим, суттєвим обмеженням концепції є ігнорування особливостей роботизованих систем та бойового середовища, що створює значні перешкоди для її практичного застосування.

Велика кількість публікацій мають фрагментарний характер і зосереджені на окремих аспектах. Одні автори приділяють увагу лише технічним параметрам бойових платформ, інші – фізіологічним характеристикам військових або аналітичним алгоритмам штучного інтелекту. У більшості досліджень відсутнє глибоке опрацювання когнітивного аспекту, який має визначальне значення у бойових умовах, коли швидкість і точність мислення оператора є критичними для виживання. Додатковим недоліком є недостатня перевірка таких підходів у реальних умовах. Більшість результатів базується на моделюванні та демонстраційних експериментах, які не відображають повною мірою динаміку реального бойового середовища.

У підсумку сформувався дослідницький ландшафт, де окремі напрямки активно розвиваються, але брак комплексності і системності не дозволяє вивести концепцію цифрового двійника у ЛМІ на рівень практичної архітектури, здатної забезпечити адаптивне керування бойовим середовищем.

Виявлені у попередньому аналізі обмеження засвідчують потребу у формуванні нової науково-технічної концепції, здатної поєднати ЦД оператора та роботизованої системи в єдину архітектуру управління, доповнену штучним інтелектом та кібернетичним контуром прогнозування. Такий підхід дозволяє перейти від фрагментарних досліджень до цілісної системи, яка відповідає вимогам сучасного бойового середовища.

Мета дослідження полягає у розробці методу адаптивного керування бойовим середовищем на основі ЛМІ з інтегрованим ЦД, АІ-помічником та кібернетичним контуром прогнозування.

3. Виклад основного матеріалу

3.1. *Архітектура адаптивного ЛМІ з ЦД та АІ-помічником*

Запропонована архітектура ґрунтується на ідеї інтеграції трьох ключових елементів: ЦД оператора, ЦД технічної системи та АІ-помічника, об’єднаних у єдиному кібернетичному контурі прогнозування. Така інтеграція дозволяє створити замкнену інформаційно-керуючу систему, здатну одночасно відображати стан людини, стан виконавчої системи та прогнозувати результати їхньої взаємодії у віртуальному середовищі.

ЦД оператора виступає відображенням когнітивних і психофізіологічних характеристик людини, включаючи її стиль мислення, швидкість реакцій і типові стратегії ухвалення рішень. Він дає змогу уніфікувати ці індивідуальні особливості в моделі, яка може бути інтегрована в архітектуру управління. ЦД виконавчої роботизованої системи, у свою чергу, моделює динамічні параметри бойової платформи – від технічного стану агрегатів до здатності виконувати складні маневри у змінному середовищі.

АІ-помічник посідає центральне місце в архітектурі, виконуючи роль інтегратора. Його завдання полягає у синтезі інформаційних потоків від двох ЦД, у проведенні багатофакторного аналізу та формуванні рекомендацій для оператора. Він також здатний здійснювати предиктивну аналітику, оцінюючи ймовірні сценарії розвитку ситуації та пропонуючи оптимальні варіанти дій.

Ключовим інноваційним елементом виступає кібернетичний контур прогнозування. Цей модуль є віртуальним симулятором, який заздалегідь «програє» сценарії, що виникають внаслідок дій оператора, аналізуючи їхні наслідки ще до передачі команди виконавчій системі. Контур забезпечує своєрідний «фільтр безпеки», що відсіює потенційно негативні сценарії, знижує ймовірність помилкових рішень і підвищує стійкість управління в умовах стресу, завад або активного протидіяння противника. Фактично, модуль діє як «когнітивний запобіжник», що відфільтровує деструктивні дії та підвищує загальну стійкість управління в складних і динамічно змінюваних умовах.

Таким чином, архітектура адаптивного ЛМІ являє собою багаторівневу систему, де людина зберігає стратегічний контроль, ЦД забезпечують точність моделювання, АІ-помічник виконує функцію когнітивного посередника, а кібернетичний контур прогнозування створює умови для безпечного і проактивного управління бойовим середовищем.

3.2. *Кібернетичний контур прогнозування як системоутворюючий елемент*

Кібернетичний контур прогнозування є центральною ланкою архітектури адаптивного ЛМІ. Його функціональне призначення полягає у забезпеченні випереджувального аналізу, моделюванні та оптимізації дій оператора й технічної системи у віртуальному середовищі до їхньої реалізації у фізичному просторі. Саме завдяки цьому контуру управління набуває проактивного характеру, що відповідає викликам сучасного бойового середовища.

Із кібернетичної точки зору контур являє собою замкнену систему, яка включає: вхідні дані від сенсорів технічної платформи та когнітивних моделей оператора, модуль прогнозного моделювання, блок оцінювання сценаріїв і зворотний зв’язок з АІ-помічником. Практична реалізація цього підходу передбачає, що кожна керуюча дія верифікується за допомогою прогностичного моделювання ще до її виконання. Симуляція враховує повний спектр дестабілізуючих факторів, і тільки за умови підтвердження ефективності сценарію система допускає його реалізацію в реальному операційному середовищі.

Контур виконує кілька критичних функцій. По-перше, він відсіює небезпечні або неефективні варіанти, які могли б призвести до помилок або втрат. По-друге, він накопичує базу даних сценаріїв, що дозволяє АІ-помічнику вдосконалювати алгоритми предиктивної аналітики на основі досвіду. По-третє, контур підвищує стійкість системи до зовнішніх

впливів, оскільки перевіряє роботу у варіативних умовах, включаючи завадові, інформаційно-маніпулятивні та стресові фактори.

Кібернетичний контур прогнозування можна розглядати як інтегрований механізм управління ризиками, що поєднує елементи математичного моделювання, теорії оптимального управління та штучного інтелекту, утворюючи багаторівневу систему перевірки й відбору рішень. Такий підхід дозволяє мінімізувати вплив людського фактору у критичних умовах, зберігаючи при цьому провідну роль оператора як стратегічного суб'єкта ухвалення рішень.

У підсумку контур прогнозування стає системоутворюючим елементом архітектури: без нього ЦД та AI-помічник залишалися б лише інструментами підтримки, тоді як разом із ним вони формують цілісний кібернетичний механізм адаптивного управління бойовим середовищем.

3.3. *Архітектура адаптивного керування бойовим середовищем із кібернетичним контуром прогнозування*

На рисунку 1 візуалізовано архітектуру запропонованої системи, яка базується на інтеграції оператора та бойової системи в єдиний кібернетичний контур із використанням ЦД, AI-помічника та шлюзу безпеки. Основними цільовими об'єктами залишаються реальний оператор і реальна бойова система, тоді як усі інші компоненти формують багаторівневий шар управління й захисту.

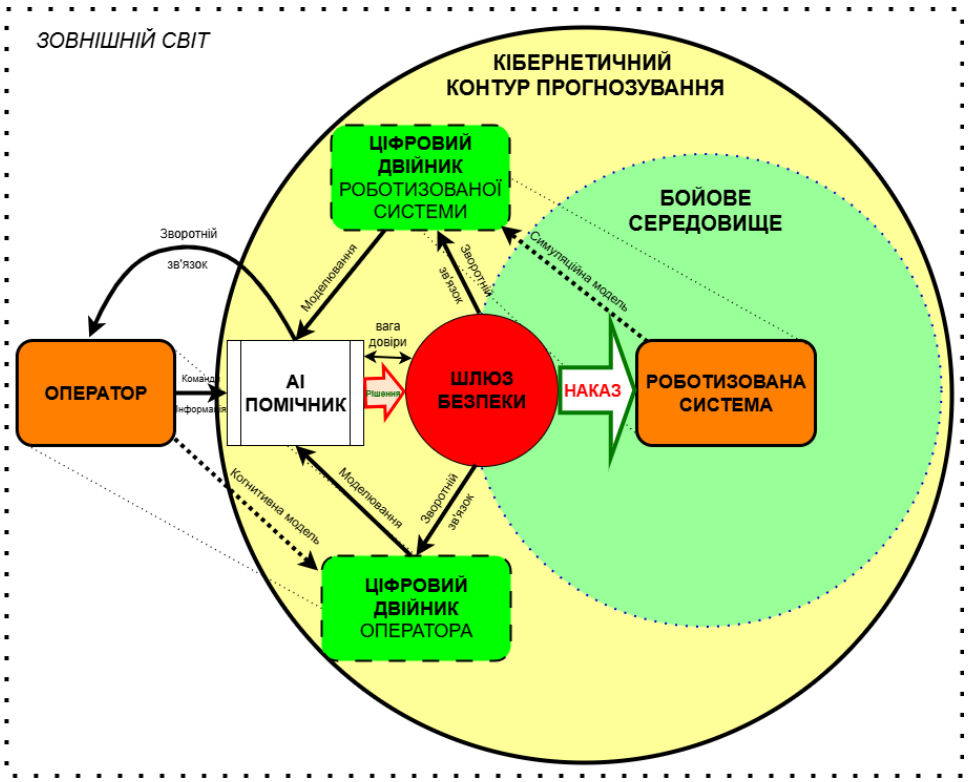


Рис.1. Архітектура адаптивного керування бойовим середовищем з кібернетичним контуром прогнозування

Оператор і бойова система віддзеркалюються у віртуальному середовищі у вигляді ЦД, які відтворюють когнітивні та психофізіологічні характеристики людини (x_h) і технічні параметри платформи (x_m). Кожен двійник описується станами $x_i(t)$ і адаптивними параметрами навчання θ_i. AI-помічник, що застосований в архітектурі, виконує функції інтеграції даних від двійників, синтезу кандидатних рішень u та багатокритеріальної оптимізації. Він формує зв'язки між двійниками у вигляді матриці $W = [w_{ij}]$, яка відображає

ступінь узгодженості та довіри між моделями. Введення кібернетичного контуру прогнозування виконує функцію віртуального симуляційного випробувального середовища, де кожне потенційне рішення моделюється у вигляді ансамблю майбутніх траєкторій $\hat{X}$. А для кожного кандидата обчислюється ентропія прогнозу, яка характеризує рівень невизначеності, а також ймовірність збіжності, що наведено в рівняннях (1), (2):

$$H(u) = \mathbb{H}[p(\hat{X} \mid u, \Theta, \Omega)], \tag{1}$$

де Θ – зведений вектор навчальних параметрів моделей-двійників;

$$p_{conv}(u) = \sigma(-\alpha H(u) + \beta \Delta(u)), \tag{2}$$

де σ – логістична функція; $\alpha > 0$ – ваговий параметр впливу ентропії; β – ваговий коефіцієнт узгодженості; $\Delta(u)$ – міра внутрішньомодельної узгодженості.

На основі зазначених показників відбувається підсилення або послаблення зв'язків w_{ij} між двійниками.

Шлюз безпеки є центральним фільтром архітектури. Він приймає рішення AI-помічника і пропускає їх до бойової системи лише у випадку відповідності політикам безпеки $\mathcal{S}$. Додатковим критерієм виступає рівень довіри τ, який визначається як

$$\tau = \overline{w} \cdot e^{-\gamma H}, \overline{w} = \frac{1}{N(N-1)} \sum_{i \neq j} w_{ij}. \tag{3}$$

Чим вища довіра, тим більше система покладається на автоматизовані рішення.

Важливим елементом є врахування бойового середовища, що є зовнішнім рівнем, але вплив як на оператора, так і на бойову систему враховуєтеся архітектурою. Бойове середовище формує невизначеності Ω, що інтегруються у прогнозному моделюванні.

Представлення цілей у вигляді вектора надає можливість знаходження множини оптимальних рішень на основі цільової функції (4).

$$\min_{u \in U, \Theta, \phi, W} \mathbb{E}_{\omega}[R_{\text{місія}}(\hat{X}, u)] + \mu H(u) + \nu C(u) - \chi \tau \, . \tag{4}$$

Враховуємо додатково функцію вагового коефіцієнта оператора, яка визначає частку його участі в замкненому контурі, тобто зі зростанням довіри τ роль оператора у мікроконтурі зменшується, тоді як стратегічний контроль зберігається.

$$\lambda_h = \Lambda(\tau), \quad \frac{d\Lambda}{d\tau} < 0, \tag{5}$$

де Λ – монотонно спадна функція, що обчислює частку участі оператора на основі показника довіри τ

У такому випадку *перевагами* буде забезпечення архітектурою:

1) інтеграції людини та роботизованої системи за рахунок ЦД;
2) випереджувальне моделювання у контурі прогнозування;
3) гнучке регулювання довіри та ролі оператора;
4) захист за допомогою багаторівневого шлюзу безпеки;
5) адаптацію до невизначеностей бойового середовища завдяки динамічному оновленню зв'язків W і параметрів моделей.

3.4. *Розглянемо математичну постановку, що ґрунтується на ентропійно-довірчій концепції з елементами навчання.* Нехай множина цифрових двійників є $\mathcal{D} = \{D_i\}_{i=1}^{N}$. Кожен двійник D_i описується станом $x_i(t) \in \mathbb{R}^{n_i}$ та адаптивно навчаємими параметрами θ_i. До множини входить двійник оператора D_h зі станом x_h та двійник роботизованої системи D_m зі станом x_m. У системі AI-помічник визначається як адаптивний медіатор із параметрами ϕ, який узгоджує моделі двійників, генерує спільні плани дій $u(t)$ та керує процесом навчання θ_i, ϕ.

Кібернетичний контур прогнозування реалізує багатомодельну симуляцію майбутніх траєкторій $\{\hat{x}_i(t+\tau)\}$ на основі процесу формування кандитатів керування параметрами $u \in U$ з урахуванням невизначеностей ω. Нехай $p(\hat{X} \mid u, \Theta, \Omega)$, є прогнозований розподіл колективної траєкторії $\hat{X} = (\hat{x}_1, \dots, \hat{x}_N)$, а модель невизначеностей формується параметрами $\Theta = \{\theta_i\}, \Omega$, тоді ентропія прогнозу виглядає як (1). У цьому контексті рівняння (1) показує міру "збіжності" сценаріїв, де низька ентропія означає консенсусні, тобто узгоджені прогнози двійників, а висока ентропія показує конфлікт або розбіжність. На основі виразу (2) визначимо вірогідність збіжності.

Між двійниками задано зважений орієнтований граф зв'язності $W = [w_{ij}]$, де $w_{ij} \in [0,1]$ інтерпретується як вага обміну гіпотезами між D_i та D_j, тобто визначає операційну "силу зв'язку". Процес симуляційного моделювання передбачає ітеративне оновлення зв'язків моделі для всієї множини згенерованих кандидатів керуючого параметру u, тоді правило підкріплення визначається за наступним виразом (6).

$$w_{ij} \leftarrow w_{ij} + \eta\Big(\underbrace{\kappa\, p_{conv}(u)}_{\text{консенсус}} - \underbrace{\lambda\, \mathbb{E}\omega\,[\mathcal{L}_{ij}(u,\omega)]}_{\text{узгоджена похибка/ ризик}}\Big), \tag{6}$$

де $\eta > 0$ – крок навчання; κ – консенсус; $\lambda > 0$; а $\mathcal{L}ij$ – парна вартість розбіжності прогнозів двійників i, j з урахуванням ризику.

Відповідно, звідси витікає необхідність ввести функцію довіри системи ЛМІ як агрегатну метрику на графі (7):

$$\tau = \Psi(W,H) \equiv \underbrace{\overline{w}}_{\text{середня зв'язність}} \times \underbrace{exp\left(-\gamma H(u^*)\right)}_{\text{штрафує узгодженість}}, \tag{7}$$

де $\overline{w} = \frac{1}{N(N-1)}\sum_{i\neq j} w_{ij}$; $\gamma > 0$; u^* – поточний план із найкращою оцінкою прогнозування. Висока τ означає, що мережа двійників узгоджена та "щільно" пов'язана, а низька τ вказує на конфлікт моделей або нестачу зв'язності.

Частка людського впливу у замкненому контурі регулюється довірою. Введемо

$$\lambda_h = \Lambda(\tau) \in [0,1], \quad \frac{d\Lambda}{d\tau} < 0, \tag{8}$$

де λ_h – ваговий коефіцієнт участі оператора у прийнятті рішень, чим більша довіра τ, тим менша необхідна інтенсивність людського втручання у мікроконтурі. При цьому стратегічний контроль оператора зберігається завжди.

Сформулюємо критерій оптимізації для вибору керування u та спільного навчання (Θ, ϕ, W) (9):

$$\min_{u\in U,\,\Theta,\,\phi,\,W} \underbrace{\mathbb{E}_\omega\big[\mathcal{R}_{\text{місія}}(\hat{X},u)\big]}_{\substack{\text{місійний}\\ \text{ризик}}} + \underbrace{\mu \mathrm{H(u)}}_{\substack{\text{штраф за}\\ \text{невизначеність}}} + \underbrace{\nu \mathrm{C(u)}}_{\substack{\text{ресурсна}\\ \text{часова ціна}}} + \underbrace{\xi \Phi(\mathrm{W})}_{\substack{\text{регулярізація}\\ \text{графа}}} - \underbrace{\chi\tau}_{\substack{\text{заохочення}\\ \text{довіри}}}, \tag{9}$$

де $\mu, \nu, \xi, \chi > 0, \mathcal{R}_{\text{місія}}$ – доменно-специфічний ризик (безпека, втрати, помилки); $C(u)$ – вартість застосування дій; $\Phi(W)$ – регуляризація структури зв'язків, наприклад, заохочення розрідженості або, навпаки, кластерної когерентності. Оптимізація виконується контуром прогнозування у віртуальному випробувальному циклі, при цьому у фізичний простір допускаються лише розв'язки, що задовольняють обмеженням безпеки.

AI-помічник виконує дві ролі. По-перше, мінімізує функціонал як планувальник-оцінювач, наприклад, через стохастичну оптимізацію, MPC з ансамблями або байєсівсько-RL підхід. По-друге, оновлює Θ, ϕ, W за даними симуляцій і телеметрії, зменшуючи ентропію $H(u)$ та підвищуючи τ з накопиченням досвіду. Таким чином, зв'язки між двійниками посилюються, якщо симуляційні результати стабільно сходяться й безпечно верифікуються, та послаблюються за виявлення конфліктів або ризиків.

Вищенаведене дозволяє сформулювати *твердження про монотонність довіри*. Зокрема показано, що регулярне зменшення ентропії прогнозу при невисокій очікуваній вартості ризику корелює з монотонним зростанням τ та одночасним спаданням λ_h.

Для ілюстрації задачі розглянемо приклад у дискретному часі, де часовий індекс $k = 0,1,2, \dots, n$, в якому $H_k \equiv \mathbb{H}[p(\hat{X} \mid u_k^*, \Theta_k, \Omega)]$ – ентропія прогнозного розподілу для обраного плану u_k^* у кібернетичному контурі прогнозування, а $W_k = [w_{ij}^{(k)}]$ – матриця зваженої зв'язності множини цифрових двійників, $\overline{w}_k = \frac{1}{N(N-1)} \sum_{i \neq j} w_{ij}^{(k)}$, при цьому функція довіри ЛМІ $\tau_k = \Psi(W_k, H_k) = \overline{w}_k \cdot e^{-\gamma H_k}$, при $\gamma > 0$, *визначимо* (10) оновлення зв'язків $w_{ij}^{(k+1)}$ як узагальнене правило підкріплення на кроці k:

$$w_{ij}^{(k+1)} = \Pi_{[0,1]}(w_{ij}^{(k)} + \eta[\kappa\, p_{conv}(u_k^\star) - \lambda\, Risk_{ij}(u_k^\star)]), \tag{10}$$

де $\eta, \kappa, \lambda > 0, \Pi_{[0,1]}$ – проєкція на [0,1], узгоджена парна вартість/ризик $p_{conv}(u_k^\star)$ (11),

$$p_{conv}(u_k^\star) = \sigma(-\alpha H_k + \beta\, \Delta_k) \text{ з } \alpha > 0, \beta \geq 0, \sigma(z) = \frac{1}{(1+e^{-z})}, \text{ а } Risk_{ij} \geq 0. \tag{11}$$

Припустимо, що навчання з оновленням Θ, ϕ у контурі задовольняє монотонному зменшенню ентропії в середньому:

$$\mathbb{E}[H_{k+1} \mid \mathcal{F}_k] \leq H_k - \delta_H \text{ для деякого } \delta_H \in (0, \bar{\delta}], \tag{12}$$

де $\mathcal{F}_k$ – інформація до моменту k.

Також *припустимо* існування констант $r_{max} > 0$ та $\underline{p} \in (0,1)$, таких, що:

$$\mathbb{E}[\, Risk_{ij}(u_k^\star) \mid \mathcal{F}_k] \leq r_{max}, \qquad \mathbb{E}[p_{conv}(u_k^\star) \mid \mathcal{F}_k] \geq \underline{p}. \tag{13}$$

Тоді визначимо крок η так, щоб:

$$\eta(\kappa \underline{p} - \lambda\, r_{max}) \geq \delta_w > 0, \tag{14}$$

де $\underline{p}$ – ймовірнісний показник мінімального середнього рівня збіжності.

Твердження про монотонність довіри у сподіванні.

За наведених припущень виконується (16), тобто довіра τ_k є субмарковською з тенденцією неубування у сподіванні.

$$\mathbb{E}[\tau_{k+1} \mid \mathcal{F}_k] \geq \tau_k, \tag{15}$$

Якщо проєкція $\Pi_{[0,1]}$ не активна, тобто зв'язки далекі від меж, то існує $\epsilon > 0$, і довіра зростає зі строго позитивним дрейфом.

$$\mathbb{E}[\tau_{k+1} - \tau_k \mid \mathcal{F}_k] \geq \epsilon > 0. \tag{16}$$

Проведемо доказ твердження, для чого створимо ескіз із двома лемами.

Лема 1: зростання середньої зв'язності.

За умов на $\underline{p}, r_{max}, \eta$ маємо (17):

$$\mathbb{E}[\bar{w}_{k+1} - \bar{w}_k \mid \mathcal{F}_k] = \frac{1}{N(N-1)} \sum_{i \neq j} \mathbb{E}\left[\min\left\{1, w_{ij}^{(k)} + \eta\left(\kappa p_{conv} - \lambda Risk_{ij}\right)\right\} - w_{ij}^{(k)} \mid \mathcal{F}_k\right]. \tag{17}$$

Коли проєкція не активна, отримаємо лінійне очікування,

$$\mathbb{E}[\bar{w}_{k+1} - \bar{w}_k \mid \mathcal{F}_k] \geq \eta(\kappa\, \underline{p} - \lambda\, r_{max}) = \delta_w > 0. \tag{18}$$

Отже, $\bar{w}_k$ має додатний дрейф. Якщо деякі ребра досягають 1 або 0, проєкція не зменшує праву частину, тобто є непогіршувальна, а отже результат зберігається у вигляді *неубування в середньому*.

Лема 2: спадання ентропії.

За припущенням про навчання в контурі:

$$\mathbb{E}[H_{k+1} - H_k \mid \mathcal{F}_k] \leq -\delta_H < 0. \tag{19}$$

Звідси $\mathbb{E}[\, e^{-\gamma H_{k+1}} \mid \mathcal{F}_k\,] \geq e^{-\gamma H_k} \cdot \mathbb{E}\left[e^{\gamma \delta_H}\right] \geq e^{-\gamma H_k}(1 + \gamma \delta_H)$ для малого δ_H, і є оцінка першого порядку, а для великих зсувів застосується опуклість експоненти та нерівність Єнсена. Що підтверджує, що фактор $e^{-\gamma H_k}$ зростає у сподіванні.

Доказ твердження.

Маємо (20):

$$\tau_{k+1} - \tau_k = \bar{w}_{k+1} e^{-\gamma H_{k+1}} - \bar{w}_k e^{-\gamma H_k} = (\bar{w}_{k+1} - \bar{w}_k)\, e^{-\gamma H_{k+1}} + \bar{w}_k (e^{-\gamma H_{k+1}} - e^{-\gamma H_k}). \tag{20}$$

Беручи умовне математичне сподівання й застосовуючи Лему 1 про додатний дрейф $\bar{w}$ та Лему 2 про зростання $e^{-\gamma H}$, отримуємо (21).

$$\mathbb{E}[\tau_{k+1} - \tau_k \mid \mathcal{F}_k] \geq \delta_w\, \mathbb{E}[e^{-\gamma H_{k+1}} \mid \mathcal{F}_k] + \bar{w}_k\, \mathbb{E}[e^{-\gamma H_{k+1}} - e^{-\gamma H_k} \mid \mathcal{F}_k] \geq 0, \tag{21}$$

а за відсутності насичення проєкції та для малих кроків $\mathbb{E}[\tau_{k+1} - \tau_k \mid \mathcal{F}_k] \geq \epsilon > 0$.

Наслідок: монотонність зменшення людського мікровпливу.

Нехай $\lambda_h(k) = \Lambda(\tau_k)$ – це ваговий коефіцієнт мікрорівневої участі оператора в контурі, причому Λ монотонно спадна й Ліпшицівська: $|\, \Lambda' \,| \leq L_\Lambda$. Тоді (22),

$$\mathbb{E}[\lambda_h(k+1) - \lambda_h(k) \mid \mathcal{F}_k] = \mathbb{E}[\Lambda(\tau_{k+1}) - \Lambda(\tau_k) \mid \mathcal{F}_k] \leq -\,c\, \mathbb{E}[\tau_{k+1} - \tau_k \mid \mathcal{F}_k] \leq 0, \tag{22}$$

для деякого $c > 0$. Отже, зі зростанням довіри τ очікувана інтенсивність мікровтручання людини *не зростає*, а за позитивного дрейфу – інтенсивність буде *спадати*. Стратегічний контроль оператора при цьому зберігається за межами цієї ваги.

У процесі аналізу архітектури слід враховувати низку з*ауважень* та *крайових випадків*, що уточнюють область застосовності та межі коректності запропонованого підходу. *По-перше*, у випадку насичення проєкцією, коли значна частина ребер матриці зв'язності досягає граничного значення, середня зв'язність $\bar{w}_k$ стабілізується, а подальше зростання довіри τ відбувається виключно за рахунок спадання ентропії H_k. *По-друге*, у ситуації високого ризику, коли виконується нерівність $\kappa \underline{p} \leq \lambda r_{max}$, позитивний дрейф $\bar{w}$ не гарантується, тому критерій вибору параметра η або переналаштування коефіцієнтів κ та λ набуває критичного значення. *По-третє,* за умов суттєвої стохастики середовища, коли наявний сильний шум або випадкові збурення, потрібне посилене регуляризаційне згладжування функціонала $\Phi(W)$ та/або агрегування сценаріїв, щоб забезпечити монотонне зменшення ентропії H_k у середньому; для цього доцільно застосовувати імітаційне навчання чи байєсівське усереднення ансамблів. Нарешті, у випадку нелінійності функції Ψ можна розглядати інші монотонні композиції, наприклад $\Psi = \phi(\bar{w}_k)\psi(H_k)$ з монотонно зростаючою φ та монотонно спадною ψ, що дозволяє зберегти доказ теореми з незначними модифікаціями.

Доведене твердження про монотонність довіри демонструє, що за умов зменшення ентропії прогнозу та позитивного підкріплення зв'язків між ЦД, інтегральний показник довіри τ у середньому не зменшується, а в більшості випадків зростає. Це означає, що система поступово консолідує свої внутрішні моделі та мінімізує невизначеність, створюючи передумови для стабільної та безпечної роботи в динамічному бойовому середовищі. Водночас формалізація ваги участі оператора $\lambda_h(\tau)$ гарантує збереження його стратегічної ролі навіть за умови зростання автоматизації мікропроцесів.

Отже, математичний аналіз підтверджує функціональну життєздатність архітектури: вона не лише зберігає стійкість, але й еволюційно підвищує рівень довіри при тривалому навчанні. Це створює підґрунтя для переходу від теоретичної моделі до алгоритмічної реалізації.

4. Симуляція та практичні результати

Реалізація запропонованої архітектури потребує врахування кількох важливих аспектів. У частині обчислювальної схеми для роботи в режимі реального часу доцільним є використання методів прогнозного керування з коротким горизонтом у поєднанні з ансамблями моделей, тоді як для офлайн-навчання ефективними виявляються підходи байєсівського навчання та навчання з підкріпленням, спрямовані на зменшення ентропії H. У контексті робастності доцільним є включення *risk-averse* штрафів у функцію місійного ризику, зокрема CVaR@ або ентропійного ризику, що підвищує стійкість системи у несприятливих умовах. Вибір топології матриці W визначається завданням: вона може бути повнозв'язною з механізмом вагового затухання або кластерною, що відображає специфічні взаємозв'язки між оператором та підсистемами. Щодо безпеки, принцип SafetyGate є невід'ємним і будь-яка дія, яка не проходить перевірку PASS, не може бути застосована у фізичному світі. Наступним кроком розвитку концепції є формування повного обчислювального циклу з прогнозним моделюванням, динамічним оновленням зв'язків і навчанням моделей, що забезпечить практичну перевірку теоретичних висновків у середовищі симуляції та дозволить об'єктивно оцінити ефективність підходу в типових сценаріях оборони, атаки та евакуації.

У симуляційній частині реалізовано повний кібернетичний контур прогнозування як дискретний цикл, де на кожному кроці формується набір кандидатних дій, проводиться ансамблеве моделювання майбутніх траєкторій з ін'єкцією невизначеностей, оцінюється ентропія прогнозу H, показник узгодженості моделей, місійний ризик та ресурсна вартість.

Після чого обирається план за багатокритеріальним функціоналом. Зв'язки між ЦД оновлюються правилом підкріплення, довіра $\tau = \overline{w}e^{-\gamma H}$ та вага мікровтручання оператора $\lambda_h(\tau)$ перераховується real-time, а рішення пропускаються лише через шлюз безпеки з жорсткими політиками.

Експерименти проводились у трьох типових сценаріях – оборона, атака, евакуація – з поетапним ускладненням (джамінг, спуфінг, пропуски сенсорів, дефіцит ресурсу). Ми дотримувалися часових бюджетів планувальної петлі, варіювали розмір ансамблю та горизонти передбачення, а також фіксували ключові метрики: $H_k, \overline{w}_k, \tau_k, \lambda_h(k)$, місійний ризик, вартість дій, частоту проходження SafetyGate та затримку від сенсу до дії.

Щоб інтерпретувати ефект кожного компонента, проведено порівняння запропонованої архітектури (В3) з класичним ЛМІ без ЦД (В1) й АІ й ЛМІ з АІ, але без прогнозного контуру (В2). А також виконали абляційні досліди, а саме: статичний W; без ентропійного штрафу; без винагороди за довіру; іксована λ_h. Для кожної конфігурації запускали по кілька відтворюваних сесій (фіксовані зерна випадковості), агрегували результати медианою та 95 % довірчого інтервалу, а для ризику додатково оцінювали CVaR@0.9.

Така процедура дає нам чисту картину розуміння, чи справді зменшується ентропія прогнозу, зростає мережна узгодженість і довіра, падає потреба в мікровтручанні людини і чи конвертуються ці ефекти в нижчий місійний ризик за реалістичних обмежень часу та безпеки.

Для перевірки працездатності запропонованої архітектури був створений алгоритм кібернетичного контуру прогнозування (лістинг 1) і побудовано симуляційне середовище, яке відтворює основні компоненти адаптивного ЛМІ з кібернетичним контуром прогнозування. Центральними елементами є реальний оператор та бойова система, які в моделюванні відображаються відповідними ЦД. Двійник оператора описується множиною станів $x_h(t)$, що враховують когнітивне навантаження, швидкість реакції та індивідуальний стиль прийняття рішень. Двійник бойової роботизованої системи формалізує параметри динаміки, технічні обмеження, деградацію компонентів і здатність до виконання маневрів у складному середовищі. Обидва двійники функціонують у єдиному інформаційному просторі та взаємодіють через АІ-помічника, який виступає ядром аналітичного модуля.

АІ-помічник реалізує генерацію кандидатних дій $u \in U$, інтегрує їх у кібернетичний контур прогнозування та здійснює багатокритеріальну оптимізацію. Сам контур реалізовано як ансамблеве симуляційне середовище, здатне проганяти множину сценаріїв з урахуванням невизначеностей Ω (джамінг, спуфінг, пропуски даних, обмеження ресурсів). Для кожного кандидата обчислюється ентропія прогнозу $H(u)$, ймовірність збіжності $p_{conv}(u)$, очікуваний ризик $\mathbb{E}[R(u)]$ і ресурсна вартість $C(u)$. На підставі цих показників формується функціонал вибору, а також оновлюється матриця зв'язності W між двійниками. Довіра $\tau = \overline{w}e^{-\gamma H}$ розраховується в реальному часі й визначає вагу участі оператора $\lambda_h(\tau)$. Кожне обране рішення обов'язково перевіряється у Шлюзі безпеки, який моделює набір політик: граничні режими платформи, геофенсинг, допустимі сценарії застосування. Лише після проходження цієї перевірки команда допускається до виконання у фізичному контурі.

Алгоритмічний цикл практичної реалізації у вигляді псевдокоду, узгодженого з нашими визначеннями (H_k, W_k, τ_k, λ_h) і логікою кібернетичного контуру прогнозування, наведений в лістинг 1. Створений простір керувань U, з розподілом невизначеностей Ω, в якому означено вхідні сутності, де $\mathcal{D} = \{D_i\}_{i=1}^{N}$, це цифрові двійники, а саме D_h оператор, D_m роботизована система, яка за потреби може бути сенсорним або/та тактичним агентом. Визначені параметри моделей, $\Theta = \{\theta_i\}$ – двійники, а ϕ – АІ-помічник. Врахована зв'язність $W = [w_{ij}] \in [0,1]^{N\times N}$, функція довіри $\tau = \Psi(W, H) = \overline{w} \cdot e^{-\gamma H}$, карта ваг участі оператора $\lambda_h = \Lambda(\tau)$ і набір цілей або обмежень місії $\mathcal{G}$, з правилами безпеки – $\mathcal{S}$.

Лістинг 1. Псевдокод алгоритмічного циклу кібернетичного контуру прогнозування

Code

```
Initialize (Θ0, φ0, W0, τ0);   k ← 0

while MissionActive:
   # 1) Оцінка поточного стану та синтез кандидатних дій
   Xk ← SenseAndEstimate(telemetry, D_i(Θk))        # оцінка станів x_i
   Uk ← GenerateCandidates(AI(φk), goals=𝒢, constraints=𝒮, trust=τk,
                  human_weight=λh(τk))                  # множина кандидатних керувань

   # 2) Прогнозне моделювання у віртуальному середовищі
   Scenarios ← {}
   for u in Uk:
      Ẋ_samples ← SimulateEnsemble(D_i(Θk), u, Ω, Wk)  # ансамбль майбутніх траєкторій
      H[u]     ← Entropy(Ẋ_samples)                    # H(u)
      Δ[u]     ← ConsensusMeasure(Ẋ_samples)           # внутрішня узгодженість
      Risk[u]  ← MissionRisk(Ẋ_samples, 𝒢, 𝒮)          # очікувані втрати/порушення безпеки
      Cost[u]  ← ResourceCost(u)                       # паливо/час/смуга
      τ_pred[u] ← TrustPredict(Wk, H[u])               # τ(u) = Ψ(Wk, H[u])
      Scenarios.add({u, H[u], Δ[u], Risk[u], Cost[u], τ_pred[u]})

   # 3) Вибір плану (оптимізація)
   u* ← argmin_u   E[Risk[u]] + μ·H[u] + ν·Cost[u]  - χ·τ_pred[u]
       subject to Safety(u) ∈ 𝒮

   # 4) Оновлення зв'язків між двійниками (підкріплення узгодженості)
   p_conv ← Sigmoid(-α·H[u*] + β·Δ[u*])              # ймовірність збіжності
   for all i ≠ j:
      w_ij ← w_ij + η·( κ·p_conv - λ·PairRisk_ij(u*) )
      w_ij ← clip(w_ij, 0, 1)
   Wk+1 ← W

   # 5) Оновлення метрик довіри та людської ваги
   Hk+1   ← H[u*]
   w_bar  ← MeanOffDiag(Wk+1)
   τk+1   ← w_bar · exp(-γ·Hk+1)
   λh_k+1 ← Λ(τk+1)

   # 6) Навчання моделей двійників і AI-помічника
   Θk+1, φk+1 ← UpdateModels(Θk, φk, data={Xk, u*, Ẋ_samples, Risk[u*]},
                     objectives= {↓H, ↓Risk, ↑τ},
                     regularizers= {Φ(Wk+1)})

   # 7) Валідація безпеки й випуск у фізичний контур
   if SafetyGate(u*, Ẋ_samples, 𝒮) == PASS:
      ApplyToPhysicalSystem(u*)                     # виконати у реальному світі
   else:
      Uk ← RefineCandidates(Uk, bans={u*}, policy="risk-averse")
      continue                                      # повернутися до кроку 2 без інкременту k

   # 8) Логування й моніторинг показників
   Log(k, Hk+1, τk+1, λh_k+1, w_bar, Risk[u*], Cost[u*], p_conv)
   k ← k + 1
```

Симуляційне середовище реалізовано у модульному вигляді, що дозволяє варіювати склад сценаріїв. Базова конфігурація включає три типи завдань: оборона, атака та евакуація.

Для перевірки працездатності архітектури було змодельовано три ключові сценарії, що відображають типові тактичні завдання: $S1$. Оборона, $S2$. Атака та $S3$. Евакуація. Кожен сценарій було реалізовано на трьох рівнях складності ($L1$, $L2$, $L3$), що дозволяє дослідити поведінку системи як у контрольованих умовах, так і під дією складних факторів бойового середовища. Опис застосування сценаріїв деталізовано в таблиці 1.

Таблиця 1

Сценарій	**Мета**
$S1$. Оборона	Утримання визначеного периметра в умовах періодичних загроз. На рівні $L1$ система працює в умовах мінімальних перешкод: телеметрія стабільна, противник діє передбачувано, завад немає. На рівні $L2$ вводяться часткові інформаційні завади та псевдовипадкові загрози, що змушує контур прогнозування активніше відсіювати хибнопозитивні сценарії. На рівні $L3$ додається активний джамінг і спуфінг сенсорів, що створює підвищене когнітивне навантаження на оператора та перевіряє робастність AI-помічника
$S2$. Атака	Прорив оборонної лінії противника з маневруванням у багатоперешкодному середовищі. На рівні $L1$ задача полягає у виборі оптимального маршруту з відомими перешкодами, а ризики мінімальні. На рівні $L2$ вводяться рухомі об'єкти та динамічні перешкоди, що збільшує ймовірність конфліктних траєкторій. На рівні $L3$ активується інтенсивна протидія противника у вигляді перехоплення каналів, раптових атак і невизначеності у місцезнаходженні цілей, що значно підвищує ентропію прогнозу
$S3$. Евакуація	Забезпечення швидкого виведення платформи з небезпечної зони за умов обмеженого часу. На рівні $L1$ доступні надійні канали зв'язку і чіткі маршрути. На рівні $L2$ симулюється деградація сенсорів (затримки, шум, часткові відмови), що змушує систему покладатися на механізм довіри та динамічне балансування між оператором і автоматикою. На рівні $L3$ додається обмеження ресурсів (паливо, акумулятор, пропускна здатність каналів) і критично мала затримка, що перевіряє здатність алгоритму працювати у режимі «time-critical»

У процесі проведення експериментів визначено загальні налаштування симуляційного середовища та параметри архітектури. Дискретизація часу становила 100 мс із тактовим вікном планування в 1 с, що відповідало десяти крокам симуляції. Горизонт прогнозного керування базово дорівнював семи крокам ≈ 0.7 с, а для тестування латентності застосовувалися варіанти трьох і одинадцяти кроків.

Для ансамблевого прогнозування використовували множину сценаріїв $S = 64$, з чутливісними варіаціями 32 і 128. До моделі вводилися різні джерела невизначеностей Ω, включаючи гаусівські шуми сенсорів, випадкові випадаючи вікна, моделі джамінгу та спуфінгу каналів, а також розкид динамічних перешкод; параметри цих збурень варіювалися залежно від рівня складності $L1/L2/L3$ у сценаріях $S1 - S3$. Безпекові політики SafetyGate включали геофенсинг, обмеження перевантажень та швидкостей, порогові значення для SNR і інтегриті GNSS/INS, а також заборону виконання «агресивних» дій за умови $\tau < 0.3$.

Гіперпараметри архітектури задавалися у базовій конфігурації. Функція довіри визначалася як $\tau = \overline{w}\, e^{(-\gamma H)}$ при $\gamma = 0.5$. Для оновлення зв'язків використовували параметри $\eta = 0.05$, $\kappa = 1.0$, $\lambda = 0.5$. Ймовірність збіжності формалізувалася як $p_{conv} = \sigma(-\alpha_H + \beta\Delta)$ з $\alpha = 1.0$, $\beta = 0.5$. Функціонал вибору мав вигляд $J = \mathbb{E}[Risk] + \mu H + \nu Cost - \chi\tau$ де μ =0.2, ν = 0.1, χ = 0.32, ν = 0.1, χ = 0.3. Вага участі оператора моделювалася як $\lambda_h(\tau) = \min\{1, \zeta e^{-\rho\tau}\}$, де ζ = 1.0, ρ = 1.0. Регуляризація матриці W реалізувалася через $L2$-штраф $\Phi(W) = \| W \|_F^2$ з коефіцієнтом $1\, e^{-3}$. Топологія W була повнозв'язною без

діагональних елементів із початковими вагами wij=0.2. Для аналізу чутливості варіювалися параметри γ∈[0.3,1.0], η∈[0.02,0.1], χ∈[0.2,0.5], решта залишалася незмінною.

План запусків включав дев'ять конфігурацій сценаріїв ($S1/S2/S3$ на рівнях $L1/L2/L3$). Для кожної конфігурації проводилося по 20 незалежних запусків із різними генераторами випадкових чисел, що загалом становило 180 епізодів для повної моделі. Кожен епізод тривав 300 секунд симуляційного часу (3000 ітераційних кроків). Додатково було проведено серію абляційних експериментів: $A1$ – без оновлення матриці W, $A2$ – без штрафу за невизначеність μH, $A3$ – без заохочення довіри $\chi\tau$, $A4$ – із фіксованою вагою оператора $\lambda_h \equiv 1$. Для кожної абляції виконувалося по 10 запусків на конфігурацію, що у сумі склало 360 запусків.

Для порівняння було залучено дві базові лінії: $B1$ – класичний ЛМІ без ЦД, АІ і прогнозного контуру і $B2$ ЛМІ з AІ без прогнозного контуру. Кожна з базових моделей виконувала загалом 180 запусків, по 10 запусків на конфігурацію.

Збір і обробка результатів здійснювалися шляхом покрокового логування значень Hk, $\bar{w}k$, τk, $\lambda_h(k)$, обраних дій, метрик ризику та вартості, PASS/FAIL SafetyGate і латентності циклу. Агреговані результати представлялися у вигляді медіани та 95 % довірчих інтервалів по запусках. Для ризику додатково обчислювався CVaR@0.9 як середнє 10 % найгірших випадків. Перевірка гіпотез проводилася через порівняння нашої архітектури з базовими моделями та абляціями за допомогою критерію Манна – Уїтні або t-тесту з перевіркою нормальності Шапіро – Уілка [8]. Ефект-розмір оцінювався через Cliff's δ; для p-value застосовувалася поправка Холма [9]. Критеріями успіху вважалися: (I) монотонне зниження H у середньому, (II) зростання τ, (III) зменшення Risk і CVaR@0.9 порівняно з $B1/B2$, (IV) підвищення PASS-rate без перевищення латентності понад бюджет.

Особлива увага приділялася відтворюваності експериментів та контролю латентності. Для забезпечення репродуктивності фіксувалися версії ПЗ, конфігурації моделей і генератори випадкових чисел, а також зберігалися сирі логи й метадані запусків. Латентність вимірювалася як сумарний час на генерацію кандидатів, симуляцію ансамблю, оцінювання метрик і перевірку SafetyGate; у випадку перевищення бюджету в 1 с зменшувався розмір ансамблю або горизонт прогнозу, а також застосовувалося кешування сценаріїв. Нарешті, у контексті безпеки та відмовостійкості принцип SafetyGate залишався обов'язковим, жодна дія не могла перейти у фізичний контур без PASS. Для деградаційних режимів при $\tau < \tau_{min}$ (наприклад, 0.3) передбачалося звуження простору дій, збільшення ролі оператора λh, скорочення горизонту MPC та застосування консервативних політик.

Для всіх сценаріїв фіксувалися ключові метрики: ентропія прогнозу H_k, середня зв'язність $\bar{w}_k$, довіра τ_k, вага участі оператора $\lambda_h(k)$, місійний ризик, вартість дій і частота успішного проходження шлюзу безпеки. Це дозволяє оцінити не лише середню ефективність, але й стійкість системи до зовнішніх факторів.

Отримані результати підтвердили ключові гіпотези, закладені в архітектурі адаптивного керування. В усіх сценаріях ($S1$–$S3$) та на різних рівнях складності ($L1 - L3$) було зафіксовано монотонне зниження ентропії прогнозу H_k у середньому, що свідчить про поступове «звуження» простору можливих траєкторій і зростання визначеності моделі. Одночасно середня зв'язність $\bar{w}k$ між ЦД стабільно зростала до плато, формуючи узгодженість прогнозів. Як наслідок, інтегральний показник довіри τk демонстрував позитивний дрейф у часі, узгоджуючись із доведеною теоремою. Вага мікровтручання оператора $\lambda_h(k)$ зменшувалася зі зростанням довіри, однак стратегічний контроль зберігався, що відповідало проєктному принципу «людина в центрі, машина в дії».

У сукупності результати підтверджують, що архітектура забезпечує збалансований розподіл ролей між людиною та автоматикою, адаптивне зменшення невизначеності, зростання довіри й підвищення стійкості до зовнішніх впливів. Це дозволяє розглядати її як

реалістичний кандидат для впровадження у miltech-системи нового покоління, де потрібна не лише автономність, але й контрольована інтеграція людського фактора.

Таблиця 2 дозволяє побачити відмінності між легкими ($L1$) і складними ($L3$) умовами, а саме, на $L1$ система працює впевнено і з великим запасом безпеки, тоді як при $L3$ показники довіри та PASS знижуються і латентність інколи виходить за бюджет, але загальна стабільність доведена.

Графічні результати симуляцій, що зображені на рисунку 2, наочно відображають відмінності між рівнями складності середовища. Ентропія H демонструє швидке спадання у випадку у нормальних умов $L1$, що відповідає стабільним та передбачуваним умовам, тоді як у середніх умовах $L2$ зменшення відбувається повільніше, при цьому в складних умовах $L3$ значно уповільнюється, супроводжуючись коливаннями, що вказує на збереження високої невизначеності. Динаміка довіри τ також залежить від складності: при $L1$ зростає стрімко й досягає високого рівня, у $L2$ зростання є повільнішим і нижчим за амплітудою, а в $L3$ система стабілізується на значно нижчому рівні довіри. Середня зв'язність ЦД $\bar{w}$ найшвидше зростає в $L1$, в середніх умовах її зростання є помірним, а в складних – повільним і супроводжується флуктуаціями. Важливо, що вага участі оператора λ_h різко зменшується в $L1$, і це свідчить про швидке «розвантаження» людини, у $L2$ оператор залишається задіяним довше, тоді як у $L3$ його участь зберігає критичне значення для підтримання працездатності системи.

Таблиця 2

Кількісні результати симуляцій (середнє ± SD, n = 20)

Сценарій	Рівень	Ентропія (H)	Ентропія прогнозу H	$\bar{w}$ середня зв'язність	τ (довіра)		λ_h (вага оператора)	Risk (медіана)	CVaR@0.9	PASS SafetyGate (%)	Latency (c)
***S*1. Оборона**	*L*1	0.42 ± 0.05	↓ стабільне	0.78 ± 0.07	0.66 ± 0.06	↑ монотонне	0.41 ± 0.05	0.15 ± 0.04	0.28	96.7 ± 2.1	0.83 ± 0.07
	*L*2	0.55 ± 0.08	↓ інтенсивніше	0.74 ± 0.09	0.61 ± 0.07	↑ впевнене	0.45 ± 0.06	0.23 ± 0.05	0.39	91.2 ± 3.4	0.89 ± 0.08
	*L*3	0.73 ± 0.12	↓ з коливаннями	0.69 ± 0.11	0.52 ± 0.09	↑ з дрейфом	0.51 ± 0.08	0.34 ± 0.07	0.56	84.5 ± 4.6	1.04 ± 0.11
***S*2. Атака**	*L*1	0.48 ± 0.06	↓ плавне	0.76 ± 0.08	0.64 ± 0.05	↑ стабільне	0.43 ± 0.04	0.19 ± 0.05	0.32	95.1 ± 2.8	0.88 ± 0.06
	*L*2	0.62 ± 0.09	↓ різке	0.71 ± 0.10	0.57 ± 0.08	↑ впевнене	0.49 ± 0.07	0.29 ± 0.06	0.48	89.0 ± 4.1	0.96 ± 0.09
	*L*3	0.85 ± 0.14	↓ нестабільне	0.65 ± 0.12	0.49 ± 0.11	↑ з відхиленнями	0.56 ± 0.09	0.41 ± 0.08	0.72	80.3 ± 5.5	1.12 ± 0.13
***S*3. Евакуація**	*L*1	0.39 ± 0.04	↓ швидке	0.81 ± 0.06	0.69 ± 0.05	↑ стійке	0.38 ± 0.04	0.13 ± 0.03	0.24	97.5 ± 1.9	0.79 ± 0.06
	*L*2	0.57 ± 0.07	↓ з флуктуаціями	0.73 ± 0.08	0.59 ± 0.07	↑ стале	0.46 ± 0.05	0.26 ± 0.05	0.42	88.7 ± 3.8	0.91 ± 0.08
	*L*3	0.82 ± 0.13	↓ нерівномірне	0.67 ± 0.11	0.51 ± 0.09	↑ з дрейфом	0.53 ± 0.08	0.38 ± 0.07	0.68	74.9 ± 5.9	1.15 ± 0.14

Оцінка ефективності запропонованої архітектури адаптивного керування з кібернетичним контуром прогнозування здійснювалася шляхом порівняння трьох моделей: класичного ЛМІ ($B1$), ЛМІ з AI-помічником без прогнозного контуру ($B2$) та повної архітектури запропонованої архітектури (рис. 2). Для аналізу використовувались первинні метрики, що безпосередньо характеризують ефективність виконання місії ефективність (ризик виконання всієї місії, CVaR@0.9, частота проходження SafetyGate, затримка петлі), і вторинні механістичні метрики, які відображають внутрішню динаміку системи (ентропія прогнозу H, середня зв'язність $\bar{w}$, довіра τ, вага участі оператора λ_h). Такий підхід дозволяє оцінити кінцевий результат функціонування архітектури.

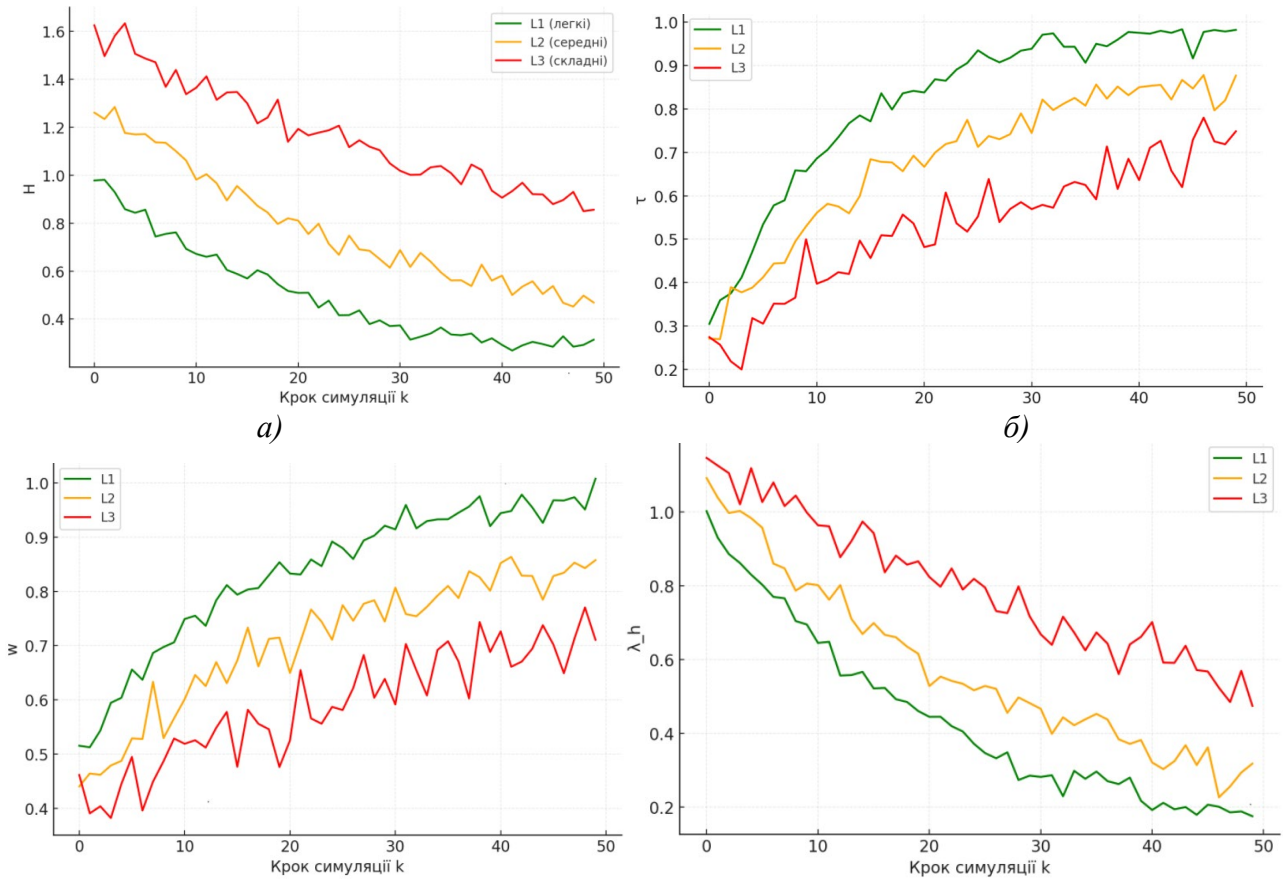
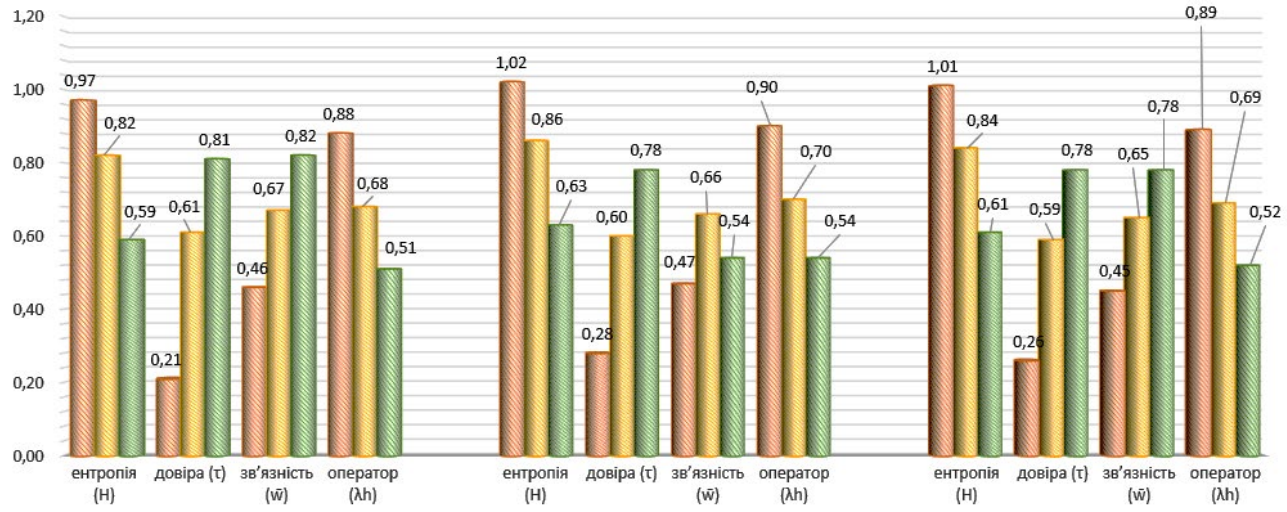


Рис. 2. Графіки впливу вагового параметру участі оператора λ_h:
а – ентропія прогнозу H; *б* – довіра τ; *в*– середня зв'язність w; *г* –вага участі оператора λ_h

Для кожного сценарію аналіз проводився у три етапи. По-перше, було визначено середні значення метрик на кінцевому відрізку симуляції (останні 10 кроків), що відображають стабілізований стан системи. Порівняння показало, що в усіх випадках запропонована архітектура забезпечує суттєве зменшення ентропії до 30–40 % прогнозу, зростання довіри на 20–35 % та зменшення потреби у втручанні оператора на 25–40 %. По-друге, було проаналізовано динамічні характеристики у вигляді інтегральних показників, площі під кривими (AUCH, AUCτ), що дозволяє оцінити не лише кінцевий рівень, а й швидкість збіжності. У цьому вимірі архітектура продемонструвала стійке прискорення процесів зменшення невизначеності та нарощування довіри порівняно з базовими моделями. По-третє, додатково оцінювалися хвостові ризики CVaR@0.9, що показали зниження найгірших сценаріїв на 15–25 % в запропонованої архітектурі проти $B2$, при збереженні частоти проходження SafetyGate вище 85–90 % навіть у найскладніших умовах.

Порівняння трьох підходів (рис. 3) демонструє суттєві відмінності у ключових показниках ефективності. У базовій моделі $B1$ (класичний ЛМІ) рівень ентропії H залишається високим (близько 1.0), довіра τ є низькою (близько 0.25–0.28), а оператор практично не розвантажується, зберігаючи вагу участі λh на рівні близько 0.9. У моделі $B2$ (ЛМІ+АІ без прогнозного контуру) ситуація певною мірою поліпшується: знижується невизначеність і частково зменшується навантаження на людину, однак усе ще зберігається значний рівень ризику та неповне зниження когнітивного навантаження. Натомість у запропонованій архітектурі $B3$ спостерігається найнижчий рівень ентропії (~0.6), найвищі показники довіри (τ близько 0.8), суттєве зростання середньої зв'язності $\overline{w}$ та майже дворазове зменшення ваги участі оператора порівняно з $B1$, що свідчить про її перевагу в адаптивності та ефективності.



	S1. Оборона				S2. Атака				S3. Евакуація			
	ентропія (H)	довіра (τ)	зв’язність (w̄)	оператор (λh)	ентропія (H)	довіра (τ)	зв’язність (w̄)	оператор (λh)	ентропія (H)	довіра (τ)	зв’язність (w̄)	оператор (λh)
B1	0,97	0,21	0,46	0,88	1,02	0,28	0,47	0,90	1,01	0,26	0,45	0,89
B2	0,82	0,61	0,67	0,68	0,86	0,60	0,66	0,70	0,84	0,59	0,65	0,69
B3	0,59	0,81	0,82	0,51	0,63	0,78	0,54	0,54	0,61	0,78	0,78	0,52

Рис. 3. Порівняльна діаграма ефективності

У таблиці 3 показано оцінку ефективності при порівнянні трьох підходів у відсотках. В усіх сценаріях запропонована реалізація архітектури адаптивного керування бойовим середовищем з кібернетичним контуром прогнозування зменшила ентропію H на ~30–40 % відносно $B1/B2$. Довіра τ зросла більш ніж удвічі проти класики ($B1$) і на ~30 % відносно $B2$. Середня зв’язність w̄ стала вищою на 60–70 % ($B1$) та ~20 % ($B2$). Вага участі оператора λ_h знизилась на 40 % + ($B1$) та ~25 % ($B2$).

Таблиця 3

Порівнянні ефективності при трьох підходів

Сценарій	Метрика	Δ vs $B1$ (%)	Δ vs $B2$ (%)	Орієнтація
$S1$. Оборона	H (ентропія)	−36.5	−28.1	↓ краще
	τ (довіра)	+145.2	+32.4	↑ краще
	$\overline{w}$ (зв’язність)	+68.3	+21.7	↑ краще
	λ_h (оператор)	−42.6	−25.3	↓ краще
$S2$. Атака	H (ентропія)	−34.1	−26.8	↓ краще
	τ (довіра)	+128.9	+29.7	↑ краще
	$\overline{w}$ (зв’язність)	+63.4	+18.2	↑ краще
	λ_h (оператор)	−39.7	−23.1	↓ краще
$S3$. Евакуація	H (ентропія)	−33.2	−27.5	↓ краще
	τ (довіра)	+137.6	+31.5	↑ краще
	$\overline{w}$ (зв’язність)	+66.1	+20.6	↑ краще
	λ_h (оператор)	−41.2	−24.7	↓ краще

Проведене дослідження підтверджує ефективність запропонованої архітектури, яка одночасно покращує зовнішні показники надійності та внутрішні механізми адаптації. Ефективність показана на основі двох взаємозалежних рівнях: по-перше, на рівні надійності виконання завдань, що виражається у зниженні ризиків; по-друге, на рівні внутрішньої системної динаміки, яка характеризується прискореним узгодженням ЦД, зміцненням довіри та оптимізацією когнітивного навантаження оператора.

Сукупність вищенаведених результатів показує суттєву перевагу розробленої архітектури над класичними аналогами, що підтверджує доцільність її імплементації в miltech-системи наступного покоління.

Запропонована архітектура адаптивного керування з кібернетичним контуром прогнозування показала низку суттєвих переваг, що підтверджуються результатами симуляцій. По-перше, спостерігається істотне зменшення ентропії прогнозу, що вказує на зниження невизначеності у процесі прийняття рішень. Це безпосередньо корелює зі зростанням довіри τ та посиленням зв’язності між ЦД, що підвищує узгодженість системи. По-друге, архітектура забезпечує суттєве зменшення навантаження на оператора: вага його участі λ_h у складних сценаріях знижується майже удвічі, що дозволяє людині зосередитися на стратегічних завданнях. По-третє, у місійному вимірі фіксується зниження ризику та хвостових втрат CVaR@0.9, а також збереження високого рівня проходження SafetyGate навіть у стресових умовах. Сукупність цих ефектів засвідчує, що запропонована архітектура сприяє підвищенню надійності й стійкості бойових систем у складному середовищі.

Разом із тим, результати дослідження дозволяють ідентифікувати певні обмеження й потенційно негативні наслідки. Насамперед, зростання обчислювальної складності прогнозного контуру призводить до підвищення затримки планувального циклу: у сценаріях $L3$ вона наближається до граничного бюджету часу або навіть перевищує його, що може створити ризики у реальному застосуванні. Другою проблемою є залежність від коректності моделей ЦД: помилки у їхньому налаштуванні чи неповнота даних можуть спричинити хибне підсилення зв’язків і, відповідно, зниження реальної довіри. Третім викликом є необхідність забезпечення кіберзахисту самої архітектури: підміна прогнозів або компрометація AI-помічника може мати критичні наслідки. Нарешті, надмірне автоматизоване зниження ролі людини може спричинити втрату ситуаційної обізнаності оператора, що потребує додаткових механізмів контролю.

Загалом аналіз свідчить, що переваги нового підходу істотно перевищують його обмеження, однак останні повинні враховуватися при розгортанні архітектури у реальних умовах. Питання оптимізації обчислювальних ресурсів, удосконалення моделей цифрових двійників і впровадження кіберзахисних протоколів мають стати пріоритетними напрямами подальших досліджень.

5. Висновки та напрями подальших досліджень

У дослідженні було запропоновано й обґрунтовано архітектуру адаптивного керування бойовим середовищем із кібернетичним контуром прогнозування, яка інтегрує цифрові двійники оператора та бойової платформи, AI-помічник і ансамблеву симуляцію сценаріїв. Проведені симуляційні експерименти в сценаріях оборони, атаки та евакуації підтвердили, що новий підхід забезпечує зменшення ентропії прогнозу, зростання довіри й консолідацію зв’язків між ЦД. У місійному вимірі архітектура показала зниження ризику й хвостових втрат CVaR@0.9, високу частоту проходження SafetyGate і суттєве зменшення когнітивного навантаження на оператора. Отримані результати демонструють, що запропонований підхід є стійким і ефективним навіть за умов підвищеної невизначеності й протидії, й формують науково-технічне підґрунтя для переходу від концептуального рівня до експериментально-випробувальної стадії в реальних miltech-системах.

Наукова новизна роботи полягає у формалізації теореми монотонності довіри в системах ЛМІ з ЦД та в інтеграції кібернетичного контуру прогнозування, що забезпечує адаптивне балансування між автоматизованими рішеннями й участю оператора. Запропоновано методику обчислення довіри на основі ентропії прогнозу та матриці зв’язності, що доповнює існуючі підходи в теорії керування людина – машина. Практичне значення полягає у створенні архітектури, яка здатна підвищити надійність і безпеку застосування бойових роботизованих систем, оптимізувати розподіл функцій між людиною та автоматикою й забезпечити інструменти для випробувань у симуляційних середовищах.

Попри досягнуті результати, дослідження має низку обмежень. По-перше, симуляційні експерименти відбувалися в умовах моделей, що спрощують реальну динаміку бойових операцій, тому необхідні випробування у більш реалістичних і гібридних середовищах.

По-друге, зростання обчислювальної складності прогнозного контуру може обмежувати застосування у сценаріях із критичною затримкою. По-третє, залишаються відкритими питання кіберзахисту архітектури, а також адаптації моделей ЦД до неповних або спотворених даних.

Перспективи розвитку запропонованої архітектури пов’язані з кількома взаємодоповнювальними напрямами. Передусім, актуальним є розширення моделі на мультиагентні системи з координацією кількох роботизованих платформ, де взаємодія цифрових двійників різних рівнів ієрархії (оператор – група – рій) стане критичним фактором успіху. Другим напрямом є інтеграція архітектури з реальними сенсорними комплексами та комунікаційними мережами, що дозволить оцінити її стійкість до фізичних обмежень і кібератак у польових умовах. Третім вектором є впровадження адаптивних алгоритмів оптимізації в прогнозному контурі, зокрема застосування методів глибинного підкріплення й варіаційних підходів до моделювання невизначеності, що підвищить швидкість і точність прийняття рішень. Четвертим напрямом є створення гібридних симуляційно-реальних полігонів, де ЦД будуть поєднуватися з фізичними платформами, утворюючи основу для валідації та сертифікації архітектури.

Окрему увагу слід приділити розробці стандартів безпеки та протоколів довіри для систем із прогнозним контуром, що дозволить уніфікувати механізми прийняття рішень і знизити ризики неконтрольованої автоматизації. Додатково перспективним є застосування архітектури в некласичних середовищах (кіберпростір, космічні місії, підводні операції), де традиційні підходи до ЛМІ є обмеженими. Таким чином, подальші дослідження мають зосередитися не лише на оптимізації окремих компонентів, а й на створенні цілісної доктрини інтеграції людини й роботизованої системи в адаптивному, прогнозово-керованому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бернацький А. П., Коваленко О. О. Адаптивне керування бойовим середовищем на основі просторово – часової ентропії // Системи і технології зв’язку, інформатизації та кібербезпеки. 2025. № 7. С. 5–19. DOI: 10.58254/viti.7.2025.01.05.

2. Giberna M., Voos H., Tavares P., Nunes J. et al. On Digital Twins in Defence: Overview and Applications // arXiv. 2025. DOI: arXiv: 2508.05717v1.

3. Kwon P. O., Zientara G. P., Thota D. S. et al. Digital Twins for a Digital World: Data-Driven Training Optimizing the Ready Medical Force // Special Warfare Journal. 2025.

4. Bain W. Real-time digital twins with AI/ML: A new level of battlefield intelligence // Military embedded systems. 2025.

5. Zhou Y. Digital twins: fostering efficient network modernization // Military embedded systems. 2025.

6. Asad U., Khan M., Khalid A., Akbar W. Lughmani Human-Centric Digital Twins in Industry: A Comprehensive Review of Enabling Technologies and Implementation Strategies // MDPI. Vol. 6. 2023. № 23 (8). P. 3938. DOI: 10.3390/s23083938.

7. Mohammed A. M., Mohammad A. A., Ortiz J. A. et al. A Human Digital Twin Architecture for Knowledge-based Interactions and Context-Aware Conversations // Interservice Industry Training, Simulation, and Education Conference (I/ITSEC) / Paper No. 24366. 2025. DOI: 10.48550/arXiv.2504.03147.

8. 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.

9. Shapiro S. S., Wilk M. B. An analysis of variance test for normality (complete samples) // Biometrika. № 52 (3–4). Pp. 591–611. (1965). DOI: 10.1093/biomet/52.3-4.591.

10. Sture Holm. A Simple Sequentially Rejective Multiple Test Procedure // Scandinavian Journal of Statistics. 1979. Vol. 6, No. 2. Pp. 65–70.

DOI: 10.58254/viti.8.2025.02.24

УДК 004.8+004.49

д-р філософії Власенко О. В. ORCID: 0000-0001-6671-870X (ВІТІ ім. Героїв Крут)

ІНТЕГРАЦІЯ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ В АРХІТЕКТУРУ SIEM-СИСТЕМИ

В умовах ескалації гібридних кіберзагроз та інтенсифікації кібернетичного протиборства, проблематика забезпечення стійкості і захищеності об'єктів критичної інфраструктури набуває особливої актуальності та стратегічного значення. Найвищого ступеня критичності це питання досягає у військово-оборонній сфері, де будь-яка компрометація інформаційних активів або порушення штатного функціонування інформаційно-комунікаційних систем здатні спричинити незворотні деструктивні наслідки для обороноздатності держави.

У роботі досліджено обмеження традиційних SIEM-систем, що базуються на детермінованих правилах і демонструють низьку ефективність у детектуванні невідомих загроз, високий рівень хибних спрацьовувань та проблеми масштабування. Здійснено формалізацію класичної архітектури SIEM-системи для ідентифікації її функціональних компонентів. На основі цього аналізу запропоновано удосконалену концептуальну модель SIEM-системи нового покоління, посилену можливостями генеративного штучного інтелекту. Ключовими елементами запропонованої моделі є модуль проактивного моделювання загроз, який використовує генеративний штучний інтелект для генерації гіпотез про невідомі вектори атак, та модуль генеративної верифікації і пріоритетизації, що застосовує глибокий семантичний аналіз для автоматичного валідування та контекстуального збагачення кіберінцидентів.

Запропонована архітектура забезпечує концептуальний перехід від реактивного моніторингу до проактивного, семантично-орієнтованого аналізу, підвищуючи ефективність виявлення кіберінцидентів, знижуючи навантаження на аналітиків та прискорюючи час реагування на критичні кіберінциденти, що є надзвичайно важливим для захисту стратегічних об'єктів. Перспективи подальших досліджень включають практичну реалізацію та валідацію запропонованих модулів, а також розробку методоки оцінки їхньої обчислювальної ефективності та масштабованості.

Ключові слова: *кібербезпека, штучний інтелект, SIEM-система, кіберінцидент, кіберзахист, інформаційно-комунікаційна система.*

O. Vlasenko. Integration of generative artificial intelligence into the architecture of the SIEM system

In the context of escalating hybrid cyber threats and the intensification of cyber conflict, the problem of ensuring the resilience and security of critical infrastructure facilities acquires particular urgency and strategic importance. This issue reaches its highest degree of criticality in the military and defense sector, where any compromise of information assets or disruption of the standard functioning of information and communication systems can lead to irreversible destructive consequences for the state's defense capability.

This paper investigates the limitations of traditional SIEM systems, which are based on deterministic rules and demonstrate low efficiency in detecting unknown threats, a high rate of false positives, and scalability issues. A formalization of the classical SIEM architecture was carried out to identify its functional components. Based on this analysis, an improved conceptual model for a next-generation SIEM system is proposed, enhanced with the capabilities of Generative Artificial Intelligence (GenAI). The key elements of the proposed model are a proactive threat modeling module, which uses GenAI to generate hypotheses about unknown attack vectors, and a generative verification and prioritization module, which applies deep semantic analysis for the automated validation and contextual enrichment of cyber incidents.

The proposed architecture provides a conceptual shift from reactive monitoring to proactive, semantically-oriented analysis, significantly increasing threat detection effectiveness, reducing the workload on analysts, and accelerating response times to critical cyber incidents, which is extremely important for the protection of strategic assets. Future research directions include the practical implementation and validation of the proposed modules, as well as the development of methodologies for evaluating their computational efficiency and scalability.

Keywords: *cybersecurity, artificial intelligence, SIEM system, cyber incident, cyber defense, information and communication system.*

Актуальність та постановка завдання в загальному вигляді. Динамічний розвиток інформаційних технологій та їх глибока інтеграція в усі сфери життєдіяльності супроводжуються пропорційним зростанням кількості та рівня складності кібератак. Існуючі системи кіберзахисту, що здебільшого базуються на реактивних та сигнатурних методах, дедалі частіше виявляються неспроможними ефективно протидіяти адаптивним,

багатовекторним та раніше невідомим кібератакам. Це зумовлює необхідність у проведенні наукових досліджень, спрямованих на вдосконалення теоретико-методологічних засад кібербезпеки та розробку інноваційних методів і моделей захисту інформаційно-комунікаційних систем (ІКС).

Особливої важливості зазначена проблематика набуває у військовій сфері, що характеризується дедалі глибшою інтеграцією ІКС в усі ланки управління військами. Функціональне призначення таких систем полягає у забезпеченні процесів оперативного управління військами та озброєнням, веденні розвідки, підвищенні ситуаційної обізнаності та автоматизації циклів прийняття рішень. Зважаючи на те, що стабільне та захищене функціонування ІКС військового призначення безпосередньо корелює з ефективністю виконання бойових завдань та є критичним фактором забезпечення обороноздатності держави, завдання щодо їх надійного кіберзахисту стає одним із пріоритетних імперативів національної безпеки.

Для вирішення завдань комплексного захисту та забезпечення належного рівня кіберстійкості ІКС військового призначення створюються спеціалізовані організаційно-технічні структури — центри моніторингу та реагування на кіберінциденти (Security Operations Center, SOC). Такі центри виконують функції безперервного моніторингу стану безпеки підконтрольних інформаційних ресурсів, проактивного виявлення загроз, а також оперативного реагування на кіберінциденти. Організаційно-технологічним ядром, що забезпечує агрегацію, нормалізацію, кореляцію та інтелектуальний аналіз потоків подій безпеки з різноманітних джерел в рамках SOC, виступають системи класу Security Information and Event Management (SIEM-системи) [1].

SIEM-системи, виступаючи технологічним ядром SOC, дозволяють ефективно вирішувати задачі виявлення кіберінцидентів, що базуються на попередньо визначених правилах кореляції та відомих сигнатурах атак. Це значно підвищує рівень ситуаційної обізнаності та скорочує середній час реагування. Водночас, такий підхід, детермінований наявністю експертних знань для формування правил, демонструє іманентні обмеження при зіткненні з раніше невідомими загрозами, складними багатоетапними атаками та векторами, що використовують адаптивні тактики ухилення. Крім того, нездатність класичних систем до глибокого семантичного аналізу контексту подій призводить до генерації значного обсягу хибних спрацьовувань (False Positives), що перевантажує роботу аналітиків. Зазначені недоліки зумовлюють гостру науково-практичну потребу в удосконаленні аналітичних можливостей SIEM-систем шляхом їх інтеграції з проактивними модулями, здатними до когнітивної обробки даних та автономного навчання.

Сучасний етап розвитку інформаційних технологій характеризується прискореною еволюцією методологій штучного інтелекту (ШІ), що охоплюють широкий спектр: від класичного машинного навчання до складних глибоких нейронних мереж. Одним із найбільш динамічних елементів цього розвитку є генеративний ШІ, зокрема технології великих мовних моделей (LLM). Визначний потенціал генеративного ШІ у задачах аналізу, структурування та інтерпретації великомасштабних, неструктурованих масивів даних стимулює наукову спільноту до активного дослідження перспектив його інтеграції у прикладні галузі, серед яких одним із найактуальніших напрямків є посилення аналітичних функцій систем кібербезпеки.

Інтеграція модулів на основі генеративного ШІ в архітектуру SIEM-систем відкриває новий напрям розвитку інтелектуальних засобів кіберзахисту. Такий підхід дає змогу усунути традиційні обмеження SIEM-систем шляхом автоматичного формування нових правил кореляції, динамічного оновлення баз знань, зниження кількості хибних спрацьовувань та підвищення ефективності виявлення складних, багатовекторних атак. Використання генеративного ШІ у SIEM-системах може стати основою для формування самонавчальних систем кіберзахисту, здатних адаптуватися до змінного кіберсередовища й забезпечувати проактивне виявлення загроз у режимі реального часу.

Аналіз попередніх досліджень. Оскільки інтеграція генеративного ШІ в системи кіберзахисту є відносно новим напрямом, для визначення актуальних тенденцій та наукових підходів до його реалізації доцільним є проведення аналізу попередніх досліджень у цій галузі. Сучасна наукова спільнота демонструє підвищений інтерес до застосування генеративного ШІ у сфері кібербезпеки, зокрема в контексті автоматизації процесів виявлення кіберінцидентів, аналізу загроз та підвищення адаптивності захисних систем. Огляд основних публікацій дозволить виявити основні наукові підходи, існуючі моделі й інструменти, що базуються на генеративних методах, а також визначити наявні обмеження, які потребують подальшого вдосконалення в контексті інтеграції генеративного ШІ в архітектуру SIEM-систем.

У [2] наведено аналіз трансформаційного впливу генеративного ШІ, зокрема Великих Мовних Моделей (LLMs) та Генеративно-Змагальних Мереж (GANs), на сфери оцінки вразливостей та управління ризиками у кібербезпеці. Суть роботи полягає у розробці комплексної таксономії, яка класифікує подвійне використання генеративного ШІ (наступальне та оборонне) на усіх етапах життєвого циклу оцінки вразливостей та управління ризиками, включаючи виявлення вразливостей, моделювання загроз, оцінку ризиків та автоматизоване усунення.

Дослідження підкреслює, що генеративний ШІ здатний автоматизувати сортування логів, скорочувати час реагування та підвищувати точність виявлення складних кіберзагроз. На основі проведеного систематичного огляду зроблено висновки, що генеративний ШІ може допомогти у вирішенні багатьох традиційних проблем циклу оцінки вразливостей та управління ризиками. Однак, його повна інтеграція стримується ключовими викликами, серед яких вразливість самих моделей ШІ до кібератак (наприклад, data poisoning та prompt injection), проблеми зрозумілості (explainability) рішень у критично важливих доменах та необхідність забезпечення надійності (trustworthiness) згенерованого коду. Для подолання цих обмежень запропоновано пріоритетні напрямки майбутніх досліджень, що сфокусовані на розробці систем безперервного навчання, які адаптуються до загроз у реальному часі; еволюції процесу зрозумілості до інтерпретованих за задумом архітектур; створенні гібридних фреймворків "людина-ШІ" для нагляду та зворотного зв'язку, а також запровадженні стандартизованих рамок оцінювання ШІ-інструментів для підтвердження їхньої стійкості, надійності та відповідності етичним нормам.

У статті [3] автори досліджують ключову та трансформаційну роль генеративного ШІ у сучасній кібербезпеці, наголошуючи на його потенціалі посилити виявлення та реагування на кіберінциденти і удоскналити процеси прийняття рішень. Публікація ґрунтується на систематичному огляді літератури, переважна більшість якої опублікована у 2023 році, що підкреслює релевантність і сучасність даних, враховуючи новизну генеративного ШІ у дослідницькій арені.

Необхідність інтеграції генеративного ШІ обумовлена тим, що традиційні підходи часто поступаються темпам еволюції кіберзагроз та є реактивними, залишаючи організації вразливими до нових методів та моделей кібератак. Технології генеративного ШІ, використовуючи принципи глибокого навчання та нейронних мереж, позиціонується як проактивний елемент, що здатен автономно генерувати рішення та виявляти аномалії в мережевому трафіку, поведінці користувачів та системних логах у реальному часі.

Дослідження визначає конкретні технології застосування генеративного ШІ, що включають: підвищення ефективності аналізу кіберінцидентів та захисту від шкідливого програмного забезпечення шляхом вивчення патернів; посилення автентифікації через біометричні та поведінкові патерни користувачів; швидке та точне сканування програмних кодів для виявлення прихованих вразливостей; а також генерацію надійних паролів і симуляцію кібератак для виявлення слабких місць. Автори роблять висновки, що генеративний ШІ забезпечує постійне вдосконалення безпеки, оскільки інтелектуальні системи адаптуються до нових технік експлуатації та можуть пріоритезувати ризики під час

одночасних кібератак. Водночас, наголошується на значних обмеженнях, включно з неспроможністю ШІ імітувати людське мислення, його залежністю від великих та точних наборів даних і вразливістю самих систем на базі генеративного ШІ до зловмисного використання. Кінцевим висновком є те, що найбільш ефективна стратегія кібербезпеки полягає у об'єднанні традиційних методів із можливостями генеративного ШІ.

Комплексний систематичним оглядом публікацій, присвяченим дослідженню ролі Генеративного ШІ у підвищенні ефективності розвідки кіберзагроз (Cyber Threat Intelligence, CTI) висвітлено у публікації [4]. Дослідження використовує методологію PRISMA та охоплює 330 релевантних публікацій за період з 2018 по 2024 роки з метою надання наскрізного (end-to-end) огляду застосувань, типів моделей, викликів та обмежень генеративного ШІ у сфері CTI. Автори систематизують генеративний ШІ на дві основні категорії: Великі Мовні Моделі (LLMs) та Глибокі Генеративні Моделі (DGMs). У роботі детально проаналізовано інтеграцію генеративного ШІ з різнорідними джерелами CTI, такими як текстові дані, мережевий трафік, зразки шкідливого програмного забезпечення, дані Dark Web та платформи розвідки загроз. Публікація висвітлює ключові аспекти застосування генеративного ШІ, які охоплюють виявлення шкідливого ПЗ, аналіз мережевих аномалій, детекцію фішингу, атрибуцію суб'єктів загроз та захист від соціальної інженерії.

Зроблено висновок, що технології генеративного ШІ значно удосконалили сферу CTI, пропонуючи адаптивні та проактивні рішення, що перевершують традиційні методи та моделі. Водночас, у статті виділено критичні виклики, включно з вразливістю до змагальних атак, питаннями конфіденційності даних (зокрема, через deepfakes та prompt injection), необхідністю інтерпретованості та прозорості моделей, а також проблемою адаптації до загроз, що постійно еволюціонують.

Публікація [5] присвячена аналізу потенціалу, реальних застосувань та обмежень генеративного ШІ у сфері кібербезпеки. Публікація розглядає генеративний ШІ як ефективний інструмент для протидії зростаючій частоті, витонченості та впливу кібератак, дозволяючи системам перейти від традиційного захисного підходу (countermeasures once an attack has been made) до наступального (проактивного), здатного передбачати ймовірну тактику зловмисників. Генеративний ШІ надає можливість автоматизовано вирішувати загальні ситуації з загрозами, дозволяючи фахівцям концентруватися на більш критичних аспектах безпеки, що вимагають людського втручання. У статті систематизовано застосування генеративного ШІ, включно з генеруванням безпечного коду, скануванням уразливостей із фільтрацією помилкових спрацювань на основі контексту, симуляцією реалістичних атак (Red Team simulations), створенням динамічних приманок (Honeypots) та генерацією запитів для полювання на загрози (threat-hunting queries).

Серед комерційних рішень, що використовують GAI, аналізуються Microsoft Security Copilot, Google Cloud Security AI Workbench та SentinelOne Purple AI. Водночас, автори публікації підкреслюють, що застосування генеративного ШІ несе значні ризики, зокрема: схильність надавати невірні/неетичні результати, легкість експлуатації зловмисниками, проблеми інтерпретованості та зрозумілості ("black box" nature), контекстуальні обмеження та відсутність стандартизованих метрик для емпіричної оцінки систем на базі генеративного ШІ. Зроблено висновок про необхідність розробки етичних настанов та надійних запобіжних заходів для запобігання зловмисному використанню генеративного ШІ.

Аналіз публікацій, присвячених інтеграції генеративного ШІ в процеси кіберзахисту, підтверджує високу актуальність та доцільність цього напрямку. Проте, переважна більшість робіт обмежується декларативним описом загальних перспектив та потенційних переваг, не пропонуючи конкретних прикладних рішень чи деталізованих моделей для впровадження. Зокрема, питання методологічних та архітектурних засад інтеграції генеративних компонентів із SIEM-системами для посилення їхніх аналітичних можливостей залишається практично нерозкритим. Ця недостатня дослідженість проблеми на практичному рівні формує чітку

наукову прогалину та підтверджує доцільність подальшої роботи над розробкою відповідних методів та моделей.

Метою статті є розробка удосконаленої моделі архітектури SIEM-системи з інтегрованими модулями на основі генеративного штучного інтелекту для підвищення ефективності виявлення кіберінцидентів в інформаційно-комунікаційних системах військового призначення.

Виклад основного матеріалу. SIEM-система виконує роль центральної аналітичної платформи у SOC, забезпечуючи консолідацію та інтелектуальну обробку потоків подій (event streams) з усього спектру контрольованих інформаційних ресурсів (мережеве обладнання, сервери, кінцеві точки, засоби захисту). Її фундаментальна цінність полягає у трансформації величезних масивів "сирих" даних, які самі по собі мають низьку інформативність, у верифіковані, пріоритезовані та збагачені контекстом кіберінциденти, що є прямими директивами для реагування аналітиками. Таким чином, SIEM-система реалізує повний цикл операційного управління подіями безпеки – від первинного збору до генерації сповіщення. Ключові функціональні модулі та процеси, що забезпечують цей цикл, деталізовано наведено в таблиці 1 [1; 6–8].

Таблиця 1

Декомпозиція функціональних компонентів SIEM-системи

Функціональний компонент	Деталізований опис призначення та механізмів
Збір та Агрегація даних	Прийом та консолідація потоків даних з гетерогенних джерел (кінцеві точки, сервери, мережеві пристрої, СЗІ). Використовуються різні протоколи (Syslog, SNMP, NetFlow) та механізми (агенти, API-інтеграція)
Парсинг та Нормалізація	Перетворення логів з різноманітних, пропрієтарних форматів у єдину канонічну модель даних (Common Event Format). Цей етап є критично важливим, оскільки уможливлює подальший спільний аналіз та кореляцію подій з різних джерел
Кореляція подій	Основний аналітичний механізм класичних SIEM-систем. Виконує детермінований аналіз нормалізованих подій у реальному часі на основі попередньо заданої бази правил (correlation rules) для виявлення складних, розподілених у часі та просторі патернів атак
Збагачення даних	Процес автоматичного додавання додаткового контексту до подій або кіберінцидентів. Може включати дані геолокації, інформацію про користувача з Active Directory, репутаційні дані з Threat Intelligence каналів
Генерація сповіщень	Формування та пріоритезація сповіщення для аналітика SOC при спрацюванні кореляційного правила. Ефективність цього модуля визначається співвідношенням True Positives до False Positives
Довготривале зберігання та Індексація	Забезпечення захищеного та відмовостійкого довготривалого зберігання (часто з використанням WORM-технологій) як "сирих", так і нормалізованих даних для потреб ретроспективного аналізу (Threat Hunting), розслідувань (Forensics) та аудиту відповідності (Compliance)
Візуалізація та Звітність	Надання інструментів для оперативного моніторингу та формування аналітичної і статистичної звітності (reports) для технічних спеціалістів та керівництва, а також для підтвердження відповідності регуляторним вимогам

На основі ґрунтовного аналізу провідних наукових публікацій [8–11], присвячених архітектурі та функціонуванню SIEM-систем, було визначено ключові функціональних компонентів: збір та агрегація, парсинг та нормалізація, кореляція подій, збагачення даних, генерація сповіщень, довготривале зберігання та візуалізація/звітність.

Для формалізації взаємозв'язків між цими компонентами та опису системи на концептуальному рівні, запропоновано впорядковану модель (1):

$$S = \langle C_{coll}, P_{norm}, E_{corr}, D_{enrich}, A_{alert}, S_{store}, V_{report} \rangle, \quad (1)$$

де кожен елемент є підсистемою (або множиною функцій), що виконує специфічне завдання:

C_{coll} (*Збір та Агрегація*) – це вхідна функція системи. Вона приймає множину потоків сирих даних (D_{raw}) з множини джерел (I) і передає їх на наступний етап (2):

$$C_{coll} : I \rightarrow D_{raw}; \tag{2}$$

P_{norm} (*Парсинг та Нормалізація*) – функція, що перетворює хаотичні сирі дані (D_{raw}) у структурований, єдиний формат (таксономію) системи (D_{norm}), дозволяє нормалізувати дані (3):

$$P_{norm} : D_{raw} \rightarrow D_{norm}\ ; \tag{3}$$

E_{corr} (*Кореляція подій*) – це множина правил та алгоритмів (R), які застосовуються до потоку нормалізованих подій (D_{norm}) для виявлення значущих патернів загроз (4)

$$(P_{threat}).E_{corr} : D_{norm} \times R \rightarrow P_{threat}; \tag{4}$$

D_{enrich} (*Збагачення даних*) – функція, що додає контекст (C_{tx}) до виявлених патернів або подій. Вона використовує зовнішні та внутрішні (списки активів, дані користувачів) джерела (5):

$$D_{enrich} : (P_{threat} \cup D_{norm}) \times C_{tx} \rightarrow P_{enriched}); \tag{5}$$

A_{alert} (*Генерація сповіщень*) – підсистема, що приймає збагачені патерни загроз $P_{enriced}$ і перетворює їх на конкретні, пріоритезовані кіберінциденти (алерти, A) для аналітиків (6):

$$A_{alert} : P_{enriched} \rightarrow A; \tag{6}$$

S_{store} (*Зберігання та Індексація*) – Підсистема, що відповідає за довготривале, захищене від втручання зберігання всіх даних (як D_{raw}, так і D_{norm}, і A) та їх ефективну індексацію для швидкого пошуку.

V_{report} (*Візуалізація та Звітність*) – інтерфейс представлення інформації. Це компонент, який надає інструменти (дашборди, звіти, інструменти пошуку) для взаємодії аналітика з кіберінцидентами (A) та збереженими даними (S_{store}).

Модель репрезентує архітектуру SIEM-системи як логічно послідовний механізм обробки даних про події безпеки, де кожен елемент є функціональною підсистемою, що перетворює дані, забезпечуючи перехід від логів до пріоритезованих кіберінцидентів та аналітичних звітів.

Таблиця 2

Аналіз іманентних обмежень класичних SIEM-систем

Категорія обмеження	Сутність проблеми	Негативний наслідок для SOC
Детермінована логіка аналізу	Ефективність виявлення інцидентів прямо детермінована повнотою та актуальністю бази кореляційних правил, що задаються експертами	"Сліпота" до невідомих загроз. Низька або нульова ефективність проти атак Zero-Day, нетипових векторів та складних багатоетапних загроз (APT), які не мають відомих сигнатур
Високий рівень хибних спрацьовувань	Відсутність глибокого семантичного аналізу та розуміння контексту призводить до генерації значної кількості сповіщень	Перевантаження аналітиків. Розсіювання уваги, збільшення часу на "ручну" верифікацію та тріаж, що критично підвищує

Категорія обмеження	Сутність проблеми	Негативний наслідок для SOC
	(алертів), що не є реальними інцидентами (False Positives)	середній час реагування (MTTR) на справжні загрози
Реактивний характер	Системи переважно реагують на події, що вже відбулися та відповідають заданим правилам, замість проактивного виявлення підготовки до атаки чи аномальної активності	Втрата критичного часу; виявлення інциденту вже після настання деструктивних наслідків або компрометації системи
Проблема масштабування аналізу	Експоненційне зростання обсягів даних (Big Data) у сучасних ІКС призводить до того, що аналіз на основі правил стає обчислювально складним та нездатним охопити всі нелінійні залежності	Пропуск складних інцидентів. Нездатність виявити слабкі, приховані сигнали (weak signals) або складні, розподілені атаки, що "губляться" у загальному шумі даних

Після деталізації функціональних компонентів SIEM-систем стає можливим проведення їх критичного аналізу в контексті протидії сучасним багатовекторним та адаптивним кіберзагрозам. Попри свою фундаментальну роль у SOC, традиційні SIEM-системи мають низку іманентних архітектурних та методологічних обмежень, які представлено у таблиці 2.

Аналіз актуальних викликів, притаманних традиційним архітектурам SIEM-систем, що охоплює детерміновану логіку аналізу, високий рівень хибних спрацьовувань (False Positives) та проблеми масштабування при роботі з великими даними, чітко вказує на потребу в парадигмальних змінах. Існуючі підходи, засновані на статичних кореляційних правилах , а також у лінійному аналізі, демонструють "сліпоту" до невідомих загроз, атак класу Zero-Day та комплексних багатоетапних загроз (APT), які не мають відомих сигнатур.

Крім того, відсутність глибокого семантичного розуміння контексту подій призводить до перевантаження аналітиків SOC нерелевантними оповіщеннями, істотно збільшуючи середній час реагування. З огляду на ці обмеження, запропоновано інтеграцію модулів, що використовують можливості генеративного ШІ, для трансформації ключових функціональних компонентів SIEM-системи [4; 5].

Зокрема, для подолання детермінованості та реактивності розроблено *модуль проактивного моделювання загроз*, який інтегрується у компонент кореляції подій (E_{corr}), перетворюючи його на гібридний кореляційний механізм (E^{*}_{corr}).

Модуль проактивного моделювання загроз являє собою компонент, що застосовує генеративні моделі для емуляції когнітивних процесів та тактик потенційного зловмисника (adversarial thinking). На відміну від традиційних систем, що оперують на основі спрацювання статичних правил, даний модуль виконує наступні функції:

генерація гіпотетичних векторів атак. Модуль здійснює синтез та валідацію гіпотез щодо можливих векторів компрометації. Цей процес базується на аналізі "слабких сигналів" (weak signals) – даних низької інтенсивності або непрямих індикаторів, які зазвичай фільтруються або ігноруються стандартними системами моніторингу;

симуляційне моделювання загроз. Компонент виконує симуляції за сценаріями (scenario-based simulation) для моделювання невідомих та раніше не ідентифікованих загроз, включно з атаками нульового дня. Це дозволяє створювати синтетичні набори даних, що репрезентують патерни новітніх загроз, які ще не внесені до баз сигнатур;

метод детекції аномалій. Виявлення аномальної активності відбувається не на основі порівняння з встановленою базовою лінією "нормальної" поведінки (як у системах UEBA), а шляхом кореляції спостережуваних подій зі згенерованими модулем проактивними патернами атак.

Застосування *модуля проактвиного моделювання загроз* спрямоване на подолання двох ключових обмежень існуючих підходів до моніторингу безпеки:

подолання детермінованої логіки аналізу. Модуль долає обмеження систем, заснованих на правилах (rule-based systems), які демонструють низьку ефективність при зіткненні з невідомими загрозами. Він забезпечує перехід від статичного детермінізму до динамічної генерації гіпотез, що є критично важливим для ідентифікації та протидії складним багатоетапним атакам та експлойтам нульового дня;

трансформація реактивного підходу. Компонент змінює парадигму кібербезпеки, переводячи її з режиму реактивного реагування на вже доконані кіберінциденти (reactive incident response) до проактивного прогнозування, моделювання та превентивного виявлення загроз (proactive threat modeling and forecasting).

Також для мінімізації хибних спрацьовувань та оптимізації процесу аналізу великих обсягів даних введено новий компонент – *модуль генеративної верифікації та пріоритетизації* (M_{gvp}). Цей модуль, розташований після збагачення даних (D_{enrich}) та перед генерацією сповіщень (A_{alert}), використовує генеративний ШІ для глибокого семантичного аналізу, автоматичної верифікації кіберінцидентів та створення контекстуально збагачених резюме, тим самим знижуючи навантаження на аналітиків та прискорюючи реагування.

Модуль генеративної верифікації та пріоритетизації функціонує як автоматизований аналітичний компонент, що еквівалентний функціям аналітика SOC першого рівня (Tier 1 Analyst), реалізований на базі генеративного ШІ. Усі потенційні кіберінциденти, згенеровані гібридним кореляційним механізмом (E^*_{corr}), першочергово надходять до цього модуля для автоматизованої обробки.

Основні функції *модуля генеративної верифікації та пріоритетизації*:

Семантичний аналіз подій. Модуль виконує поглиблений семантичний розбір сутностей та контексту подій безпеки, переходячи від простого зіставлення полів (field matching) до розуміння логіки та намірів, що стоять за послідовністю дій.

Автоматизована верифікація. Модуль миттєво ініціює процес розслідування (automated investigation) для кожного згенерованого звіту про кіберінцидент. Це включає автоматичний збір додаткових релевантних даних із сховища (S_{store}), збагачення подій контекстуальною інформацією та винесення вердикту щодо класифікації кіберінциденту.

Генерація природномовного резюме. Замість надання аналітику необробленого списку логів, модуль синтезує стислий, когнітивно засвоювальний опис кіберінциденту природною мовою. Це резюме містить пояснення виявленої небезпеки, її потенційного впливу та перелік вже виконаних кроків верифікації.

Виявлення прихованих зв'язків. Модуль здатен ідентифікувати латентні кореляції та недосконалі сигнали, розподілені у великих масивах даних, які не були виявлені на початковому етапі кореляції через їхню низьку амплітуду або неявний характер.

Впровадження *модуля генеративної верифікації та пріоритетизації* безпосередньо вирішує наступні критичні проблеми:

Мітигація високого рівня хибних спрацьовувань. Модуль виконує превентивну фільтрацію та відсіювання некоректних повідомлень до їх ескалації на рівень людського аналізу. Це призводить до значного зниження когнітивного навантаження на персонал SOC та скорочення середнього часу реагування (Mean Time to Respond).

Розв'язання проблеми масштабування аналізу. Забезпечує здатність до осмислення (comprehension) та аналізу великої кількості необроблених подій у режимі реального часу. Це дозволяє виявляти складні, приховані патерни атак, які в традиційних системах "губляться у шумі" (lost in the noise) через обмежені можливості обробки та кореляції даних.

На підставі проведеного аналізу фундаментальних обмежень, притаманних традиційним SIEM-системам, зокрема їхньої детермінованої логіки, реактивного характеру та нездатності ефективно обробляти великі обсяги даних, у даній роботі запропоновано удосконалену архітектурну модель SIEM-системи (7):

$$S_{GenAI} = \langle C_{coll}, P_{norm}, \boldsymbol{E^*_{corr}}, D_{enrich}, \boldsymbol{M_{gvp}}, A_{alert}, S_{store}, V_{report} \rangle, \quad (7)$$

де E^*_{corr} (*Гібридний кореляційний механізм*) – це розширення E_{corr}. $E^*_{corr} = E_{corr} \cup M_{pmv}$, включення *модулю проактивного моделювання загроз.*

M_{gvp} (*Модуль генеративної верифікації та пріоретизації*) – це новий, вбудований компонент, що виконує функції семантичного аналізу, верифікації та пріоритетизація перед тим, як кіберінцидент потрапить до A_{alert}.

Удосконалена модель S_{GenAI} інтегрує спеціалізовані модулі на базі генеративного штучного інтелекту. Впровадження модуля проакативного моделювання загроз, інтегрованого у гібридний кореляційний механізм, та модуля генеративної верифікації і пріоритетизації як нового компоненту архітектури, безпосередньо спрямоване на подолання вищезазначених недоліків.

Таким чином, запропонована модель забезпечує удосконалений механізм від пасивного моніторингу до проактивного, семантично-обґрунтованого аналізу загроз, що є критично важливим для виявлення невідомих кібератак та зниження навантаження на аналітиків SOC.

Висновки. У статті було формалізовано архітектуру традиційної SIEM-системи, що дозволило чітко ідентифікувати її фундаментальні обмеження, такі як детермінованість аналізу, реактивний характер та високий рівень хибних спрацьовувань.

Для подолання цих недоліків, що є критичними в умовах сучасних кіберзагроз, було розроблено та запропоновано удосконалену модель архітектури. Ключовою інновацією запропонованої архітектури є інтеграція двох спеціалізованих модулів на базі генеративного штучного інтелекту: Модуля проактивного моделювання загроз, що трансформує компонент кореляції у гібридний прогностичний механізм, та модуля генеративної верифікації та пріоритетизації, який впроваджує семантичний аналіз для автоматичної верифікації кіберінцидентів.

Таким чином, розроблена модель забезпечує парадигмальний перехід від реактивного моніторингу до проактивного, контекстуально-обґрунтованого аналізу загроз, що підвищує ефективність виявлення кіберіцидентів та знижує навантаження на аналітиків SOC.

Ключовим напрямом подальших досліджень є практична реалізація запропонованих модулів на базі генеративного ШІ. Це завдання передбачає проведення поглибленого дослідження з метою вибору та адаптації найбільш ефективних архітектур генеративних моделей для вирішення специфічних завдань проактивного моделювання загроз та семантичної верифікації кіберінцидентів у режимі реального часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Miloslavskaya N. Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers. *Advances in Intelligent Systems and Computing*. P. 282–288. URL: https://doi.org/10.1007/978-3-319-63940-6_40.

2. Seyedeh Leili Mirtaheri, Narges Movahed, Reza Shahbazian, Valerio Pascucci, Andrea Pugliese. Cybersecurity in the age of generative AI: A systematic taxonomy of AI-powered vulnerability assessment and risk management. *Future Generation Computer Systems*. 2025. Vol. 175. URL: https://doi.org/10.1016/j.future.2025.108107.

3. Curran K., Curran E., Killen J., Duffy C. The role of generative AI in cyber security. *Metaverse*. 2024. No. 5 (2): 2796. URL: https://doi.org/10.54517/m2796.

4. Balasubramanian P., Liyana S., Sankaran H. et al. Generative AI for cyber threat intelligence: applications, challenges, and analysis of real-world case studies. *Artif Intell Rev 58*. 2025. URL: https://doi.org/10.1007/s10462-025-11338-z.

5. Sai S., Yashvardhan U., Chamola V., Sikdar B. Generative AI for cyber security: analyzing the potential of ChatGPT, DALL-E and other models for enhancing the security space. *IEEE Access PP (99)*. 2024. P. 53499–53516. URL: https://doi.org/10.1109/ACCESS.2024.3385107.

6. T. Laue, C. Kleiner, K.-O. Detken and T. Klecker. A SIEM Architecture for Multidimensional Anomaly Detection. 2021. 1*1th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland*. 2021. Pp. 136–142. URL: https://doi.org/10.1109/IDAACS53288.2021.9660903.

7. Sheeraz M., Paracha M. A., Haque M. U., Durad M. H., Mohsin S. M., Band S. S., Mosavi A. Effective security monitoring using efficient SIEM architecture. *Hum.-Centric Comput. Inf. Sci*, 13, P. 1–18. URL: https://doi.org/10.22967/HCIS.2023.13.02.

8. González-Granadillo, Gustavo, Susana González-Zarzosa, and Rodrigo Diaz. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors 2021*. No. 14: 4759. URL: https://doi.org/10.3390/s21144759.

9. І. Субач, В. Кубрак, А. Микитюк. Архітектура та функціональна модель перспективної проактивної інтелектуальної системи SIEM-системи для кіберзахисту об’єктів критичної інфраструктури. *Information Technology and Security*. 2019. № 7 (2). Pp. 208–215. URL: https://doi.org/10.20535/2411-1031.2019.7.2.190570.

10. Субач І., Власенко О. Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-телекомунікаційних системах військового призначення. *Збірник наукових праць ВІТІ.* 2023. № 4. С. 82–92. URL: https://doi.org/10.58254/viti.4.2023.07.82.

11. SIEM Architecture Explained: Components, Design & Best Practices. *PuppyGraph Cybersecurity*. URL: https://www.puppygraph.com/blog/siem-architecture.

DOI: 10.58254/viti.8.2025.03.34

УДК 621.391

канд. техн. наук, доцент Гурський Т. Г. ORCID: 0000-0001-7646-853X (НДІ ВР)
канд. техн. наук, доцент Панченко І. В. ORCID: 0000-0001-5690-3813 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Восколович О. І. ORCID: 0000-0002-6353-868X (ВІТІ ім. Героїв Крут)
Салій О. С. ORCID: 0009-0002-7021-5288 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Котенко В. М. ORCID: 0009-0003-4177-6841 (ЖВІ ім. С. П. Корольова)

ОЦІНКА ЕФЕКТИВНОСТІ РАДІОЕЛЕКТРОННОГО ПОДАВЛЕННЯ КАНАЛІВ УПРАВЛІННЯ БПЛА ТИПУ FPV

У ході широкомасштабної агресії проти України збройні сили російської федерації широко застосовують мультироторні БпЛА типу FPV у якості "дронів-камікадзе".

Одним з найбільш ефективних способів захисту особового складу Сил оборони України, озброєння та військової техніки в таких умовах є застосування малопотужних засобів РЕБ, завданням яких є унеможливлення роботи каналу управління ворожим БпЛА. Одним із основних показників ефективності таких засобів є відстань, на якій забезпечується подавлення каналу управління ворожим БпЛА.

Тому, метою статті є розроблення математичної моделі для розрахунку відстані гарантованого подавлення каналів дистанційного управління безпілотними літальними апаратами засобами радіоелектронної боротьби.

У статті розроблено відповідну математичну модель, яка враховує топологію розташування засобу РЕБ, ворожого БпЛА та його наземної станції управління, їх енергетичні параметри, ширину смуги завади, параметри корисного сигналу та інші параметри. Для полегшення розрахунків, з урахуванням прийнятих обмежень і припущень (зокрема – втрати сигналу при розповсюдженні у середовищі відповідають втратам у вільному просторі), отримана спрощена математична модель. У якості прикладу наведені розрахунки очікуваної відстані гарантованого подавлення каналів управління, реалізованих на базі протоколів ELRS та Crossfire в діапазоні частот 900 МГц, при застосуванні загороджувальної завади з шириною спектру 25 МГц при значеннях потужності передавача засобу РЕБ 10, 50 та 100 Вт, для відстані між наземною станцією управління та засобом постановки завад 5 та 10 км, для висот польоту ворожого безпілотного літального апарату від 50 до 1000 м.

Розроблена модель може використовуватися при плануванні та організації захисту від ворожих БпЛА типу FPV, які виконують польотну місію "дрона-камікадзе".

Ключові слова: *рівняння радіолінії, втрати у вільному просторі, радіоелектронне подавлення, наземна станція управління, безпілотний літальний апарат, відношення сигнал/завада, відстань гарантованого подавлення.*

T. Hurskyi, I. Panchenko, O. Voskolovych, O. Saliy, I. Kotenko. Evaluation of the efficiency of radio electronic suppression of FPV UAV control channels

During the large-scale aggression against Ukraine, the armed forces of the russian federation widely use multi-rotor UAV of the FPV type as "kamikaze drones."

One of the most effective ways to protect the personnel of the Ukrainnian Defence Forces, weapons and military equipment in such conditions is the use of low-power electronic warfare (EW) means, the task of which is to disable the operation of the enemy UAV control channel. One of the main indicators of the effectiveness of such means is the distance at which the suppression of the enemy UAV control channel is ensured.

Therefore, the purpose of the article is to develop a mathematical model for calculating the distance of guaranteed suppression of remote control channels of unmanned aerial vehicles by electronic warfare means.

The article develops a corresponding mathematical model that takes into account the topology of the location of the electronic warfare system, the enemy UAV and its ground control station, their energy parameters, the width of the interference bandwidth, the parameters of the useful signal and other parameters. To facilitate calculations, taking into account the adopted restrictions and assumptions (in particular, signal losses during propagation in the environment correspond to losses in free space), a simplified mathematical model was obtained. As an example, calculations of the expected distance of guaranteed suppression of control channels implemented on the basis of the ELRS and Crossfire protocols in the 900 MHz frequency range are given, when using a blocking jammer with a spectrum width of 25 MHz at EW transmitter power values of 10, 50 and 100 W, for a distance between the ground control station and the jamming device of 5 and 10 km, for flight altitudes of the enemy unmanned aerial vehicle from 50 to 1000 m.

The developed model can be used in planning and organizing defense against enemy FPV UAVs that perform a "kamikaze drone" flight mission.

Keywords: *radio link equation, free space losses, radio electronic suppression, ground control station, unmanned aerial vehicle, signal/interference ratio, guaranteed suppression distance.*

Постановка проблеми

В останні десятиліття стрімко розвивається теорія і практика бойового застосування безпілотних літальних апаратів (БпЛА) [1]. Зокрема, у ході широкомасштабної агресії проти України противник широко застосовує мультироторні безпілотні літальні апарати (БпЛА) типу FPV (з англ. First Person View – в режимі "управління від першої особи") у якості "дронів-камікадзе" для ураження особового складу та техніки Сил оборони України [2]. Невелика вартість таких дронів робить їх застосування масовим.

Одним із ключових умов, які визначають ефективність виконання польотної місії таких БпЛА, є забезпечення надійного радіозв'язку з їх наземними станціями управління для передавання команд дистанційного управління та приймання сигналів телеметрії. Тому, найбільш ефективним засобом протидії ворожим БпЛА є радіоелектронне подавлення сигналу управління на входах їх приймачів, які передаються відповідними ворожими наземними станціями управління (НСУ). При цьому, завдання виявлення сигналів дистанційного управління БпЛА вирішується засобами радіоелектронної розвідки, які можуть застосовуватись як окремо, так і бути інтегрованими у засоби (комплекси) радіоелектронної боротьби (РЕБ).

За час широкомасштабної російсько-української війни в Україні вироблено велику кількість модифікацій засобів, призначених для захисту від FPV-дронів, які називають "окопними" або "купольними" засобами РЕБ [3; 4]. Як правило, такі засоби здатні одночасно створювати декілька загороджувальних завад у діапазонах частот від 300 МГц до 6000 МГц. Оцінка ефективності застосування таких засобів є важливим та актуальним завданням на етапі планування радіоелектронного захисту підрозділів Сил оборони України. Одним з основних параметрів, який визначає ефективність застосування засобів РЕБ, є відстань ефективного (гарантованого) подавлення, на якій створюється таке відношення сигнал/завада на вході приймача каналу управління БпЛА, при якому приймання цифрового сигналу із заданою достовірністю (ймовірністю бітової помилки) буде неможливе.

Аналіз останніх досліджень і публікацій

На сьогодні відомі декілька варіантів реалізації протоколу управління БпЛА типу FPV [5]. Аналіз характеристик та можливостей деяких засобів РЕБ, призначених для радіоелектронного подавлення каналів радіоліній дистанційного управління БпЛА типу FPV, наведено в [4]. Виробники цих засобів, як правило, надають орієнтовні дані щодо відстані гарантованого подавлення (ефективного радіусу дії), проте не наводять умов (енергетичні параметри НСУ, відстань від НСУ до засобу РЕБ тощо), яким вони відповідають. У роботах [6; 7] запропоновано підхід до оцінювання завадозахищеності повітряного ретранслятора радіомережі, на приймач якого впливає наземний постановник завад. На основі цього ж підходу можна вирішити і зворотну задачу – оцінити ефективність застосування засобу РЕБ (відстань гарантованого подавлення каналу управління ворожого БпЛА) в конкретних умовах.

Метою статті є розроблення математичної моделі для розрахунку відстані гарантованого подавлення каналів дистанційного управління ворожого БпЛА засобами радіоелектронної боротьби.

Виклад основного матеріалу дослідження

Для визначення відстані подавлення каналу управління ворожого БпЛА необхідно розрахувати відношення σ рівня сигналу НСУ до рівня завади, створюваної засобом РЕБ (постановником завад, ПЗ) на вході приймача ворожого БпЛА, для різних відстаней між БпЛА та ПЗ

$$\sigma\,(R_j) = P_{\text{с}} - P_{\text{з}}, \tag{1}$$

де $P_{\text{с}}$ – рівень сигнала НСУ на вході приймача БпЛА, дБ;

$P_{\text{з}}$ – рівень завади на вході приймача БпЛА, дБ;

R_j – відстань між ПЗ та БпЛА, м,
і визначити відстань, при якій це відношення стає меншим за допустиме для забезпечення можливості успішного приймання сигналу управління ворожим БпЛА.

Для визначення як $P_с$, так і $P_з$, необхідно розв'язати задачу з розрахунку рівня сигналу на вході приймача, згідно з концепцією втрат передачі для радіолінії при розповсюдженні радіохвиль [8]:

$$P_2 = P_1 + G_1 + G_2 - L_{ф1} - L_{ф2} - L_\Sigma - W_з, \tag{2}$$

де P_2 – рівень сигналу на вході приймача, дБмВт;
P_1 – рівень сигналу на виході передавача, дБмВт;
G_1, G_2 – коефіцієнти підсилення передавальної та приймальної антен, відповідно, дБі;
$L_{ф1}$, $L_{ф2}$ – втрати у антенно-фідерних трактах на передачі та прийомі, відповідно, дБ;
L_Σ – сумарні втрати сигналу при розповсюдженні радіохвиль, дБ,
$W_з$ – енергетичний запас, який враховують для забезпечення компенсації втрат сигналу на прийомі через низку несприятливих факторів, дБ (при проведенні розрахунків у системах радіозв'язку зазвичай приймається рівним 10–15 дБ).

Сумарні втрати визначаються згідно з виразом

$$L_\Sigma = L_0 + L_{сер}, \tag{3}$$

де L_0 – основні втрати радіолінії (втрати у вільному просторі);
$L_{сер}$ – втрати, які визначають вплив реального середовища на розповсюдження радіохвиль (так званий множник ослаблення).

Втрати у вільному просторі визначаються за формулою [8]

$$L_0 = 10\lg\left(\frac{4\pi R}{\lambda}\right)^2, \tag{4}$$

де R – відстань між передавачем та приймачем;
λ – довжина хвилі.

На підставі виразу (2) можуть здійснюватися розрахунки для будь-яких радіоліній. Відмінність полягає у методиці розрахунку сумарних втрат L_Σ.

Геометрична модель взаємного розташування ПЗ, ворожого БпЛА та його НСУ наведена на рисунку 1, де R_0 – відстань між НСУ та ПЗ, h – висота польоту БпЛА. Якщо з точки поточного розташування БпЛА опустити проекцію на Землю (у точку S), то відстань від НСУ до точки S позначимо R_i, тоді для відповідного положення БпЛА відстань між ним та ПЗ становитиме R_j, при цьому

$$R_i = R_0 - R_j. \tag{5}$$

Тоді у кожній точці траєкторії руху БпЛА у напрямку на ПЗ відстань від між ПЗ та БпЛА можна виразити, як

$$R_{ПЗ} = \sqrt{\left(R_j^2 + h^2\right)}, \tag{6}$$

а відстань від НСУ до БпЛА, з урахуванням (5)

$$R_{\text{НСУ}} = \sqrt{\left(R_i^2 + h^2\right)} = \sqrt{\left(\left(R_0 - R_j\right)^2 + h^2\right)}. \tag{7}$$

З рисунка 1 видно, що відстань гарантованого подавлення може бути задана як абсолютна відстань від ПЗ до БпЛА $R_{\text{ПЗ}}$, так і відносна відстань – R_j, при яких забезпечується необхідне відношення сигнал/завада на вході приймача каналу управління БпЛА (при цьому для усунення неоднозначності у обох випадках необхідно зазначати, якій висоті польоту БпЛА відповідає це значення).

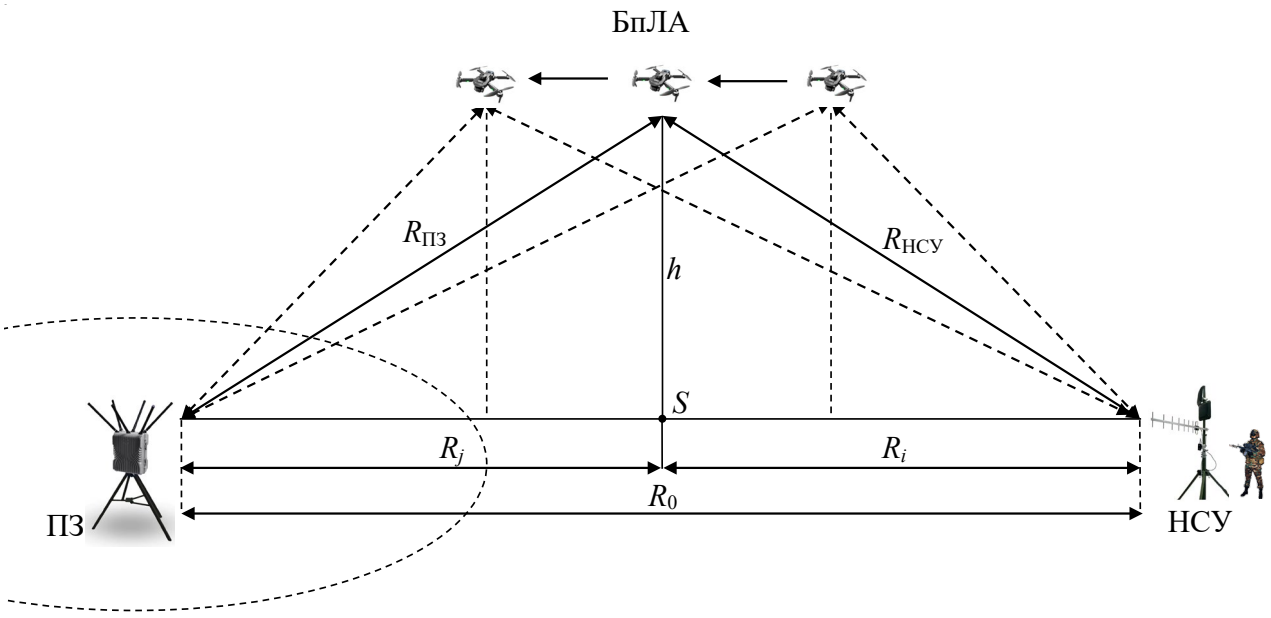


Рис. 1. Геометрична модель взаємного розташування НСУ, ПЗ та БпЛА під час його польоту

Основні параметри сигналів деяких найбільш поширених протоколів управління FPV-дронами, необхідні для проведення розрахунків, наведено в таблиці 1.

Таблиця 1

Параметри сигналів деяких протоколів управління FPV-дронами

Протокол / модуляція	Розширення спектра	Смуга частот, МГц	Миттєва ширина спектра сигналу, кГц
Express LRS / ЛЧМ	ППРЧ	902–927	500
Crossfire / ЛЧМ	ППРЧ	868–893	250
ЧМ-2	ППРЧ	902–927	90

Наведені протоколи використовують псевдовипадкове перестроювання робочої частоти (ППРЧ). Тому, спектральна щільність потужності завади, яка перекриває смугу частот сигналу дистанційного управління БпЛА, буде дорівнювати [7]:

$$S_{\text{ПЗ}} = P_{\text{ПЗ}} / \Delta F_{\text{Ш}}, \tag{8}$$

де $S_{ПЗ}$ – спектральна щільність потужності завади, дБмВт/Гц; $P_{ПЗ}$ – потужність передавача станції завад, дБмВт; $\Delta F_{Ш}$ – смуга частот шумової завади, Гц.

У режимі ППРЧ на радіолінії дистанційного управління між НСУ та БпЛА в кожен момент часу використовується один з умовних елементарних каналів шириною $\Delta f_К$ з потужністю $P_{НСУ}$, що дорівнює вихідній потужності передавача НСУ. У смузі завади шириною $\Delta F_{ПЗ}$ міститься

$$N = \Delta F_{ПЗ} / \Delta f_К$$

умовних елементарних каналів. Потужність завади $P_{ПЗ0}$, що приходиться на один умовний елементарний канал на вході приймача БпЛА, дорівнює:

$$P_{ПЗ0} = S_{ПЗ} \cdot \Delta f_К = P_{ПЗ} / N. \quad (9)$$

Фактично, N дорівнює коефіцієнту розширення спектра сигналу, і чим воно більше, тим менше значення $P_{ПЗ0}$ і тим більший енергетичний виграш отримує радіолінія між БпЛА та НСУ (лінія дистанційного управління ворожим БпЛА) відносно постановника широкосмугової завади. Саме значення $P_{ПЗ0}$ необхідно підставляти у вираз (2) замість P_1 при розрахунку рівня завади $P_з$ на вході приймача.

Перепишемо вираз (1) з урахуванням (2), (8), (9) (при цьому для обох радіоліній (як НСУ – БпЛА, так і ПЗ – БпЛА) втрати у антенно-фідерних трактах приймемо рівними нулю, енергетичний запас – однаковим, коефіцієнт підсилення антени БпЛА – однаковим):

$$\varsigma(R_j) = P_{НСУ} + G_{НСУ} - L_{\Sigma_{НСУ}} - P_{ПЗ} \frac{\Delta f_К}{\Delta F_{ПЗ}} - G_{ПЗ} + L_{\Sigma_{ПЗ}}, \quad (10)$$

де $P_{НСУ}$ – потужність передавача НСУ, дБмВт;

$G_{НСУ}$ – коефіцієнт підсилення антени НСУ, дБі;

$L_{\Sigma_{НСУ}}$ – сумарні втрати радіосигналу при розповсюдженні радіохвиль на радіолінії НСУ – БпЛА, дБ;

$P_{ПЗ}$ – потужність передавача ПЗ, дБмВт;

$G_{ПЗ}$ – коефіцієнт підсилення антени ПЗ, дБі;

$L_{\Sigma_{ПЗ}}$ – сумарні втрати сигналу на радіолінії ПЗ – БпЛА.

Для спрощення розрахунків введемо такі обмеження припущення:

1) сумарні втрати на радіолініях ПЗ – БпЛА та НСУ – БпЛА дорівнюють втратам у вільному просторі $\left(L_{\Sigma_{НСУ}} = L_{0_{НСУ}};\ L_{\Sigma_{ПЗ}} = L_{0_{ПЗ}}\right)$;

2) БпЛА злітає вертикально вгору над НСУ, піднімається на висоту h і починає рух у напрямку постановника завад, не змінюючи при цьому висоту польоту;

3) відстань гарантованого подавлення будемо визначати, як відносну відстань R_j.

Тоді вираз (10) з урахуванням (3)–(7) можна переписати таким чином:

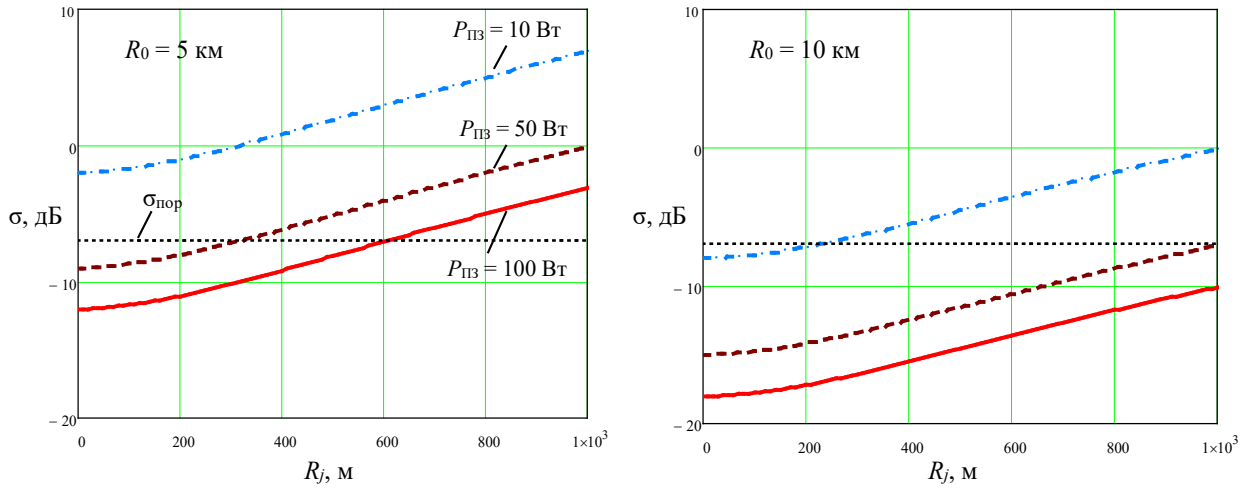
$$\varsigma(R_j) = P_{НСУ} + G_{НСУ} - P_{ПЗ} \frac{\Delta f_К}{\Delta F_{ПЗ}} - G_{ПЗ} + 10 \lg\left(\frac{R_j^2 + h^2}{\left(R_0 - R_j\right)^2 + h^2}\right), \quad (11)$$

де позначення R_0 та R_j відповідають рисунку 1.

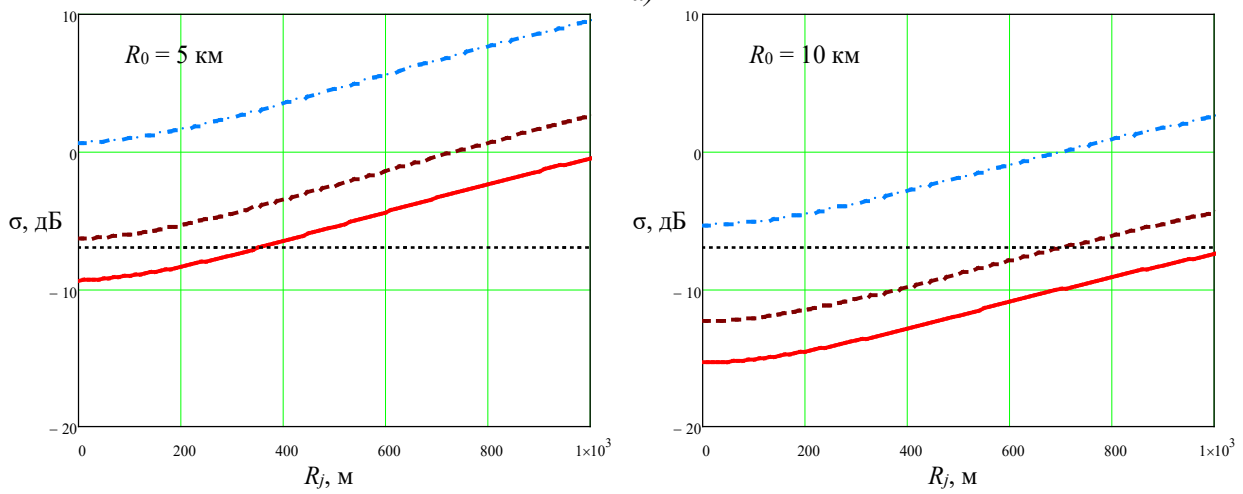
На рисунку 2 для прикладу наведені результати розрахунків залежності відношення сигнал/завада на вході приймача БпЛА від відстані між ПЗ та БпЛА для таких вихідних даних: h = 500 м; R_0 приймає значення 5 та 10 км; $P_{НСУ}$ = 2 Вт; $G_{НСУ}$ = 13 дБі (антена типу “хвильовий канал”); $P_{ПЗ}$ може приймати значення 10, 50 і 100 Вт; $G_{ПЗ}$ = 5 дБі (всеспрямована антена); протоколи, які використовуються для дистанційного управління БпЛА, відповідають таблиці 1; ПЗ використовує шумову загороджувальну заваду з шириною спектра $\Delta F_{ПЗ}$, яка дорівнює ширині смуги ППРЧ каналу управління БпЛА (25 МГц).

Для протоколу Crossfire успішний прийом сигналу можливий при забезпеченні відношення сигнал/шум (сигнал/завада) не нижче – 6 дБ [9]. Приймемо, що відношення сигнал/завада, яке необхідно забезпечити для гарантованого подавлення каналу управління, для протоколів з використанням лінійної частотної модуляції (ЛЧМ), становить $\varsigma_{пор} \leq -7$ дБ, а для протоколу, який використовує двійкову частотну маніпуляцію – $\varsigma_{пор} \leq 3$ дБ (для проведення розрахунків у реальних умовах, необхідно використовувати точні значення $\varsigma_{пор}$ для конкретного протоколу з відповідними значеннями параметрів сигналу, які використовуються).

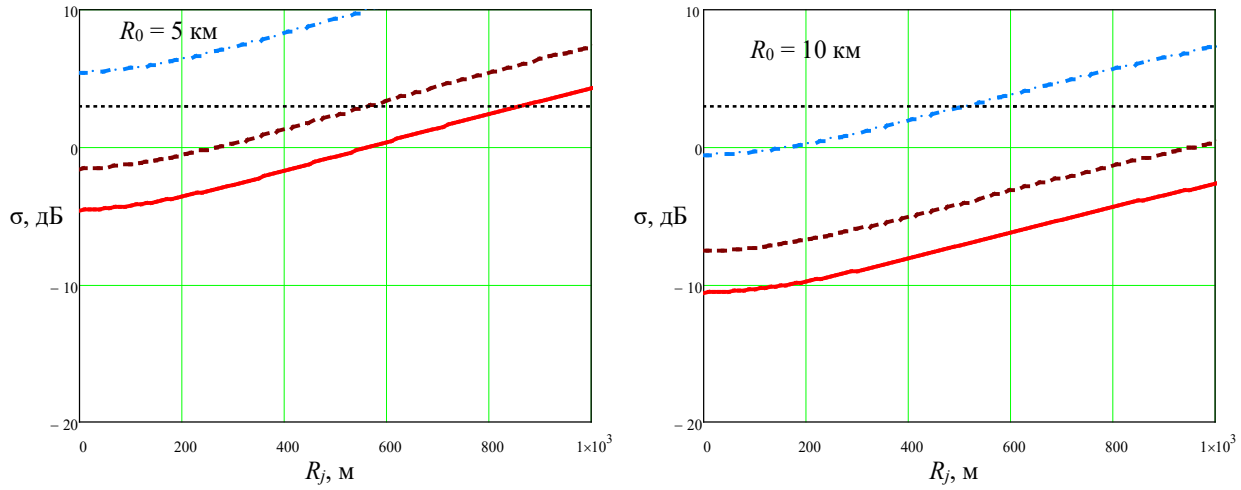
Криві, нанесені на рисунку 2 суцільною лінією, відповідають потужності передавача ПЗ, рівній 100 Вт (50 дБмВт), штрих-пунктирною – 50 Вт (47 дБмВт), пунктирною – 10 Вт (40 дБмВт). Штриховою прямою лінією на графіках позначений пороговий рівень відношення сигнал/завада $\varsigma_{пор}$, при забезпеченні якого лінія дистанційного управління (радіолінія між НСУ та БпЛА) вважається подавленою, а відповідне йому значення R_j є відстанню гарантованого подавлення.



а)



б)



в)

Рис. 2. Графіки залежності відношення сигнал/завада на вході приймача БпЛА від відстані між ПЗ та БпЛА R_j при h = 500 м:
а – протокол Express LRS; *б* – протокол Crossfire; *в* – протокол з використанням ЧМ-2

У таблиці 2 наведено результати розрахунків відстані гарантованого подавлення R_j для різних протоколів каналу управління БпЛА для тих самих вихідних даних, але для різних значень висоти польоту БпЛА.

Таблиця 2

Відстань гарантованого подавлення каналу управління FPV-дроном

h, м	$P_{ПЗ}$, Вт	Відстань гарантованого подавлення R_j, м					
		Протокол Express LRS		Протокол Crossfire		Протокол з ЧМ-2	
		R_0, км		R_0, км		R_0, км	
		5	10	5	10	5	10
50	10	260	530	190	390	340	690
	50	550	1110	420	840	720	1440
	100	750	1500	570	1150	960	1920
100	10	250	520	170	380	330	690
	50	550	1110	410	840	710	1440
	100	750	1500	570	1150	950	1920
200	10	180	490	40	340	290	670
	50	530	1100	370	820	690	1430
	100	730	1490	540	1140	940	1910
500	10	-	230	-	-	-	510
	50	310	1010	-	700	560	1370
	100	600	1440	350	1050	860	1870
1000	10	-	-	-	-	-	-
	50	-	630	-	-	-	1130
	100	-	1200	-	700	470	1720

На рисунку 3 наведено результати розрахунків залежності відношення сигнал/завада на вході приймача БпЛА від висоти його польоту h для наступних вихідних даних: відстань між ПЗ та БпЛА – 50, 100, 200, 500 і 1000 м; R_0 дорівнює 5 та 10 км; $P_{НСУ}$ = 2 Вт; $G_{НСУ}$ = 13 дБі; $P_{ПЗ}$ = 50 Вт; $G_{ПЗ}$ = 5 дБі; протокол, який використовується для дистанційного управління БпЛА – Express LRS; ПЗ використовує шумову загороджувальну заваду з шириною спектра $\Delta F_{ПЗ}$, яка дорівнює ширині смуги ППРЧ каналу управління БпЛА (25 МГц).

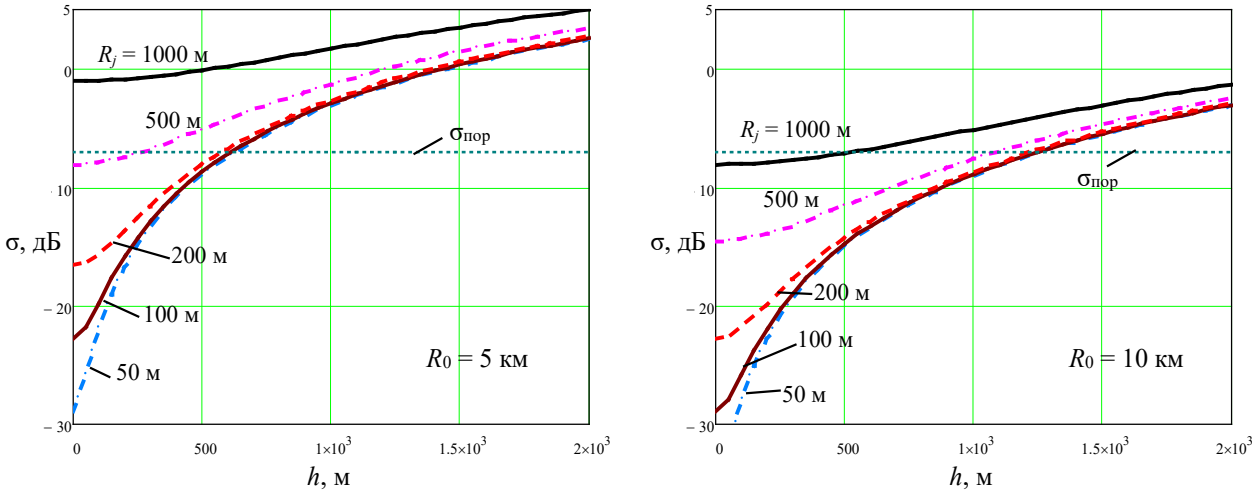


Рис. 3. Графіки залежності відношення сигнал/завада на вході приймача БпЛА від висоти його польоту h для різних відстаней R_j між ПЗ та БпЛА при $P_{ПЗ}$ = 50 Вт, протокол Express LRS

З графіків на рисунках 2, 3 та розрахункових даних у таблиці 2 можна зробити наступні висновки:

1) серед розглянутих протоколів найскладніше подавити канал управління БпЛА на базі протоколу Crossfire з ЛЧМ, найлегше – на базі протоколу з ЧМ-2;

2) відстань гарантованого подавлення зменшується:

при зменшенні відстані між ворожою НСУ та постановником завад;

при збільшенні висоти польоту ворожого БпЛА;

при збільшенні коефіцієнта розширення спектра сигналу радіолінії дистанційного управління ворожим БпЛА.

Підвищити ефективність радіоелектронного подавлення каналів дистанційного управління БпЛА можна за рахунок наступних заходів:

збільшення потужності передавача постановника завад, що призведе до збільшення ймовірності виявлення координат постановника завад засобами радіоелектронної розвідки противника;

використання антен з більшим коефіцієнтом підсилення (у випадку спрямованих антен типу "хвильовий канал" при одночасному застосуванні противником декількох БпЛА збільшиться ймовірність "пропуску цілей" з інших просторових напрямків);

використання більш ефективних типів завад, зокрема, завад у відповідь (ЗВ) [12] з шириною спектра, яка відповідає миттєвій ширині спектра сигналу. Це дасть змогу забезпечити вимоги до відстані ефективного подавлення при меншій потужності передавача.

Значно вища ефективність ЗВ, порівняно із загороджувальною, підтверджується графіками на рисунку 4, де наведені результати розрахунків залежності відношення сигнал/завада на вході приймача БпЛА від відстані між ПЗ та БпЛА для таких вихідних даних: h = 500 м; R_0 приймає значення 5 та 10 км; $P_{НСУ}$ = 2 Вт; $G_{НСУ}$ = 13 дБі; $P_{ПЗ}$ = 50 Вт; $G_{ПЗ}$ = 5 дБі; протокол, який використовується для дистанційного управління БпЛА – Express LRS; ПЗ №1 використовує шумову загороджувальну заваду з шириною спектра $\Delta F_{ПЗ}$, яка дорівнює ширині смуги ППРЧ каналу управління БпЛА (25 МГц); ПЗ № 2 – ЗВ з шириною спектра, рівною миттєвій ширині спектра сигналу (500 кГц), при цьому приймалося припущення, що затримкою, з якою ЗВ змінює частоту вслід за частотою сигналу лінії дистанційного управління БпЛА, можна знехтувати.

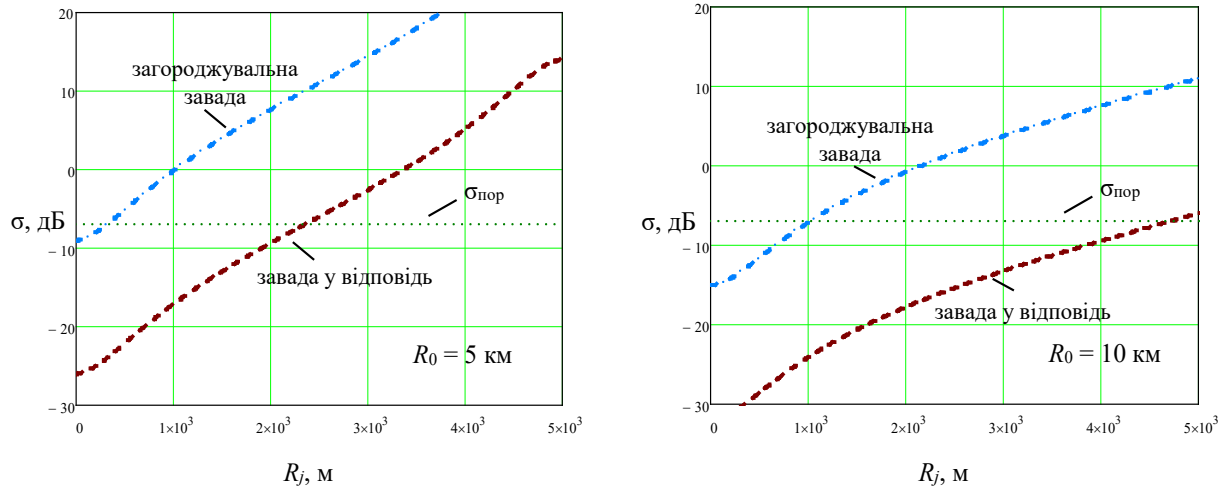


Рис. 4. Графіки залежності відношення сигнал/завада на вході приймача БпЛА від відстані між ПЗ та БпЛА R_j при h = 500 м, $P_{ПЗ}$ = 50 Вт, протокол Express LRS

Водночас, в умовах застосування завад у відповідь (ЗВ), при одночасному застосуванні противником декількох БпЛА з каналами дистанційного управління в одному діапазоні частот, завдання їх одночасного ефективного подавлення суттєво ускладнюється, а його вирішення буде залежати від технічних можливостей засобу РЕБ.

Для більш точного розрахунку втрат сигналу під час розповсюдженні радіохвиль при моделюванні радіоелектронного подавлення каналів телеметрії БпЛА, доцільно використовувати рекомендацію ITU-R P.528 [10], яку можна застосовувати в діапазоні частот 125–15500 МГц при зміні висот підвісу як передавальної, так і приймальної антен, від 1,5 м до 20000 м.

На офіційних сайтах ITU [10] та Інституту досліджень у галузі телекомунікацій (The Institute for Telecommunication Sciences (ITS)) [11], розміщені версії програмної реалізації рекомендації P.528, що дозволяють здійснювати розрахунки L_Σ для будь-яких допустимих вихідних даних.

На рисунку 5 показано результати розрахунку сумарних втрат сигналу з використанням програмного додатку [11] для таких вихідних даних: частота – 915 МГц, висота антени передавача (НСУ) – 2 м, висота антени приймача (БпЛА) – 50, 100, 200, 500, 1000 м. Для висот БпЛА від 200 м і більше, криві практично відповідають втратам у вільному просторі, для висоти 100 м реальні втрати стають дещо більшими починаючи з відстані 6 км, а для висоти 50 м – починаючи з відстані 3 км. Тому, значення відстані гарантованого подавлення для висот БпЛА 50 і 100 м будуть більшими, порівняно з наведеними у таблиці 2. При цьому, зі збільшенням частоти, різниця між кривими, отриманими за допомогою рекомендації P.528, та кривою, що відповідає втратам у вільному просторі, принаймні для відстаней до 10 км, зменшується. Тому, запропонована у статті спрощена модель цілком може бути застосована для орієнтовних розрахунків відстані гарантованого радіоелектронного подавлення каналу дистанційного управління БпЛА з дальністю польоту до 10 км (типу FPV) у типових діапазонах частот від 300 до 6000 МГц.

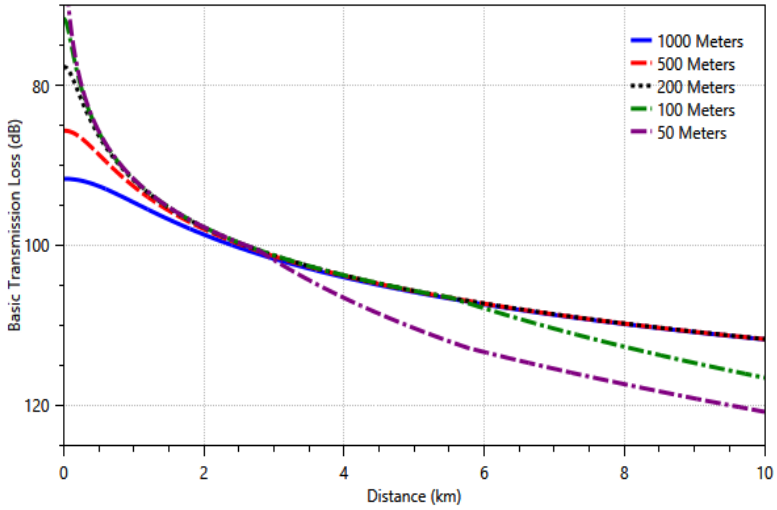


Рис. 5. Втрати сигналу на частоті 915 МГц, розраховані згідно з рекомендацією Р-528

Висновки і перспективи подальших досліджень

Таким чином, у статті розроблено математичну модель, призначену для оцінки ефективності радіоелектронного подавлення каналів управління БпЛА типу FPV. Запропонована модель дає змогу здійснювати розрахунки відношення сигнал/завада на вході приймача каналу управління БпЛА та визначати відстань ефективного (гарантованого) подавлення.

Із використанням спрощеної моделі, для якої втрати сигналу при розповсюдженні радіохвиль приймались рівними втратам у вільному просторі, проведено розрахунки відстані гарантованого подавлення для типових вихідних даних: канали дистанційного управління БпЛА реалізовані на базі протоколів ELRS та Crossfire в діапазоні частот 900 МГц; тип завади – загороджувальна, з шириною спектра 25 МГц; можливі значення потужності передавача засобу РЕБ – 10, 50 та 100 Вт; можливі значення відстані між наземною станцією управління та постановником завад – 5 та 10 км; можливі значення висоти польоту ворожого БпЛА – 50, 100, 200, 500 та 1000 м.

Запропонована математична модель може використовуватися на початковому етапі планування радіоелектронного захисту підрозділів Сил оборони України як від БпЛА типу FPV, так і від БпЛА інших типів, політ яких здійснюється з використанням радіоліній дистанційного управління. Крім того, вона може застосовуватися розробниками перспективних засобів РЕБ, призначених для подавлення каналів управління ворожих БпЛА, для вибору таких значень енергетичних параметрів, а також типів та параметрів завад, які забезпечуватимуть вимоги до ефективного радіуса дії (відстані гарантованого подавлення).

Напрямком подальших досліджень є програмна реалізація запропонованої моделі з використанням рекомендації ITU-R P.528.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основи теорії і практики використання безпілотних авіаційних комплексів ретрансляторів: навч. посіб. / Панченко І. В. та ін. Київ, 2021. 248 с.

2. Панченко І. В. Аналіз бойового застосування мультироторних безпілотних літальних апаратів в умовах роботи спеціального озброєння // Системи і технології зв'язку, інформатизації та кібербезпеки. 2022. № 2 (2). С. 42–47.

3. "Окопна РЕБ" проти БПЛА. URL: https://armyinform.com.ua/2023/07/15/okopna-reb-proty-bpla.

4. Порівняльна таблиця РЕБ комплексів для авто, позицій та піхоти. URL: https://lockey.com.ua/vergleich.

5. Протокол керування дроном: що це, які існують та для чого потрібні? URL: https://fx-drones.com/protokol-keruvannia-dronom/.

6. Аналіз завадозахищеності радіомереж з використанням повітряних ретрансляторів в умовах навмисних шумових завад / [Гурський Т. Г., Сова О. Я., Гриценок К. М., Гай Ю. І.] // Збірник наукових праць ВІТІ. 2018. № 4. С. 26–33.

7. Гурський Т. Г. Аналітична модель оцінки впливу засобів РЕБ на радіолінії з ППРЧ у радіомережах з повітряним та наземним ретрансляторами / Т. Г. Гурський // Збірник наукових праць ВІТІ. 2019. № 3. С. 23–32.

8. Recommendation ITU-R P.341-7 (2019). The concept of transmission loss for radio links. P Series. Radiowave propagation. Електронна публікація, Женева, 2017. ITU 2017. URL: http://www.itu.int/publ/R-REC/en).

9. TBS Crossfire R/C System. Manual. Revision 2022-08-08. URL: https://www.team-blacksheep.com/media/files/tbs-crossfire-manual.pdf?srsltid=AfmBOorxv2d0nbyS-YUXSrUWDXOLPQGGBW7Jv50gZ_WF9Frc7Ry9sClA.

10. Recommendation ITU-R P.528-4 (08/2019). A propagation prediction method for aeronautical mobile and radionavigation services using the VHF, UHF and SHF bands. P Series. Radiowave propagation [Ел. ресурс]. URL: https://www.itu.int/rec/R-REC-P.528-4-201908-I/en.

11. Програмна реалізація Рекомендації Р.528-4. URL: https://github.com/NTIA/p528-gui/releases.

12. Аналіз завадозахищеності радіомереж з ППРЧ в умовах впливу завад у відповідь / Ольшанський В. В., Гурський Т. Г., Остапчук В. М., Лозунов В. К. // Збірник наукових праць ВІТІ. 2020. № 3. С. 56–62.

DOI: 10.58254/viti.8.2025.04.45

УДК 629.7.004

канд. техн. наук, доц. Данилюк І. А. ORCID: 0000-0003-0955-0108 (ВІТІ ім. Героїв Крут)
Куцаєв В. В. ORCID: 0000-0001-8213-4739 (ВІТІ ім. Героїв Крут)
Семитківська І. В. ORCID: 0009-0000-9962-5032 (ВІТІ ім. Героїв Крут)
Зінченко Н. Р. ORCID: 0009-0004-1837-2838 (ВІТІ ім. Героїв Крут)
Міроненко О. В. ORCID: 0000-0002-3763-5478 (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ДІЙ ОПЕРАТОРА БЕЗПІЛОТНОЇ ПЛАТФОРМИ

У статті розглянуто актуальні питання ефективності функціонування Сил Безпілотних Систем у контексті активного розвитку та масштабування процесів створення, логістики й бойового застосування безпілотних і роботизованих комплексів різного призначення (повітряних, наземних, надводних, підводних тощо). Представлено результати дослідження моделі «ручного управління» дроном, у межах якої центральною ланкою контуру управління виступає людина-оператор. Наукова мета роботи полягає у вивченні можливостей, вимог та функціональних характеристик оператора дрону, що забезпечує "вищий" рівень управління, у той час як апаратно-програмний комплекс виконує роль "нижчого" технічного рівня.

Проведені експерименти підтвердили високу ефективність управління дроном підготовленим бойовим оператором, який здатен самостійно орієнтуватися без використання GPS, розпізнавати цілі, приймати рішення в реальному часі та підтримувати усвідомлений інформаційний обмін. Особливо наголошено на здатності оператора до навчання, донавчання й самонавчання, що є ключовим чинником зростання ефективності під час виконання бойових завдань.

Разом із виявленими перевагами відзначено і певні обмеження – зокрема, швидкість обробки інформації, реакції та прийняття рішень оператором, а також залежність результативності від його психологічно-емоційного стану.

Перспективним напрямом подальших досліджень визначено створення та аналіз автоматизованих і автоматичних моделей управління безпілотними роботизованими комплексами з використанням методів машинного зору, штучного інтелекту та технологій адаптивної взаємодії людини з технічними системами.

Ключові слова: *дрон, оператор, апаратно-програмний комплекс, ручне управління, автоматизована модель управління, штучний інтелект, бойова ефективність.*

I. Danyliuk, V. Kutsaiev, I. Semytkivska, N. Zinchenko, O. Mironenko. Research on the effectiveness of the operator's actions

The article examines the current effectiveness of the Unmanned Systems Forces in the context of the rapid development and large-scale deployment of unmanned and robotic complexes of various types (aerial, ground, and others). The research focuses on the manual drone control model, where the human operator acts as the central element of the control loop. The scientific objective of this study is to explore the operator's capabilities, functional requirements, and cognitive workload in performing higher-level control functions, while the hardware–software complex (HSC) provides lower-level technical control.

Experimental results demonstrate the high efficiency of drone control performed by a well-trained operator capable of independently orienting without GPS, identifying and selecting targets, evaluating mission status, generating control commands, and maintaining situational awareness through conscious information exchange. A key factor contributing to mission success is the operator's ability to learn, relearn, and self-learn, which enhances operational performance and adaptability in combat conditions.

At the same time, several constraints have been identified, including limited information-processing speed, reaction time, and decision-making rate, as well as the influence of the operator's psychological and emotional state on combat effectiveness.

Future research will focus on developing and analyzing automated and fully automatic control models for robotic systems, integrating machine vision, artificial intelligence, and adaptive human–machine interaction technologies to improve mission reliability and efficiency.

Keywords: *drone, operator, hardware–software complex, manual control, automated control model, artificial intelligence, combat effectiveness.*

Постановка проблеми

У сучасних умовах стрімкого розвитку робототехніки, штучного інтелекту та автономних систем центральна наукова проблема, сформульована авторами, набуває особливої актуальності, а саме забезпечення оптимальної, стійкої та адаптивної ефективності

управління автоматизованими роботизованими комплексами, в тому числі безпілотними платформами, за рахунок інтеграції когнітивних переваг людини-оператора з обчислювальними та аналітичними можливостями інтелектуальних систем управління. Наукова новизна полягає у пошуку динамічної рівноваги між рівнем автономності системи та ступенем людського контролю, що передбачає розроблення моделей гібридної людино-машинної взаємодії, оптимізацію інтерфейсів ситуаційного сприйняття та формування архітектури адаптивного керування, здатної реагувати на змінні умови середовища у реальному часі. Такий підхід відповідає сучасним тенденціям розвитку інтелектуальних бойових систем, когнітивної автоматизації та концепції “human-in-the-loop AI”, що поєднує автономність із надійністю та етичним контролем людини.

Для комплексного розуміння цього процесу авторами запропоновано розглядати повний життєвий цикл створення та бойового застосування безпілотних платформ (БП) як послідовність етапів, що показані на діаграмі рисунка 1.

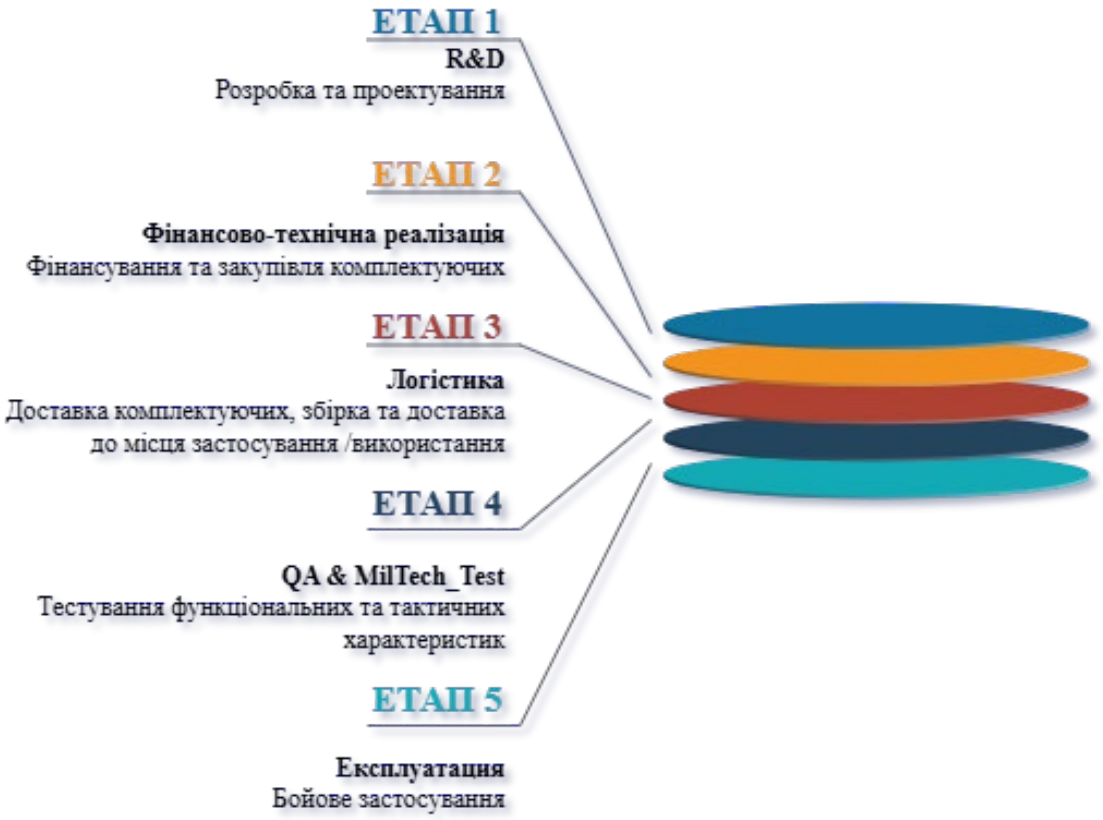


Рис. 1. Діаграма етапів процесу повного життєвого циклу

Як ключовий етап дослідження автори розглядають саме п’ятий етап життєвого циклу – експлатацію/застосування моделей управління БП. У сучасних умовах Сили Оборони України використовують комбіновану схему керування, що поєднує три взаємодоповнювальні моделі: ручну; автоматизовану; автоматичну. При цьому ручна модель розглядається авторами як базова, оскільки саме вона є відправною точкою для побудови гібридних систем прийняття рішень і управління у реальних бойових сценаріях.

На рисунку 2 подано спрощений контур управління, у центрі якого розташовано людину-оператора БП (ОБП), що виконує функції управління “вищого рівня”. У цій моделі оператор формує стратегічні та тактичні рішення, визначає пріоритети місії, координує взаємодію з апаратно-програмним комплексом (АПК), який реалізує технічне управління на “нижчому рівні”.

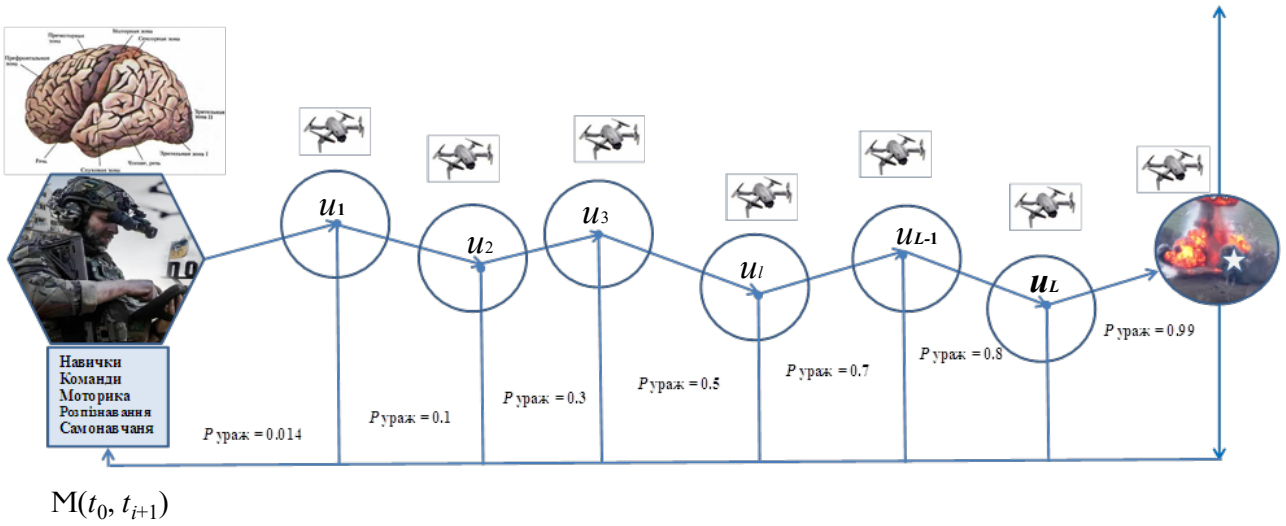


Рис. 2. Модель ручного управління дроном:

u_l – рішення ОБП на кроці $l = (1…L)$; L – загальна кількість рішень ОБП під час виконання місії; $P_{ураж}$ – ймовірність ураження цілі на кроці l.

ОБП володіє унікальними функціональними можливостями, які забезпечують його ключову роль у процесі управління:

усвідомлений обмін бойовими командами та підтримка ефективної комунікації зі спостережними і виконавчими підсистемами;

розвинені моторні навички пілотування та маніпулювання органами керування, що забезпечують точність і чутливість реакції системи;

здатність орієнтуватися на місцевості та розпізнавати рельєф навіть за умов відсутності навігаційних засобів (зокрема GPS);

уміння ідентифікувати ворожі об’єкти, оцінювати пріоритети цілей і приймати рішення в умовах обмеженого часу;

висока адаптивність до навчання й самонавчання, що дозволяє ефективно підвищувати рівень підготовки в польових умовах.

Таким чином, у запропонованій концепції оператор розглядається як “вищий рівень” управління, що забезпечує гнучкість та адаптацію до змін оперативної обстановки. Це підкреслює необхідність подальших досліджень щодо оптимізації взаємодії між людиною та автоматизованими підсистемами, а також пошуку балансу між автономністю БП та контролем оператора у комбінованих режимах бойового застосування.

Методологічні передумови дослідження

Для спрощення моделювання процесів управління та підвищення точності результатів автори ввели низку припущень і обмежень:

ОБП є навчений, досвідчений та боєздатний;

дрон перебуває у стані повної боєготовності (100 %);

система GPS відключена;

умови видимості оцінюються як добрі;

вплив засобів радіоелектронної боротьби (РЕБ) відсутній.

За цих умов боєготовність ОБП ($B_{ОД}$) та боєздатність БП визначають ймовірність успішного ураження цілі. Висока ефективність БП досягається у випадку, коли показник ефективності ураження $(E_у)$ наближається до одиниці $(E_у \rightarrow 1.0)$.

У цьому разі, кількість успішних бойових місій дронів $(N_у)$ має прагнути до кількості застосованих дронів $(N_з)$, що формалізується виразом (1):

$$E_{\text{у}} = \frac{N_{\text{у}}}{N_{\text{з}}}, \quad (1)$$

де N_y – кількість успішних бойових місій;
$N_з$ – кількість застосованих дронів.

Модель боєздатності БП

Боєздатність БП в момент часу t_i ($B_{\text{БП}}(t_i)$) визначається як функція незалежних показників: надійності комплектуючих, якості складання та ефективності логістики, та описується рівнянням (2):

$$B_{\text{БП}}(t_i) = N\text{к}(t_i) * Y\text{з}(t_i) * Л_{\text{БП}}(t_i), \quad (2)$$

де t_i – момент часу оцінювання параметрів;
$N_к(t_i)$ – надійність комплектуючих БП;
$Y_з(t_i)$ – якість збирання БП;
$Л_{БП}(t_i)$ – успішність комплексної логістичного забезпечення.

Модель боєготовності ОБП

Боєготовність ОБП $B_{\text{ОД}}(t_i)$ визначається трьома основними чинниками: навченістю, бойовим досвідом (самонавчанням) та функціональним станом. Цю залежність описує вираз (3):

$$B_{ОБП}(t_i) = \mu_{НОБП}(t_i) * \mu_{SOБП}(t_i) * \Phi_{ОБП}(t_i), \quad (3)$$

де $\mu_{НОБП}$ – рівень навченості оператора;
$\mu_{SOБП}$ – бойовий досвід або здатність до самонавчання;
$Ф_{ОБП}$ – поточний функціональний стан оператора.

Імовірність успіху бойової місії

Загальна ймовірність успіху місії *(Mission(*1+*))* при незалежності параметрів $B_{\text{БП}}$ $B_{\text{ОБП}}$ визначається за формулою (4):

$$Mission(1+, t_0, t_i, \prod u_i) = B_{\text{БП}}(t_0, t_i) * B_{\text{ОБП}}(t_0, t_i) * U(\prod u_i), \quad (4)$$

де U – узагальнений показник якості рішень, що приймає оператор:
$U = 1$, якщо всі рішення є правильними;
$U = 0$, якщо хоча б одне рішення є помилковим.

Аналіз останніх досліджень і публікацій

Проведений авторами аналіз наукових джерел показав, що попередні роботи переважно фокусуються на технічних, кінематичних та алгоритмічних аспектах функціонування БП, тоді як роль ОБП в чистій моделі ручного управління залишається недостатньо вивченою.

Так, у роботі [1], обґрунтовано функцію щільності розподілу цілей, що використовується для планування ефективного застосування БП (безпілотних літальних апаратів, БпЛА).

У [2] проаналізовано ефективність зенітно-ракетного комплексу "Стріла-10" при ураженні цілей типу БпЛА "Форпост", що дозволяє оцінювати бойову результативність дронів-камікадзе порівняно з традиційними вогневими засобами.

Дослідження [3] застосовує алгебру дуальних кватерніонів для моделювання просторового руху БпЛА, що дозволяє поєднати поступальний та обертальний рух і підвищити точність симуляцій.

У [4] доведено, що метод наведення з динамічним упередженням є ефективнішим за пряме наведення, що відкриває перспективи для оптимізації ручного пілотування у бойових умовах.

У роботах [5; 6] розглядаються нейрофізіологічні основи навчання, сприйняття та прийняття рішень людиною**,** що має безпосереднє відношення до когнітивної моделі ОБП.

Джерело [8] присвячене автоматизованому розпізнаванню типів БП за їх радіосигналами, що відноситься до "нижчого рівня" управління, тоді як людський мозок реалізує "вищий рівень" управління (інтерпретації даними).

У [18] описано принципи створення автономних та розподілених робототехнічних систем, що формують основу для майбутніх досліджень у сфері автоматичного управління БП.

На думку авторів, вказані роботи [1–6; 8] недостатньо розкривають механізми діяльності ОБП у "чистій" моделі ручного управління, що визначає актуальність створення формалізованої моделі ОБП як "вищого рівня" управління.

Перспективними напрямками подальших досліджень автори статті вважають автоматизовані та автоматичні моделі управління, а також інтеграцію систем машинного зору та штучного інтелекту у контури взаємодії з ОБП з його вищим командуванням (керівником місії).

Метою статті є дослідження моделі ручного управління БП та оцінка ефективності роботи ОБП.

Виклад основного матеріалу

Опис моделі "ручного управління" БП

Автори розглядають модель "ручного управління" БП, що реалізується ОБП за умов, коли БП є боєздатною, навігаційна система GPS відключена, рівень видимості оцінюється як задовільний, вплив засобів радіоелектронної боротьби відсутній, а системи машинного зору та штучного інтелекту не застосовуються. При цьому вважається, що ОБП перебуває у стані повної боєготовності.

В таблиці 1 вказано рівні управління, складові БП та їхні функції.

У зазначеній моделі ОБП реалізує "вищий рівень" управління БП, приймаючи рішення стратегічного характеру – зокрема щодо напрямку руху, висоти та маневрування БП. Подальша деталізація та реалізація цих команд виконується апаратно-програмним комплексом (АПК) БП, який функціонує на "нижчому (технічному) рівні" управління в автоматичному режимі у тривимірному просторі за координатами (крен (roll), тангаж (pitch), рискання (yaw)).

Завдяки здатності до мислення, навчання та самонавчання, ОБП забезпечує адаптивне управління БП на "вищому рівні". Механізм передачі команд реалізується через тактильну моторику пальців, що формує сигнали управління пультом на основі когнітивної діяльності мозку оператора. Таким чином, на кожен момент часу t формується сукупність рішень і команд, які можна формально описати виразом $M_0(t_0, t_{b+1})$, що відображає динаміку формування й реалізації рішень оператора у часовому інтервалі від моменту ініціації керування (t_0) до моменту виконання чергового циклу (t_{b+1}).

У таблиці 1 наведено узагальнені пояснення до моделі "ручного управління", які демонструють логіку прийняття рішень ОБП на "вищому рівні" та механізм реалізації команд АПК БП на "нижчому рівні" (технічному).

Таблиця 1

Рівні управління, складові БП та їх функції

Рівень управління БП	**Задіяні складові БП**	**Функції, що відпрацьовуються складовою БП**	**Особливості**
"Вищий рівень управління" (ручна складова моделі управління БП)	**ОБП**	1. Планування польоту. – визначення та прокладання маршруту руху БП; – формулювання місії (розвідка, ураження, моніторинг, доставка, відеозйомка тощо); – налаштування параметрів та режимів роботи автопілота відповідно до умов виконання завдання. 2. Управління у режимі реального часу. – здійснення ручного або напівавтоматичного керування польотом; – зміна висоти, швидкості та орієнтації БП у просторі; – виконання тактичних маневрів (зокрема, обліт перешкод, уникнення виявлення або ураження). 3. Контроль за виконанням польоту. – моніторинг основних параметрів функціонування БП (заряд акумулятора, стан двигунів, стабільність радіоканалу тощо); – аналіз та реагування на аварійні сигнали або втрату зв'язку; – прийняття рішень у нештатних або загрозливих ситуаціях з метою збереження боєздатності БП та виконання поставленого завдання	
"Нижчий рівень управління" (АПК) (технічна складова моделі управління БП)	Бортовий обчислювальний модуль (БОМ) (мікроконтролери, процесорні плати (ARM, FPGA, SoC), інтерфейси введення-виведення та контролери шин (CAN, UART, I²C)	1. Оброблення даних від сенсорів. 2. Реалізація алгоритмів стабілізації, навігації, керування та комунікації з пультом оператора	Підтримує алгоритми реального часу (RTOS), має резервування критичних функцій і забезпечує обробку команд у межах мілісекундного інтервалу
	Підсистема навігації та орієнтації (інерційна навігаційна система (IMU), барометричний висотомір, гіроскопи, акселерометри, магнітометри, GPS/GLONASS-приймачі)	Визначення просторового положення БП у трьохвимірному просторі (координати, висота, курс, крен, тангаж, рискання)	У випадку втрати GPS сигналу може переходити на інерційний або візуально-одометричний режим навігації

Рівень управління БП	Задіяні складові БП	Функції, що відпрацьовуються складовою БП	Особливості
	Система стабілізації та управління польотом (контролер польоту (Flight Controller), електронні регулятори обертів (ESC), сервоприводи, двигуни)	Реалізація низькорівневого керування двигунами та органами аеродинамічного управління, стабілізує положення БП	Працює у замкненому контурі із сенсорами та БОМ, підтримуючи стабільність польоту навіть при зовнішніх збуреннях
	Сенсорна підсистема (модулі сприйняття середовища) (оптичні та інфрачервоні камери, лідари, радари ближньої дії, ультразвукові датчики)	Збирання даних про навколишнє середовище для навігації, виявлення перешкод та цілей	У сучасних системах передбачено можливість інтеграції алгоритмів машинного зору та попередньої обробки зображень на борту
	Комунікаційна підсистема (радіомодулі (UHF/VHF), модеми передачі даних, антенні системи, криптографічні модулі захисту зв’язку)	Забезпечення двостороннього обміну інформацією між БП і пунктом управління або іншими платформами	Використовує стійкі до перешкод протоколи (FHSS, DSSS, MIMO) і може функціонувати у зашифрованих каналах відповідно до стандартів НАТО (STANAG 4586))
	Енергетична система (акумуляторні батареї (LiPo, Li-Ion), системи керування живленням (Power Management Unit, BMS), резервні джерела енергії)	Забезпечення живлення всіх підсистем БП та контроль стану енергоресурсів	Може включати функцію автоматичного відключення неважливих підсистем при критичному рівні заряду для продовження часу польоту
	Корисне навантаження (модулі відеоспостереження, системи наведення, бойові блоки, системи захоплення та транспортування)	Виконання спеціалізованих завдань відповідно до типу місії (розвідка, спостереження, ураження, доставка, інше)	Підтримує інтеграцію з АПК для автоматичного керування та передавання даних у режимі реального часу
	Програмне забезпечення АПК (прошивки контролерів, системи реального часу (RTOS), алгоритми керування польотом, системи логування та аналізу даних)	Реалізація логіки роботи всіх апаратних компонентів, обмін даними, діагностику, безпечне оновлення прошивок і шифрування трафіку	Включає модулі ШІ або машинного навчання (у розширених версіях), що забезпечують адаптивну поведінку БП у динамічному середовищі

Головний мозок людини (ГМЛ) є високоорганізованою біологічною системою, сформованою еволюцією для забезпечення адаптивної, цілеспрямованої та ефективної життєдіяльності. У процесі навчання оператора управлінню БП ГМЛ набуває спеціалізованих функціональних властивостей і трансформується у головний мозок оператора безпілотної платформи (ГМОБП). Саме в ГМОБП формується операційний центр прийняття рішень "вищого рівня", який відповідає за сприйняття зовнішніх сигналів, їх когнітивну обробку, збереження релевантної інформації та генерацію команд управління.

До ключових функцій ГМОБП належать: моторне керування польотом дрона; розпізнавання об'єктів, рельєфу та цілей; аналіз ситуаційних змін; обмін інформацією через сенсомоторні канали; формування та реалізація усвідомлених рішень щодо поведінки БП.

На рисунку 2 представлено узагальнену модель "ручного" методу управління БП, що відображає процес формування та реалізації рішення "вищого рівня" ОБП під час управління БП із наземного пункту управління.

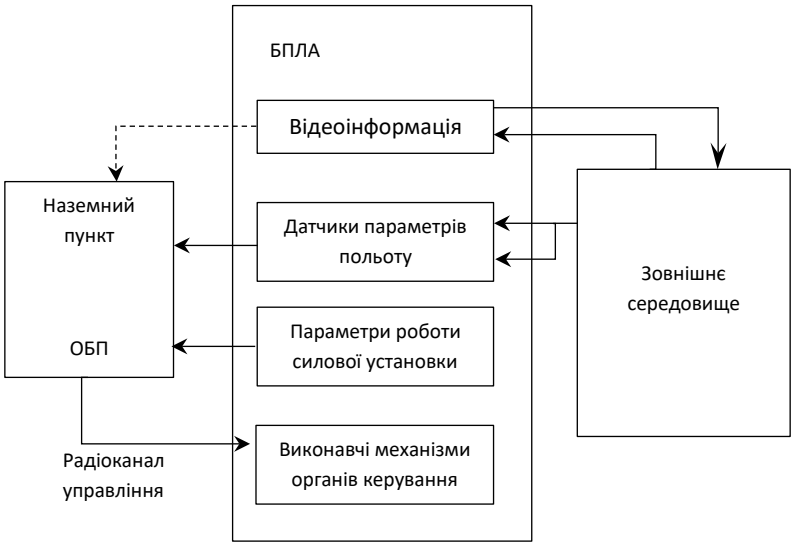


Рис. 2. Функціональна схема моделі "ручного" управління БП

Загальна модель сприйняття світу (МСС) – $M_{old}(t_0)$ – у головному мозку людини (ГМЛ) являє собою багаторівневу когнітивну структуру, яка формується в результаті індивідуального досвіду, навчання та сенсорної взаємодії з навколишнім середовищем. Вона складається з множини підмоделей $\mu_i(t_0)$, що утворюють систему знань, правил, навичок і поведінкових шаблонів, актуальних для моменту часу t_0.

МСС фізично реалізована у вигляді біонейронних ансамблів (БНА) ГМЛ – стабільних нейронних структур, що відповідають за кодування та збереження інформації про зорові, слухові, тактильні та моторні образи. При цьому вербальні конструкції (думки у формі речень) нейрофізіологічно пов'язані аксонами з відповідними БНА, які репрезентують сенсорні або моторні патерни [5].

Таким чином, загальна МСС людиною на момент t_0 може бути формально представлена як множина спеціалізованих підмоделей $M_{old}(t_0)$, що описується виразом (5):

$$M_{old}(t_0) = \{\mu_1(t_0), \mu_2(t_0), \dots, \mu_{b-1}(t_0)\}, \quad (5)$$

де b-1 – індекс останньої підмоделі поведінки, сформованої людиною до моменту часу t_0.

Модель $M_{old}(t_0)$ фіксується у масштабній біонейронній мережі людини (БНМЛ), яка налічує близько ста мільярдів нейронів. Із таким когнітивним багажем майбутній ОБП

прибуває до навчального центру. У процесі підготовки, що триває декілька місяців, здійснюється поетапна трансформація базових знань, навичок і поведінкових моделей новобранця в систему компетенцій оператора – $M_{ОБП}(t_i)$ на момент часу t_i, згідно з виразом (6):

$$\mathrm{M}_{\mathrm{ОБП}}(t_i) = \mathrm{M}_{old}(t_i) + T(\mathrm{M}_{old}(t_i)) + E(\mathrm{M}_{new}(t_i)) + S(\mathrm{M}_{new}(t_{i+1})), \quad (6)$$

де $T(Mold(t_i))$ – трансформація наявних поведінкових моделей;
$E(Mnew(t_i))$ – формування нових навичок і знань у процесі навчання;
$S(Mnew(t_{i+1}))$ – закладання основ для подальшого самонавчання.

Формування системи прийняття рішень ОБП відбувається послідовно у трьох фазах:

1. Фаза трансформації – адаптація існуючих (old) правил поведінки $M_{old}(t_0) \rightarrow T(M_{old}(t_i))$.
2. Фаза формування нових правил – утворення (new) моделей поведінки $E(M_{new}(t_i))$.
3. Фаза розвитку самонавчання – становлення механізмів $S(M_{new}(t_{i+1}))$, які забезпечують автономне вдосконалення компетенцій під час виконання бойових завдань.

Для того щоб новобранець перетворився на досвідченого оператора з оновленою моделлю сприйняття світу $M_{ОБП}(t_{i+1})$ на час t_{i+1}, біонейронні ансамблі (БНА-N) головного мозку мають засвоїти базові підмоделі поведінки відповідно до виразу (7):

$$\mathrm{M}_o(t_0, t_{i+1}) \rightarrow \{\sum \mu_{old}(t_0), \sum T\mu_{old}(t_{i-1}), \sum E\mu_{new}(t_i), \sum S\mu_{new}(t_{i+1})\}, \quad (7)$$

де $\sum \mu_{old}(t_0)$ – поведінкові підмоделі, сформовані до початку навчання;
$\sum T\mu_{old}(t_{i-1})$ – модифіковані під час навчання правила поведінки;
$\sum E\mu_{new}(t_i)$ – нові навички, набуті в навчальному центрі;
$\sum S\mu_{new}(t_{i+1})$ – підмоделі самонавчання, що реалізуються під час діяльності ОБП у бойових підрозділах.

Унаслідок дії механізму самонавчання кількість поведінкових підмоделей $\sum S\mu_{newi}(t_{b+1})$ постійно зростає.

Головний мозок оператора безпілотної платформи (ГМОБП) у своїй оперативній зоні (БНА – № 1) формує мізансцену всіх подій, включно з виконанням польотних завдань (місій) та зовнішніх умов, які надходять від сенсорних систем – $\ddot{G}oper_i(t_n, sensor)$.

Таким чином, у ГМОБП створюється когнітивна модель місії, на основі якої здійснюється прогнозування розвитку подій на кожному етапі ("l") виконання завдання. ГМОБП безперервно аналізує ситуацію відповідно до сформованої бази правил, компетенцій і навичок – $Mo(t_0, t_{i+1})$ на момент часу t_{i+1}, та генерує рішення управління $\rightarrow u(l)$. Модель мізансцени отримує дані від сенсорів оператора щодо всіх зовнішніх та внутрішніх об'єктів, процесів і явищ для моделювання та прогнозування подальшого розвитку ситуації [14]:

$$\text{ОБРАЗ} = \ddot{\mathrm{G}}_{oper_i}(t, sensor, l, \mu\text{-правила}) \rightarrow u(l+). \quad (8)$$

Для цього ГМОБП використовує когнітивну мізансцену $\ddot{\mathrm{G}}(\Delta t)$ як основу для аналізу сенсорних даних, що надходять від органів чуття оператора (зір, слух, дотик, нюх, смак). Завдяки інтеграції цих сигналів у просторі та часі, ГМОБП здатен:

передбачати розвиток подій для кожної аналізованої мізансцени – $\mu_{розвитку\_подій}(+t_i) \rightarrow u(t_i, l+)$;

приймати рішення "вищого рівня" для апаратно-програмного комплексу (АПК) безпілотної платформи – $u_{рішенняВР}(t_{i+1}) \rightarrow u(t_{i+1}, l+)$;

генерувати тактильні команди управління – $\mu_{рух}(\Delta t_{i+2})$, що реалізуються через моторну активність пальців оператора на пульті керування.

На рисунку 3 схематично зображено процес безперервного приймання, обробки, зберігання та передачі сенсорної інформації у моделі ГМОБП. Система сенсорів представлена каналами: v – зоровий (очі), z – слуховий (вуха), s – смаковий (язик), n – нюховий (ніс), d – тактильний (шкіра, відчуття температури, болю, тиску).

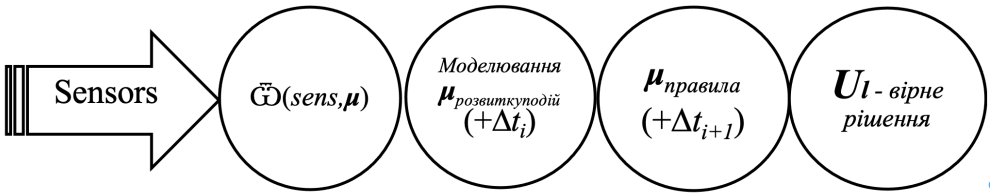


Рис. 3. Послідовність прийняття рішення *u* в ГМОБП

Функціональний ансамбль БНА – № 1 формує з цих сенсорних сигналів когнітивну мізансцену $\ddot{Ѿ}(sens, \mu)$, що включає інформацію про місце розташування оператора, стан пульта, динаміку рухів пальців, розпізнавання цілей та елементів місцевості у момент часу t_i. Отримана мізансцена $\ddot{Ѿ}_w$ далі оцінюється ГМОБП відповідно до актуальних компетенцій $\mu_i(t_i)$, після чого формується керуюче рішення u_l.

Таким чином, ГМОБП функціонує як адаптивна когнітивна система прогнозування і контролю, у якій поєднуються сенсорна інтеграція, когнітивне моделювання та моторна реалізація. Це забезпечує здатність оператора не лише реагувати на зміни зовнішнього середовища, але й проактивно формувати оптимальні дії у складних бойових сценаріях.

Модель підготовки ОБП

Розроблена модель підготовки ОБП $Mo(t_0, t_{0+}n_{міс})$ дозволяє формувати нормативи та вимоги до професійної та психофізіологічної підготовки ОБП до виконання бойових завдань у реальних умовах.

Успішність виконання місії визначається послідовністю своєчасно прийнятих і безпомилкових рішень оператора:

$$\{u_{1(+)}, u_{2(+)}, \dots, u_{L(+)}\},$$

де L – загальна кількість рішень у межах місії.

Формально місію можна подати як (9):

$$Mission(1(+), T_i) = \{u(t_{0(+)}), \dots, u(t_{i(+)})\}, \quad (9)$$

де $T_i = t_i - t_0$ – загальний час виконання місії.

Імовірнісна модель прийняття рішень

Імовірність прийняття правильного рішення на кожному кроці залежить від рівня сформованості у ГМОБП системи адекватних правил поведінки:

$$M(t_0, t_{i+1}) = \sum \mu_{old}(t_0) + \sum T\mu_{old}(t_{i-1}) + \sum E\mu_{new}(t_i) + \sum S\mu_{new}(t_{i+1}), \quad (10)$$

де μ_{old} – раніше засвоєні компетентності ОБП;

$T\mu_{old}$ – трансформовані (адаптовані) компетентності ОПБ;

$E\mu_{new}$ – нові знання, отримані під час місії;

$S\mu_{new}$ – нові сенсомоторні патерни поведінки ОБП.

Тоді ймовірність правильного рішення визначається як:

$$P(u_i) = \frac{\mathrm{M}(t_i, t_{i+1})}{\mathrm{M}_{max}(t_i, t_{i+1})} \to 1, \tag{11}$$

де M_{max} – максимально можлива система адекватних рішень ОБП.

Імовірність успіху місії

Загальна ймовірність успішного завершення місії ОБП за умови незалежності подій B_d та $B_{\text{ОБП}}$ описується виразом (12):

$$P_{mission}(1(+), L, T_i) = \prod_i (B_{\text{ОБП}.l}(\Delta t_i) * P(u_i)), \tag{12}$$

де $\Delta t_i = t_i - t_{i-1}$ – часовий інтервал між послідовними рішеннями.

На початковому етапі місії (t_0) оператор отримує завдання і починає генерувати послідовність рішень u_l, що формують команди управління апаратно-програмним комплексом (АПК) дрону:

$$u_p = g(u_1, u_2, \dots, u_L), \tag{13}$$

де u_p – сукупність керуючих дій оператора;

g – функціональна модель процесу "ручного управління" БП.

Імовірнісна оцінка успішності місії

Перший компонент моделі – це ймовірність успіху місії $P(Mission(L+))$. Якщо ймовірність того, що оператор на кожному кроці приймає правильне рішення, дорівнює p, і всі L рішень є незалежними (14):

$$P(Mission(L+)) = P_{success}(+, L, p) = p^L. \tag{14}$$

Результат місії є булевою величиною, що приймає значення:

1 – місія успішно виконана;

0 – місія провалена.

Таким чином, при кількості рішень $L = 50$ загальна ймовірність успіху дорівнює:

$$P_{success}(+) = p^{50}.$$

На рисунку 4 наведено приклад графіка залежності $P_{success}(L)$ від параметра $p \in [0; 1]$. За умови, що ОБП приймає всі рішення вірно ($p = 1$), ймовірність успішного виконання місії дорівнює (15):

$$P_{mission}(L; p) = p^L = Mission(50; 1{,}0) = 1. \tag{15}$$

На рисунку 4 відображено графік залежності ймовірності успіху місії при кількості рішень ОБП $L = 50$ від імовірності прийняття правильних рішень $p \in (0{,}9; 1{,}0)$.

Другим компонентом розробленої моделі є часова затримка τ, яка визначається сумарним часом прийняття рішення оператором u_i та часом відпрацювання відповідної команди АПК БП (16):

$$\tau_i = \Delta t_{u.i} + T_{АПК.u.i}. \tag{16}$$

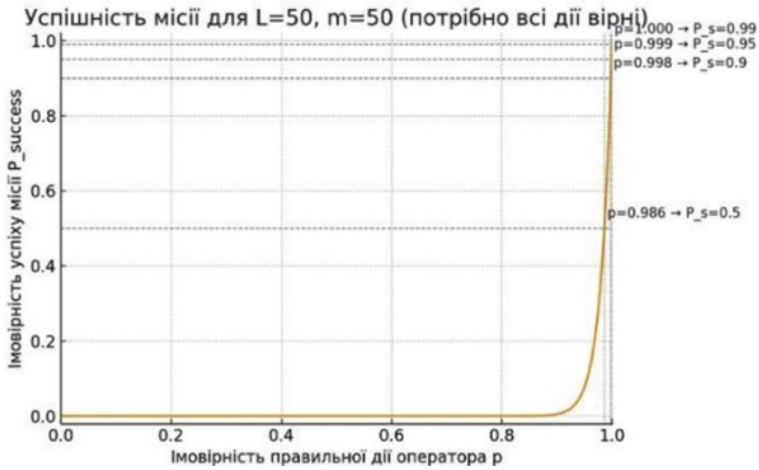


Рис. 4. Графік залежності ймовірності успіху місії від ймовірності правильних дій ОБП

На рисунку 5 наведено результати моделювання інерційності системи управління дроном у режимі "ручного управління".

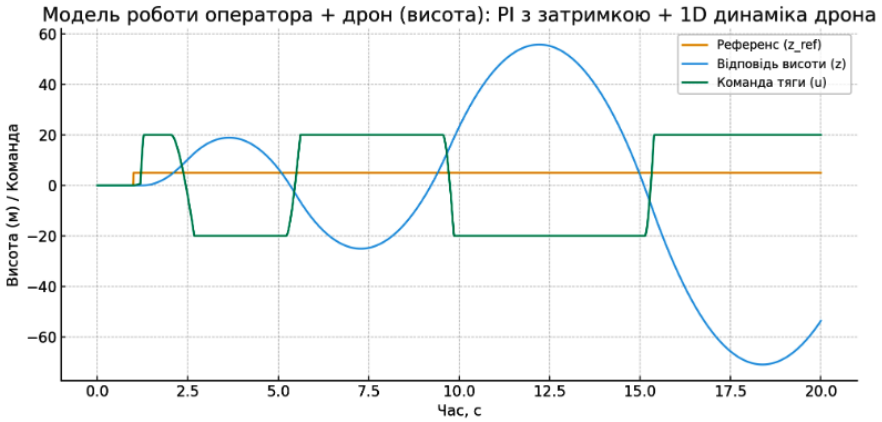


Рис. 5. Графік демонстрації інертності моделі "ручного управління" БП

Інертність реакції системи на рішення u_l зумовлює можливість виходу за допустимі часові межі τ_i, що, у свою чергу, може призвести до порушення часової послідовності виконання команд та, як наслідок, до неможливості успішного завершення місії.

За умови повної боєздатності, БП ($B_d = 1.0$), вирішальним чинником успіху місії стає ефективність дій ОБП ($E_{\text{ОБП}}$), яка вимірює здатність оператора генерувати безперервну послідовність правильних і вчасно виконаних команд для АПК БП. Формалізація цього показника наведена в рівнянні (17):

$$E_{\text{ОБП}} = B_{\text{ОБП}} \cdot \frac{\sum_{l=1}^{L} CrU_l}{L}, \tag{17}$$

де L– загальна кількість рішень у місії;
$B_{\text{ОБП}}$ – коефіцієнт боєготовності ОБП;
CrU_l – індикатор успіху на кроці l(детальніше нижче).

Успіх кожного кроку CrU_l визначається одночасною наявністю (l) правильного рішення оператора $u_{\text{ОБП},l}$ та своєчасної реалізації цього рішення АПК БП. Це формалізується як (18):

$$CrU_l = u_{\text{ОБП},l} \cdot \tau_{u,l}, \tag{18}$$

де $u_{\text{ОБП},l} = 1$, якщо рішення $l -$ є коректним (веде до успіху), і $u_{\text{ОБП},l} = 0$ – якщо рішення хибне;
$\tau_{u,l}$ – бінарний індикатор своєчасності реалізації рішення (19).

$$\tau_{u,l} = \begin{cases} 1, \text{якщо } (\Delta t_{u,\text{ОБП},l} + \Delta t_{\text{АПК},l}) < \tau_{\max} \\ 0, \text{інакше} \end{cases}, \tag{19}$$

де $\Delta t_{u,\text{ОБП},l}$ – час прийняття рішення оператором на кроці l;
$\Delta t_{\text{АПК},l}$ – час відпрацювання цієї команди АПК;
$\tau_{\max}$ – максимально допустима затримка для збереження життєздатності місії на цьому етапі.

Фактором загального успіху місії є сума послідовно своєчасно виконаних правильних рішень ОБП, яку можна оцінити як суму індикаторів кроків (20):

$$\text{C}_{\text{mission}}(L+) = \sum_{l=1}^{L} CrU_l. \tag{20}$$

Якщо для виконання місії необхідно реалізувати L своєчасних і коректних рішень, то умова успіху еквівалентна $C_{\text{mission}}(L+) = L$, інакше, при $\text{C}_{\text{mission}}(L+) < L$, місію вважатимуть нездійсненною.

Імовірнісна оцінка успіху місії формується із врахуванням імовірності коректності прийняття рішення $P(u_i)$ та фактора своєчасності CrU_i. Один із варіантів такої оцінки має вигляд (21):

$$P_{\text{mission}}(1(+), L, T_i) = B_{\text{ОБП}} \cdot \frac{\sum_{l=1}^{L} P(u_l) \cdot CrU_l}{\sum_{l=1}^{L} P(u_l) \cdot CrU_l^{\max}}, \tag{21}$$

де $CrU_l^{\max} -$ нормувальний множник для кроку l (максимально можлива оцінка успіху кроку при оптимальних умовах). Відповідно, ймовірність провалу місії (22):

$$P_{\text{mission}}(L-) = 1 - B_{\text{ОД}} \cdot \frac{\sum_{l=1}^{L} P(u_l) \cdot CrU_l}{\sum_{l=1}^{L} P(u_l) \cdot CrU_l^{\max}}. \tag{22}$$

Статистичний аналіз бойової діяльності підрозділів СБС показує [19], що для досягнення високої ймовірності успіху вимоги до послідовності рішень стають жорсткими. Наприклад, якщо в місії $P(E_{mission}(2000+))$ всі 2000 рішень ОБП будуть коректними та виконані вчасно, то послідовність $\{u_{2000}\}$ забезпечує завершення місії з імовірністю $P\big(E_{mission}(2000+)\big) = 1$. Другий приклад – ураження цілі дроном-камікадзе, або успішне завершення розвідувальної задачі. На рисунку 6 показано, що ймовірність успіху зростає зі збільшенням кількості підряд ідентично правильних рішень оператора [18].

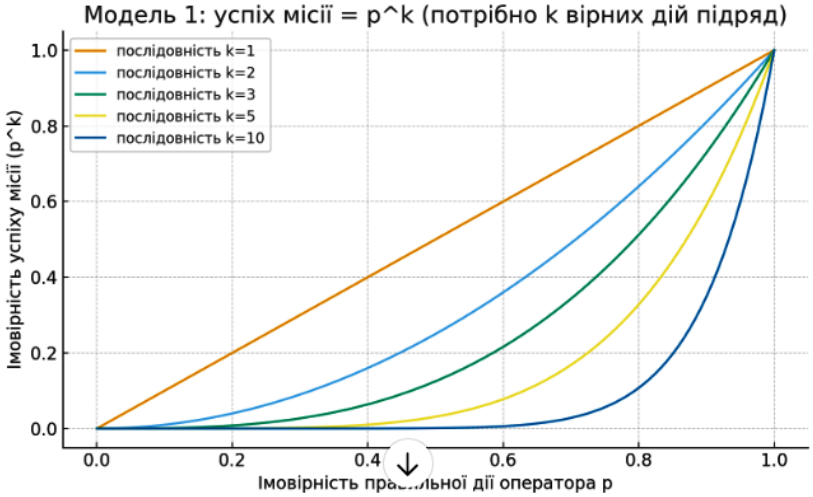


Рис. 6. Графік залежності успіху місії при кількості вірних дій ОБП підряд при k = [1, 2, 3, 4, 5, 10]

Наприклад, для забезпечення практично гарантованого успіху складної місії (в умовах L ≈ 1000 кроків), статистичні дані [18] вказують на необхідність досягнення мінімальних значень ключових показників на рівні:

$B_{\text{БП}}^{\min} > 0{,}99$ (боєздатність БП);
$B_{\text{ОБП}}^{\min} > 0{,}995$ (боєготовність оператора).

Аналіз моделі "ручного управління" БП та статистики бойового застосування [19] показує наступні емпіричні інтервали ефективності оператора ($E_{\text{ОБП}}^{N\text{ міс}}$) залежно від тривалості підготовки:

новачок (0 місяців навчання): $E_{\text{ОБП}}^{0\text{ міс}} \approx 0{,}00 - 0{,}01$;
після 1 місяця навчання: $E_{\text{ОБП}}^{1\text{ міс}} \approx 0{,}3 - 0{,}5$;
після 3 місяців навчання: $E_{\text{ОБП}}^{3\text{ міс}} \approx 0{,}90 - 0{,}95$;
досвідчений оператор (≥ 12 місяців у бойовому підрозділі): $E_{\text{ОБП}}^{12\text{ міс}} \approx 0{,}95 - 0{,}99$.

Ключовим параметром розвитку здібностей оператора є **коефіцієнт навчаємості** $K_{\text{НОБП}}$, який характеризує темпи здобуття нових навичок у процесі формальної підготовки, емпіричний інтервал для цього показника оцінюється як (23):

$$K_{\text{НОБП}} \in [0{,}90 - 0{,}99]. \quad (23)$$

Під час експлуатації в бойовому підрозділі важливим є також **коефіцієнт самонавчаємості** $K_{\text{СНОБП}}$, що відображає здатність оператора самостійно генерувати та інтегрувати нові бойові підмоделі у реальних умовах. Для бойових підрозділів СБС автори рекомендують орієнтовний інтервал самонавчаємості, згідно з (24), що свідчить про високу здатність до оперативного самовдосконалення на фронті.

$$K_{\text{СНОБП}} \in [0{,}90,\ 0{,}95]. \quad (24)$$

Завдяки самонавчаємості оператор може самостійно генерувати, перевіряти та впроваджувати нові ефективні бойові рішення, що призводить до розширення простору бойових підмоделей – набору правил, навичок і компетенцій (25).

$$\{\sum \text{Mo} + S\mu_{new_i}(t > 12 \text{ міс})\}. \quad (25)$$

Для систем штучного інтелекту (ШІ) коефіцієнт формальної навчаємості $K_{H.\text{ШІ}}$, на думку авторів, може варіюватися в межах (26), залежно від якості алгоритмів, даних навчання та діяльності конструкторів і інженерів.

$$K_{H.\text{ШІ}} \in [0{,}0 - 1{,}0]. \quad (26)$$

Натомість коефіцієнт ефективного самонавчання ШІ у польових бойових умовах, без доступу до репрезентативних міток або людської корекції, автори вважають близьким до нуля (27).

$$K_{\text{СНШІ-МЗ}} \approx 0{,}0. \quad (27)$$

Це означає, що наразі автономні системи рідко демонструють значиме самостійне покращення бойових компетенцій без зовнішнього донавчання та інженерної підтримки [18].

На рисунку 7 наведений графік емпіричної залежності ефективності оператора БП $E_{\text{ОБП}}$ від часу навчання та подальшої служби в бойовому підрозділі СБС. З огляду на отримані оцінки, для планування підготовки персоналу та формування нормативів боєздатності доцільно використовувати поєднання індикаторів $B_{\text{БП}}$, $B_{\text{ОБП}}$, $K_{\text{НОБП}}$та $K_{\text{СНОБП}}$, як вхідних параметрів при моделюванні ймовірності успіху складних місій.

Рис. 7. Графік оцінки ефективності дій ОБП під час навчання та подальшого самонавчання

Під час тримісячного курсу підготовки в навчальному центрі ОБП послідовно опановує, закріплює та удосконалює **набори базових бойових правил і моделей поведінки** $\mu_{\text{ОБП}}$, які відображають його алгоритми прийняття рішень у процесі управління БП. Завдяки систематичному тренуванню досягається поступове зростання рівня компетентності до максимально можливого значення (28).

$$M(t_{3\text{ міс}}) \to \max E_{\text{ОБП}}^{3\text{ міс}}. \quad (28)$$

Це свідчить про набуття ОБП стійких навичок контролю польоту, орієнтування в бойовій обстановці, реагування на перешкоди та ефективного виконання бойових завдань у межах типових сценаріїв.

Після переходу до служби у бойовому підрозділі сил безпілотних систем (СБС), оператор стикається з новими, непередбачуваними обставинами ведення бойових дій, для яких відсутні

раніше сформовані шаблони дій або напрацьовані заходи реагування. У таких умовах активізується **механізм самонавчання**, який можна описати як появу нових підмножин бойових правил (29), що відображають процес самостійного формування ОБП нових тактичних моделей, прийомів управління та адаптивних стратегій застосування БП, що відображають процес самостійного формування ОБП нових тактичних моделей, прийомів управління та адаптивних стратегій застосування БП.

$$\sum SM_{new_i}(t_{6-12\ \text{міс}}). \tag{29}$$

Таким чином, на етапі бойової служби формується **друга фаза розвитку компетентності оператора** – фаза самонавчання, у якій індивідуальний досвід і практична діяльність безпосередньо перетворюються на нові тактичні знання, що підвищують загальну ефективність виконання місій (30).

$$E_{\text{ОБП}}(t_{12\ \text{міс}}) = f\left(M_{\text{баз}}, \sum SM_{new_i}\right). \tag{30}$$

Цей процес має ключове значення для підвищення гнучкості та автономності дій ОБП, особливо у випадках, коли динаміка бойової обстановки вимагає прийняття нестандартних рішень у реальному часі.

Висновки

Таким чином, авторами статті досліджено модель "ручного управління" БП і проведено оцінку ефективності роботи ОБП. Ключові результати та положення наступні:

1. Показано, що ОБП у своїй роботі використовує природні когнітивні й сенсорні можливості головного мозку (оцінка візуальної інформації, сприйняття та генерація звукових команд, здатність до навчання і самонавчання), що забезпечує високий рівень адаптивності в умовах змінної оперативної обстановки.

2. Команди, сформовані на основі системи компетенцій ОБП, реалізують управління "вищого рівня" – визначають тактичні цілі та пріоритети дій. АПК БП переводить ці рішення у технічні дії на "нижчому рівні" (реалізаційному).

3. Запропонована модель "ручного управління" дозволяє імітувати та аналізувати тактичні наслідки діяльності ОБП у бойових умовах, зокрема вплив людського фактора на результати місій.

4. У статті розглянуто набір корисних коефіцієнтів та метрик для прогнозування успіху місії, зокрема ефективність дій ОБП ($E_{\text{ОБП}}$), боєздатності БП, боєготовності ОБП, а також показників навчаємості і самонавчаємості ОБП. Ці метрики можуть використовуватись для кількісної оцінки ризиків та оптимізації розподілу ролей між людиною й автоматикою.

5. Як перспективний напрям подальших досліджень визначено розробку та валідацію моделі "автоматичного управління" БП, а також дослідження комбінованих режимів взаємодії "людина – система" з метою підвищення загальної стійкості й ефективності управління в бойових сценаріях.

Надані результати формують теоретичну основу для подальшої розробки гібридних архітектур управління, що поєднують переваги людини-оператора з можливостями сучасних апаратно-програмних та інтелектуальних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пулеко І. В., Чумакевич В. О., Шестак І. М., Рикун В. Л., Свистунович І. В. Функція щільності розподілу цілей для планування застосування безпілотних літальних апаратів // Збірник наукових праць ЖВІ. Житомир, 2024. Вип. 27. С. 69–80.

2. Кудряшов В. Є., Литовченко Д. М., Воїнов В. В., Хроль Л. О., Куценко В. В. Ефективність стрільби ЗРК “Стріла-10” при виявленні цілей через оптичний визирь і автоматизованій цілевказівці // Збірник наукових праць ДНДІ ВС ОВТ. Черкаси, 2023. Вип. 4 (18). С. 41–48.

3. Пулеко І. В., Андрєєв О. В., Дубина О. Ф., Чумакевич В. О., Паламарчук А. С. Модель руху безпілотних літальних апаратів на основі алгебри дуальних кватеріонів // Збірник наукових праць ЖВІ. Житомир, 2022. Вип. 23. С. 52–61.

4. Геращенко М. М., Нестеренко С. О., Ісаченко О. О., Лось А. М., Сірик О. М. Моделі автоматичного наведення ударних безпілотних літальних апаратів на рухому ціль // Збірник наукових праць ДНДІ ВС ОВТ. Чернігів, 2021. Вип. 2 (8). С. 20–30.

5. Куцаєв В. В., Лазута Р. Г., Головко О. Є., Самелюк В. П. Обрис поширеної телекомунікаційної моделі нейрона // Вісник ВІТІ. Комунікаційні та інформаційні системи. 2024. № 1 (5). С. 32–46.

6. Блум Ф., Лейзерсон А., Хофстедтер Л. Мозок, разум і поведінка. Редакція біологічної літератури / Переклад з англ. канд. біол. наук Є. З. Годіної // RoyalLib: електронна бібліотека. URL: https://royallib.com/book/blum_floyd/mozg_razum_i_povedenie.html (дата звернення: 19.10.2022).

7. Вентцель Е. С. Теорія ймовірностейй. 6-е вид. Вищ. шк. В., 1999. С. 134.

8. Нагорнюк О. А. База даних для автоматизованого розпізнавання типу безпілотного авіаційного комплексу за його радіосигналами // Збірник наукових праць ЖВІ. 2023. Вип. 25 (І).

9. Альберт Енштейн. Теорія здобутку нових знань. Education for Independent Thought», New York Times, 1952.

10. Бернацький А. П. Основи робототехніки військового призначення / А. П. Бернацький. Київ: ЛІРА-К, 2024. 498 с.

11. Ладієва Л. Р. Методи оптимізації та пошуку оптимальних рішень: елек. мережне навч. видня / Укл. Л. Р. Ладієва. Київ: КПІ ім. Ігоря Сікорського, 2023. 73 с.

12. Матвійчук Р. Д., Данільчук О. М. Порівняння найвідоміших алгоритмів пошуку / Вісник студентського наукового товариства ДонНУ імені Василя Стуса. 2022. С. 230–234.

13. Гібсон К. Р. Еволюція людського інтелекту: ролі розміру мозку та розумової побудови // Поведінка мозку та еволюція. 2002. № 59. С. 10–20.

14. Мартін А. Представлення предметних понять в мозку // Щорічний огляд психології. № 58. С. 25–45.

15. Шерман С. М., Гільлери Р. В. Дослідження таламуса і його ролі в корковій функції. 2-ге вид. Кембридж, Массачусетс: MIT Press, 2006.

16. Олег Печененко, Ярослав Ярошенко, Олександр Блискун. Питання бойового застосування військових частин та підрозділів державної авіації україни, зенітних ракетних, радіотехнічних та спеціальних військ, зв’язку, радіотехнічного забезпечення та автоматизації управління. Загальні підходи до оцінювання ефективності протиповітряної оборони з урахуванням застосування FPV-дронів-перехоплювачів // Повітряна міць України. 2024. Том 2. № 7. С. 50–54.

17. Горбачов К. М. Часткова методика оцінювання ефективності забезпечення бойових дій підрозділів протиповітряної оборони військових формувань тактичного рівня засобами ураження // Збройна боротьба: теорія, забезпечення, досвід. 2021. № 4 (70). С. 15–21.

18. Бернацький А. П. Практичне програмування роботів: GAZEBO Military Edition: навч. посіб. Київ: Видавництво “Ліра-К”, 2025.

19. Щоденна статистика уражень дронами // URL: https://dev.ua/news/stata-sbs-1750842989 (дата звернення: 25.06.2025).

DOI: 10.58254/viti.8.2025.05.62

УДК 621.391.17

д-р техн. наук, професор Єрохін В. Ф. ORCID: 0000-0001-7194-8577 (ВІТІ ім. Героїв Крут)
канд. техн. наук, професор Радзівілов Г. Д. ORCID: 0000-0002-6047-1897 (ВІТІ ім. Героїв Крут)
Коваленко О. О. ORCID: 0009-0008-4087-8770 (ВІТІ ім. Героїв Крут)

ПОШУК ШЛЯХІВ РЕДУКЦІЇ ОПТИМАЛЬНИХ АЛГОРИТМІВ РОЗДІЛЕННЯ-ДЕМОДУЛЯЦІЇ ВЗАЄМНО НЕОРТОГОНАЛЬНИХ ЦИФРОВИХ СИГНАЛІВ

У статистичній теорії розділення (СТР) цифрових сигналів (ЦС), як у самостійному відгалуженні в теорії багатокористувацького детектування, розглядаються задачі розділення-демодуляції сигналів, взаємно неортогональних на довжині інформаційного тактового інтервалу. При цьому за критерій оптимальності вибирається мінімум імовірності помилки в оцінці групового або індивідуальних інформаційних дискретних параметрів. Аналіз завадостійкості алгоритмів обробки адитивної суміші взаємно неортогональних ЦС, що синтезуються методами СТР за індивідуальним критерієм, дозволяє одержувати відповіді на питання про межі їх потенційної завадостійкості. На сьогодні вже одержані результати такого аналізу для випадків Binary Phase Shift Keying (BPSK), коли взаємно неортогональних сигналів – не більше трьох. Однак ці результати мають скоріше теоретичне значення. Відомо, що складність алгоритмів розділення-демодуляції, оптимальних за індивідуальним критерієм, характеризується експоненціальною залежністю їх складності від кількості та позиційності ЦС, що підлягають розділенню. Лінійна залежність складності спостерігається лише в окремих випадках – наприклад, коли в спостереженні присутня деяка, наперед задана кількість взаємно ортогональних сигналів і лише один, неортогональний всім.

Виконується оцінювання можливостей спрощення оптимальних алгоритмів розділення-демодуляції і детально розглядається випадок, коли в спостереженні присутні три взаємно неортогональні сигнали BPSK, в загальному випадку асинхронні за тактовими точками. Пропонується підоптимальний редуційований алгоритм, суттєво спрощений порівняно з таким, що є оптимальним за індивідуальним критерієм оптимальності. За найгіршого випадку взаємної лінійної залежності між сигналами наведена умова його роботоспроможності. За більш загальних умов – довільних ступеней неортогональності між сигналами продемонстровано, що суттєвого спрощення алгоритму розділення-демодуляції трьох ЦС можна дістатись, забезпечивши певні відміни в миттєвих потужностях між сигналами.

Наводяться приклади редуційованих структурних схем алгоритмів розділення-демодуляції трьох взаємно неортогональних сигналів BPSK, синхронних та асинхронних за тактовими точками. Виконані оцінки втрат у завадостійкості внаслідок запропонованих спрощень.

Ключові слова: *цифрові сигнали, взаємна неортогональність, критерій оптимальності, розділення-демодуляція, редукція, імовірність помилки.*

V. Yerokhin, G. Radzivilov, O. Kovalenko. Search for ways to reduse optimal algorithms for separation-demodulation of mutially nonortogonal digital signals

In the statistical theory of separation (STS) of digital signals (DS), as in an independent branch in the theory of multi-user detection, the problems of separation-demodulation of signals that are mutually non-orthogonal in the length of the information clock interval are considered. In this case, the minimum probability of error in the estimation of group or individual information discrete parameters is chosen as the optimality criterion. Analysis of the noise immunity of algorithms for processing an additive mixture of mutually non-orthogonal DS synthesized by STS methods according to an individual criterion allows us to obtain answers to questions about the limits of their potential noise immunity. To date, the results of such an analysis have already been obtained for the cases of Binary Phase Shift Keying (BPSK), when there are no more than three mutually non-orthogonal signals. However, these results are rather of theoretical significance. The fact is that the complexity of the separation-demodulation algorithms, optimal according to the individual criterion, is characterized by an exponential dependence of their complexity on the number and position of the DS to be separated. A linear dependence of the complexity is observed only in some cases – for example, when the observation contains a certain, predetermined number of mutually orthogonal signals and one, non-orthogonal to all.

The possibilities of simplifying optimal division-demodulation algorithms are evaluated and the case is considered in detail when three mutually non-orthogonal BPSK signals are observed, in the general case asynchronous in clock points. A suboptimal reduced algorithm is proposed, significantly simplified in comparison with the one that is optimal

in terms of the individual optimality criterion. The condition for its operability is given for the worst case of mutual linear dependence between the signals. Under more general conditions - arbitrary degrees of non-orthogonality between the signals – it is demonstrated that a significant simplification of the division-demodulation algorithm for three DS can be achieved by providing certain cancellations in the instantaneous powers between the signals.

Examples of reduced structural schemes of division-demodulation algorithms for three mutually non-orthogonal BPSK signals, synchronous and asynchronous in clock points, are given. Estimates of noise immunity losses due to the proposed simplifications were made.

Keywords: *digital signals, mutual non-orthogonality, optimality criterion, separation-demodulation, reduction, error probability.*

Постановка задачі. Розв'язанню актуальної проблеми нестачі канального (частотного) радіоресурсу спеціалістами в галузі електронних комунікацій в усьому світі приділяється невпинно зростаюча увага. Бурхливо розвиваються нові дослідницькі напрямки в межах загальної теорії електронних комунікацій – теорія багатокористувацького детектування (БКД) та її самостійне відгалуження – статистична теорія розділення (СТР) цифрових сигналів (ЦС) [1–4 та ін.], неортогональний множинний доступ (НОМД) [5; 6 та ін.]. Створення та розвиток вищезазначених теорій обумовили появу прикладного напрямку їх спільного застосування – так званого НОМД з розподілом за потужністю (англ. Power Domain – Nonortogonal Multiple Access, PD-NOMA [7; 8]).

Під час дослідження питань за тематикою PD-NOMA з'ясувалось, що відміни в миттєвих потужностях взаємно неортогональних сигналів, що підлягають розділенню, повинні дорівнювати 6 дБ або дещо більше [3; 9–12], і тому з практичних міркувань на сучасному етапі слід обмежуватись застосуванням у спільному частотному ресурсі не більше, ніж трьома сигналами.

Алгоритм розділення-демодуляції трьох взаємно неортогональних ЦС з двійковою фазовою маніпуляцією (Binary Phase Shift Keying, BPSK), синтезований із залученням СТР за критерієм мінімуму ймовірності помилки в оцінці інформаційних дискретних параметрів (ДП) кожного із сигналів [3], може бути одержаний із загального рішення [1, с. 161–162]. При цьому виявилась технічно неприйнятна складність цього алгоритму навіть при взаємному тактовому синхронізмі сигналів.

Мета дослідження. Одержання прийнятних за складністю редуційованих (спрощених) підоптимальних алгоритмів розділення-демодуляції трьох нерівноенергетичних взаємно неортогональних сигналів BPSK, синхронних та асинхронних за тактовими точками. Оцінка втрат у завадостійкості внаслідок технологічно прийнятних спрощень.

Виклад основного матеріалу

1. Оцінювання можливостей редукції оптимальних алгоритмів розділення-демодуляції взаємно неортогональних цифрових сигналів

Правило прийняття рішень (ППР) $r_1^* = \overline{0,1}$ щодо значення $r_1 = \overline{0,1}$ інформаційного ДП першого ЦС, що спостерігається на фоні адитивного впливу двох подібних взаємно неортогональних ЦС, синхронних йому за тактовими точками за моделі спостереження

$$y_t = \sum_{i=1}^{3} (-1)^{r_i} s_i(t) + n(t), \tag{1}$$

$$t \in \left[t_{k-1}, t_k\right);\ r_i = \overline{0,1};\ k = 1,2,3\ldots$$

має вид (випадок, коли всі три сигнали – взаємно неортогональні, синхронні за тактовими точками та апріорі рівноймовірні за станами їх інформаційних ДП – $p(r_{1,2,3} = 0) = p(r_{1,2,3} = 1) = 0{,}5$ [3]):

$$r_1^* = rect(-K_0 thb_1 - K_{12} \cdot thb_2 - K_{13} \cdot thb_3 - K_{23} \cdot thb_1 \cdot thb_2 \cdot thb_3);$$
$$rect(x \geq 0) = 1; \quad rect(x < 0) = 0. \tag{2}$$

Тут

$$K_0 = 1 - th2R_{12} th2R_{13} th2R_{23};$$
$$K_{12} = -th2R_{12} + th2R_{13} th2R_{23};$$
$$K_{13} = -th2R_{13} + th2R_{12} th2R_{23};$$
$$K_{23} = -th2R_{23} + th2R_{12} th2R_{13}.$$

Далі,

$$b_i = \frac{2}{N_0} \int_{t_{k-1}}^{t_k} y_t s_i(t) dt; \quad R_{ij} = \frac{1}{N_0} \int_{t_{k-1}}^{t_k} s_i(t) s_j(t) dt = \rho_{ij} \sqrt{h_i^2 h_j^2};$$
$$\rho_{ij} \in (0,1]; \quad h_i^2 = \frac{1}{N_0} \int_{t_{k-1}}^{t_k} s_i^2(t) dt; \quad i, j \in \{1,2,3\}, \; i \neq j. \tag{3}$$

Відповідно, $t_k - t_{k-1} = T$ – інформаційний тактовий інтервал.

Якщо в спостереженні (1) сигналів лише 2 ($(i = \overline{1,2}$), то досить складне ППР (2) радикально спрощується:

$$r_1^* = rect(-thb_1 + thb_2 th2R_{12}), \tag{4}$$

або

$$r_1^* = rect\left[-b_1 + Arth\left(thb_2 th2R_{12}\right)\right].$$

Якщо в спостереженні (1) другий і третій сигнали – взаємно ортогональні ($R_{23} = 0$), маємо також суттєве спрощення ППР (2):

$$r_1^* = rect(-thb_1 + thb_2 th2R_{12} + thb_3 th2R_{13} + thb_1 thb_2 thb_3 th2R_{12} th2R_{13}),$$

або (застосовуючи перетворення, що не впливають на знак аргументу ППР):

$$r_1^* = rect[-b_1 + Arth(thb_2 th2R_{12}) + Arth(thb_3 th2R_{13})]. \tag{5}$$

За умови, що перший та другий сигнали один одному не заважають ($R_{12} = 0$), маємо:

$$r_1^* = rect(-thb_1 + thb_3 th2R_{13} - thb_2 th2R_{13} th2R_{23} + thb_1 thb_2 thb_3 th2R_{23}),$$

або, вважаючи перший та другий взаємно ортогональні сигнали корисними:

$$r_i^* = rect\left\{-b_i + Arth\left[th2R_{i3} th\left(b_3 - Arth(thb_{3-i} th\, 2R_{3-i;3})\right]\right)\right]\right\}, \quad i = \overline{1,2}. \tag{6}$$

За умови, що в спостереженні (1) першому сигналу заважає лише другий ($R_{13} = 0$), якому заважає лише третій, ППР (2) також редуціюється:

$$r_1^* = rect(-thb_1 + thb_2 th2R_{12} + thb_3 th2R_{12} th2R_{23} + thb_1 thb_2 thb_3 th2R_{12} th2R_{23}),$$

або (перетворюючи аргумент ППР без впливу на його знак):

$$r_1^* = rect\{-b_1 + Arth[th2R_{12}th(b_2 - Arth(thb_3 th2R_{23}))]\}. \quad (7)$$

ППР (5)–(7) за необхідності по індукції піддаються узагальненню на довільну кількість взаємно неортогональних сигналів за тих самих умов.

Тобто, в наведених прикладах, коли деякі сполучення сигналів є взаємно ортогональними, вдається уникнути експоненціального зростання складності залежно від загальної кількості сигналів, що підлягають розділенню. Однак зазначимо, що вищенаведені приклади відповідають умові синхронізму всіх сигналів за тактовими точками.

Другий метод редукції оптимальних ППР – нехтування впливом сукупностей менш потужних сигналів на більш потужні. Це можливо за умови, що будь-які пари сигналів відрізняються за потужністю не менш ніж на 6 дБ [3; 9–11]. Із результатів аналізу відомо, що в таких умовах завадостійкість більш потужних сигналів буде приблизно дорівнювати завадостійкості найменш потужного, при виділенні якого вплив більш потужних буде усуватись згідно з оптимальним ППР.

Можна показати, що навіть при такому підході до редукції алгоритмів розділення-демодуляції взаємно неортогональних сигналів BPSK їх складність (кількість ланцюгів компенсації) буде суттєво залежати від наявності взаємного синхронізму за тактовими точками:

Таблиця 1

Складність алгоритмів розділення-демодуляції
залежно від взаємного синхронізму сигналів за тактовими точками

N сигн.	2	3	4	5	6
K синхр.	1	3	6	10	15
K асинхр.	2	8	20	40	70

У таблиці 1 *N* сигн. – кількість взаємно неортогональних сигналів, *K* синхр. та *K* асинхр. – кількість ланцюгів компенсації за умов синхронізму або асинхронізму сигналів за тактовими точками відповідно. В загальному випадку:

$$K \text{ синхр.} = \sum_{i=2}^{\text{N сигн.}} (i-1); \qquad K \text{ асинхр.} = \sum_{i=2}^{\text{N сигн.}} i(i-1).$$

Виконаємо перетворення, що спрощує аргумент ППР (2). При цьому будемо застосовувати операції, що не впливають на його знак як такий, що лише він визначає прийняття рішень r_1^*. Введемо обмежуючі умови:

$$h_3^2 = 4h_2^2 = 16h_1^2; \quad \rho = 1; \quad h_1^2 >> 1. \quad (8)$$

Вимога відміни в миттєвих потужностях між сигналами в 6 дБ обумовлена тим, що ефективне розділення-демодуляція взаємно неортогональних ЦС можливе лише за такої відміни. Якщо нерівнопотужних сигналів – *N*, то треба, щоб виконувались умови (див. графіки в [3, с. 163–165]):

$$2\sum_{i=1}^{k-1}\sqrt{h_i^2} \le \sqrt{h_k^2}; \quad k = \overline{2, N}.$$

Окрім того, далі будемо застосовувати наближення $th(x) \approx sign(x); sign(x \geq 0) = 1;$ $sign(x < 0) = -1$, що є виправданим за умов (8).

Представимо попередньо ППР (2) у вигляді:

$$r_1^* = rect[-thb_1(K_0 + K_{23} \cdot thb_2 \cdot thb_3) - K_{12}thb_2 - K_{13}thb_3] =$$

$$= rect\left[-b_1 - Arth\frac{K_{12} \cdot thb_2 + K_{13} \cdot thb_3}{K_0 + K_{23} \cdot thb_2 \cdot thb_3}\right]. \quad (9)$$

Таке перетворення є припустимим, якщо знаменник у (9) є позитивним. Для цього представимо його в еквівалентній формі:

$$K_0 + K_{23} \cdot thb_2 \cdot thb_3 = \left(1 - thb_2thb_3th2R_{23}\right)\left(1 + thb_2thb_3th2R_{12}th2R_{13}\right) +$$

$$+ th2R_{12}th2R_{13}th2R_{23}\left(th^2b_2th^2b_3 - 1\right).$$

Тобто, представлення (9) в усякому разі можна застосовувати так:

$$r_1^* = rect\left[-b_1 - Arth\frac{K_{12} \cdot signb_2 + K_{13} \cdot signb_3}{K_0 + K_{23} \cdot signb_2 \cdot signb_3}\right]. \quad (10)$$

Покажемо також, що у загальному випадку знаменник аргументу ППР (9) завжди є позитивним. Для цього знайдемо його похідну за складеною змінною thb_2thb_3 і прирівняємо до нуля:

$$(K_0 + K_{23} \cdot thb_2 \cdot thb_3)'_{thb_2 \cdot thb_3} = th2R_{23} - th2R_{12}th2R_{13} = 0.$$

Звідси $th2R_{23} = th2R_{12}th2R_{13} = \alpha$.

Підставимо рішення в знаменник (9):

$$K_0 + K_{23} \cdot thb_2 \cdot thb_3 = (1 - \alpha thb_2thb_3)(1 + \alpha thb_2thb_3) + \alpha^2(th^2b_2th^2b_3 - 1) =$$
$$= 1 - \alpha^2 > 0.$$

Водночас спрощене представлення (10) цілком виправдане, тому що найслабшим тут запропоновано перший сигнал, а другий та третій відрізняються на 6 та 12 дБ в бік збільшення відповідно, а прийнятними для користувача вимоги до ймовірності помилки представляються не гірше 10^{-3}. Тобто, очікувані відношення сигнал/шум $h_2^2, h_3^2 \gg 1$, і, як наслідок, можемо припустити $thb_{2,3} \approx signb_{2,3}$. В [12] доведено, що при демодуляції-розділенні двох взаємно неортогональних сигналів таке наближення в аргументі ППР призводить до збільшення зони пониженої завадостійкості орієнтовно в межах $(1{,}5 \div 2)$ *дБ*.

З метою подальшої редукції ППР (10) покажемо, що за умов (8) можна також припустити, що $K_{23}/K_0 \approx K_{12}K_{13}/K_0^2$. Дійсно,

$$K_{12}K_{13} = th2R_{23}(-th^2 2R_{12} - th^2 2R_{13} + th2R_{12}th2R_{13}th2R_{23}) + th2R_{12}th2R_{13} \cong$$

$$\cong -th2R_{23}(2 - th2R_{12}th2R_{13}th2R_{23}) + th2R_{12}th2R_{13} \cong$$

$$\cong -th2R_{23} + th2R_{12}th2R_{13} = K_{23}.$$

Далі,

$$K_0^2 = 1 - 2th2R_{12}th2R_{13}th2R_{23} + th^2 2R_{12}th^2 2R_{13}th^2 2R_{23} =$$

$$= 1 - th2R_{12}th2R_{13}th2R_{23}(2 - th2R_{12}th2R_{13}th2R_{23}) \cong$$

$$\cong 1 - th2R_{12}th2R_{13}th2R_{23} = K_0.$$

За таких припущень ППР (10) перепишеться так:

$$r_1^* = rect\left[-b_1 - Arth\frac{(K_{12}/K_0)\cdot signb_2 + (K_{13}/K_0)\cdot signb_3}{1 + (K_{12}K_{13}/K_0^2)\cdot signb_2 \cdot signb_3}\right] =$$

$$= rect\begin{bmatrix} -b_1 + Arth\left(signb_2\dfrac{th2R_{12} - th2R_{13}th2R_{23}}{1 - th2R_{12}th2R_{13}th2R_{23}}\right) + \\ \\ +Arth\left(signb_3\dfrac{th2R_{13} - th2R_{12}th2R_{23}}{1 - th2R_{12}th2R_{13}th2R_{23}}\right) \end{bmatrix} =$$

$$= rect\begin{bmatrix} -b_1 + signb_2[2R_{12} - Arth(th2R_{13}th2R_{23})] + \\ +signb_3[2R_{13} - Arth(th2R_{12}th2R_{23})] \end{bmatrix}. \qquad (11)$$

Одержане тут редуційоване ППР (11), як буде продемонстровано нижче, потребує додаткового пояснення. Справа в наступному. Якщо взаємно неортогональних сигналів – лише два, то рішення $r_{1,2}^* = \overline{0,1}$; щодо значень ДП кожного з них можна приймати одночасно. Якщо ж сигналів більше двох, то ні оптимальне ППР (2), ні його редуційований варіант (10) працювати не будуть. Наприклад, у випадку, який тут розглядається, якщо не усувати вплив найбільш потужного, третього сигналу на другий, то за ймовірністю (враховуючи присутність в моделі спостереження впливу АБГШ) будемо мати: $r_2^* \equiv r_3^*$.

Пояснимо це твердження. Дійсно, величини на виходах кореляторів кожного з трьох сигналів (див. (3)) за умов (8) і нехтування впливом АБГШ матимуть вигляд:

$$b_1 \simeq (-1)^{r_1}2h_1^2 + (-1)^{r_2}4h_1^2 + (-1)^{r_3}8h_1^2;$$

$$b_2 \simeq (-1)^{r_1}4h_1^2 + (-1)^{r_2}8h_1^2 + (-1)^{r_3}16h_1^2;$$

$$b_3 \simeq (-1)^{r_1}8h_1^2 + (-1)^{r_2}16h_1^2 + (-1)^{r_3}32h_1^2. \qquad (12)$$

А тоді, очевидно, якщо не усувати насамперед вплив найбільш потужного сигналу, завжди будемо мати $r_2^* = signb_2 = signb_3$. Однак якщо потурбуватись за прийняття рішень r_3^* раніше за прийняття рішень r_2^* і попередньо усунути вплив третього, найбільш потужного сигналу на другий, нехтуючи при цьому найменш потужним, першим (поклавши $R_{12} = R_{13} = 0$), то з ППР (2) маємо:

$$r_2^* = rect[-b_2 + signb_3 \cdot 2R_{23}].$$

В результаті, за додаткових спрощень (згідно з (3) $R_{12}, R_{13}, R_{23} > 0$)

$$Arth(th2R_{12}th2R_{13}) \cong 2R_{12};\ Arth\big(th2R_{13}th2R_{23} \cong 2R_{23,}\big),$$

які у нашому прикладі ініційовані можливістю прозорого фізичного трактування, остаточно маємо:

$$r_1^* = rect[-b_1 + (2R_{12} - 2R_{13})sign(b_2 - 2R_{23}signb_3) + (2R_{13} - 2R_{23})signb_3]. \quad (13)$$

Можна побачити, що в нашому прикладі за умов (8) ППР (13) з урахуванням (12) набуває прозорого для фізичного трактування вигляду (рис. 1):

$$r_1^* = rect[-b_1 - 2R_{12} \cdot sign(b_2 - 2R_{23} \cdot signb_3) - 2R_{13} \cdot signb_3]. \quad (14)$$

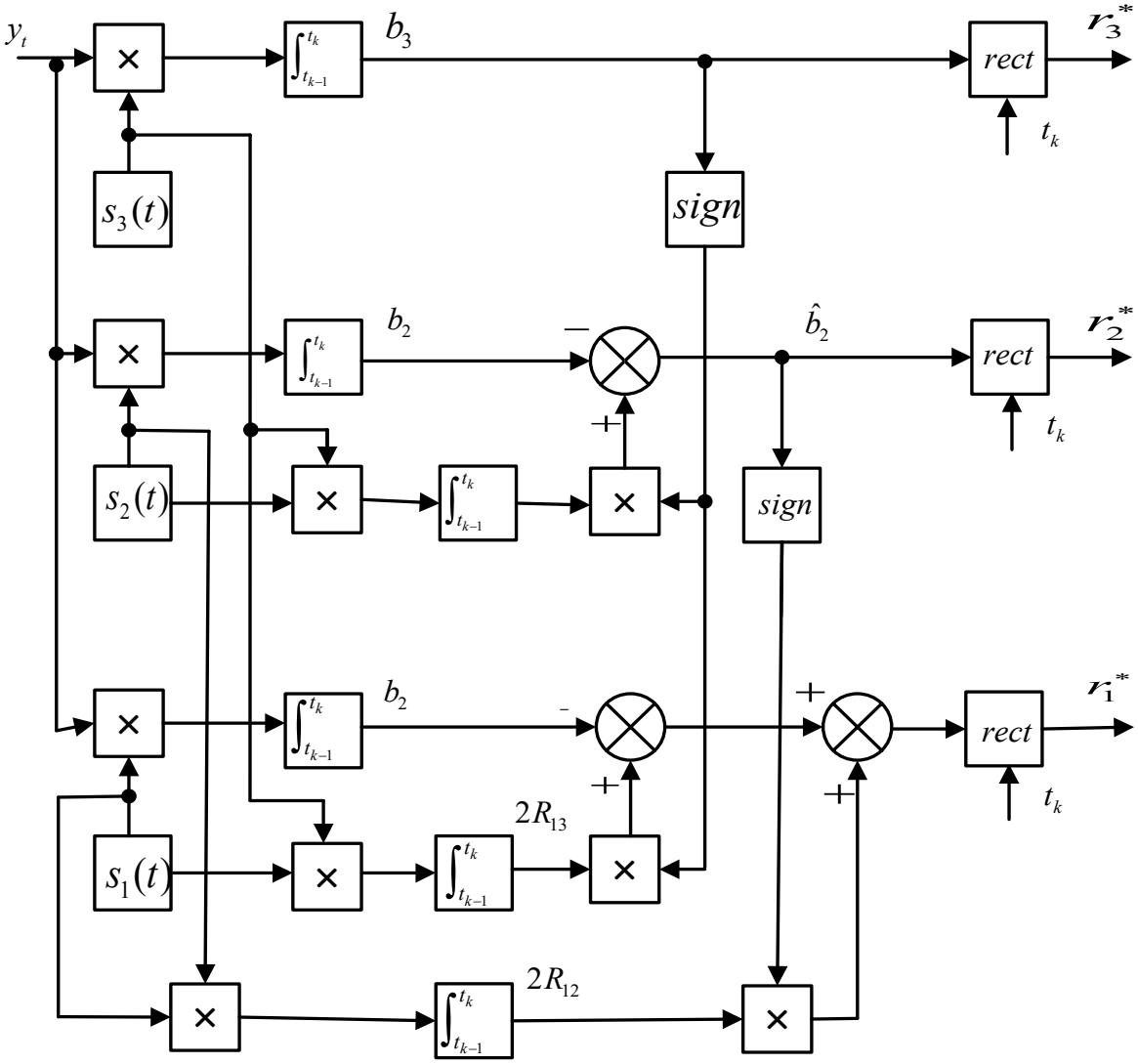


Рис. 1. Підоптимальний алгоритм розділення-демодуляції трьох синхронних нерівнопотужних сигналів BPSK

Або, за позначень (8):

$$r_1^* = rect[-b_1 - 4h_1^2 \cdot sign(b_2 - 16h_1^2 \cdot signb_3) - 8h_1^2 \cdot signb_3]. \quad (15)$$

По індукції можна одержати низку ППР для найслабкішого першого сигналу – наприклад, коли нерівнопотужних сигналів – чотири:

$$r_1^* = rect\begin{Bmatrix} -b_1 - 2R_{12} \cdot sign[b_2 - 2R_{23} \cdot sign(b_3 - 2R_{34} signb_4) - 2R_{24} signb_4] - \\ -2R_{13} \cdot sign(b_3 - 2R_{34} signb_4) - 2R_{14} signb_4 \end{Bmatrix}.$$

З метою демонстрації роботоспроможності редуційованого алгоритму (14) та його представлення (15) за позначень (12) складемо таблицю 2.

Таблиця 2

Таблиця перевірки роботоспроможності редуційованого алгоритму (14)

№	r_1	r_2	r_3	b_1	b_2	b_3	sign$b_{1,2,3}$	r_3^*
1	0	0	0	$2h_1^2 + 4h_1^2 + 8h_1^2 = 14h_1^2$	$4h_1^2 + 8h_1^2 + 16h_1^2 = 28h_1^2$	$8h_1^2 + 16h_1^2 + 32h_1^2 = 56h_1^2$	1	0
2	0	0	1	$2h_1^2 + 4h_1^2 - 8h_1^2 = -2h_1^2$	$4h_1^2 + 8h_1^2 - 16h_1^2 = -4h_1^2$	$8h_1^2 + 16h_1^2 - 32h_1^2 = -8h_1^2$	-1	1
3	0	1	0	$2h_1^2 - 4h_1^2 + 8h_1^2 = 6h_1^2$	$4h_1^2 - 8h_1^2 + 16h_1^2 = 12h_1^2$	$8h_1^2 - 16h_1^2 + 32h_1^2 = 24h_1^2$	1	0
4	0	1	1	$2h_1^2 - 4h_1^2 - 8h_1^2 = -10h_1^2$	$4h_1^2 - 8h_1^2 - 16h_1^2 = -20h_1^2$	$8h_1^2 - 16h_1^2 - 32h_1^2 = -40h_1^2$	-1	1
5	1	0	0	$-2h_1^2 + 4h_1^2 + 8h_1^2 = 10h_1^2$	$-4h_1^2 + 8h_1^2 + 16h_1^2 = 20h_1^2$	$-8h_1^2 + 16h_1^2 + 32h_1^2 = 40h_1^2$	1	0
6	1	0	1	$-2h_1^2 + 4h_1^2 - 8h_1^2 = -6h_1^2$	$-4h_1^2 + 8h_1^2 - 16h_1^2 = -12h_1^2$	$-8h_1^2 + 16h_1^2 - 32h_1^2 = -24h_1^2$	-1	1
7	1	1	0	$-2h_1^2 - 4h_1^2 + 8h_1^2 = 2h_1^2$	$-4h_1^2 - 8h_1^2 + 16h_1^2 = 4h_1^2$	$-8h_1^2 - 16h_1^2 + 32h_1^2 = 8h_1^2$	1	0
8	1	1	1	$-2h_1^2 - 4h_1^2 - 8h_1^2 = -14h_1^2$	$-4h_1^2 - 8h_1^2 - 16h_1^2 = -28h_1^2$	$-8h_1^2 - 16h_1^2 - 32h_1^2 = -56h_1^2$	-1	1

№	$-b_2 + 16h_1^2 \cdot signb_3$	r_2^*	$4h_1^2 \times sign(b_2 - 16h_1^2 \cdot signb_3)$	$8h_1^2 \cdot signb_3$	$-b_1 - 8h_1^2 \cdot signb_3 - 4h_1^2 \times \times sign(b_2 - 16h_1^2 \cdot signb_3)$	r_1^*
1	$-28h_1^2 + 16h_1^2 = -12h_1^2$	0	$-4h_1^2$	$8h_1^2$	$-14h_1^2 + 4h_1^2 + 8h_1^2 = -2h_1^2$	0
2	$4h_1^2 - 16h_1^2 = -12h_1^2$	0	$-4h_1^2$	$-8h_1^2$	$2h_1^2 + 4h_1^2 - 8h_1^2 = -2h_1^2$	0
3	$-12h_1^2 + 16h_1^2 = 4h_1^2$	1	$4h_1^2$	$8h_1^2$	$6h_1^2 - 4h_1^2 + 8h_1^2 = -2h_1^2$	0
4	$20h_1^2 - 16h_1^2 = 4h_1^2$	1	$4h_1^2$	$-8h_1^2$	$10h_1^2 - 4h_1^2 - 8h_1^2 = -2h_1^2$	0
5	$-20h_1^2 + 16h_1^2 = -4h_1^2$	0	$-4h_1^2$	$8h_1^2$	$-10h_1^2 + 4h_1^2 + 8h_1^2 = 2h_1^2$	1
6	$12h_1^2 - 16h_1^2 = -4h_1^2$	0	$-4h_1^2$	$-8h_1^2$	$6h_1^2 + 4h_1^2 - 8h_1^2 = 2h_1^2$	1
7	$-4h_1^2 + 16h_1^2 = 12h_1^2$	1	$4h_1^2$	$8h_1^2$	$-2h_1^2 - 4h_1^2 + 8h_1^2 = 2h_1^2$	1
8	$28h_1^2 - 16h_1^2 = 12h_1^2$	1	$4h_1^2$	$-8h_1^2$	$14h_1^2 - 4h_1^2 - 8h_1^2 = 2h_1^2$	1

Із такої, суттєво редуційованої форми оптимального ППР (2) витікає, що за наявності вже трьох нерівнопотужних взаємно неортогональних ЦС спочатку треба незалежно приймати рішення r_3^*, потім, компенсуючи вплив найпотужнішого сигналу, приймати рішення r_2^*, і в останню чергу – рішення r_1^* щодо значення ДП найменш потужного сигналу.

Слід зазначити, що вихідне ППР (2) хоча і синтезоване за критерієм мінімуму ймовірності помилки в оцінці ДП будь-якого з трьох сигналів (наведений приклад (2) – для першого), тобто, належить до алгоритмів, оптимальних за одним із критеріїв Maximum Likelihood (ML), принцип послідовного усунення взаємного впливу – такий само, як і в Successive Interference Cancellation (SIC) [7; 8 та ін.].

Зміст таблиці 2 підтверджує принципову роботоспроможність редуційованого ППР (14)–(15), одержаного напівевристично, за досить грубих спрощень. Таке рішення можна пропонувати лише за виконання умов (8). Зазначимо тут, що в такому разі "прозорість" ППР (14) досягнута за рахунок нехтування аналітично складним впливом випадкових величин b_1 і b_2 на випадкову величину b_3. Процедура компенсації впливу на величину b_2 величини b_1 також спростована на підставі тих самих умов.

Тепер розглянемо важливий для практики випадок, коли три взаємно неортогональні сигнали BPSK є довільно асинхронними за тактовими точками. Аналітична модель спостереження (1) узагальнюється до вигляду (рис. 2):

$$y_t = (-1)^{r_1^{k-2}} s_1[t \in t_{k-3} + \tau_1 + \tau_2, t_{k-2} + \tau_1 + \tau_2)] + \\ + \sum_{j=0}^{1} (-1)^{r_2^{k-2+j}} s_2\left[t \in t_{k-3+j} + \tau_1, t_{k-2+j} + \tau_1\right)] + \\ + \sum_{j=0}^{2} (-1)^{r_2^{k-2+j}} s_3\left[t \in t_{k-3+j}, t_{k-2+j}\right)] + n(t); \quad (16)$$

$$r_{1,2,3} = \overline{0,1}; k = 3, 4, 5 \ldots$$

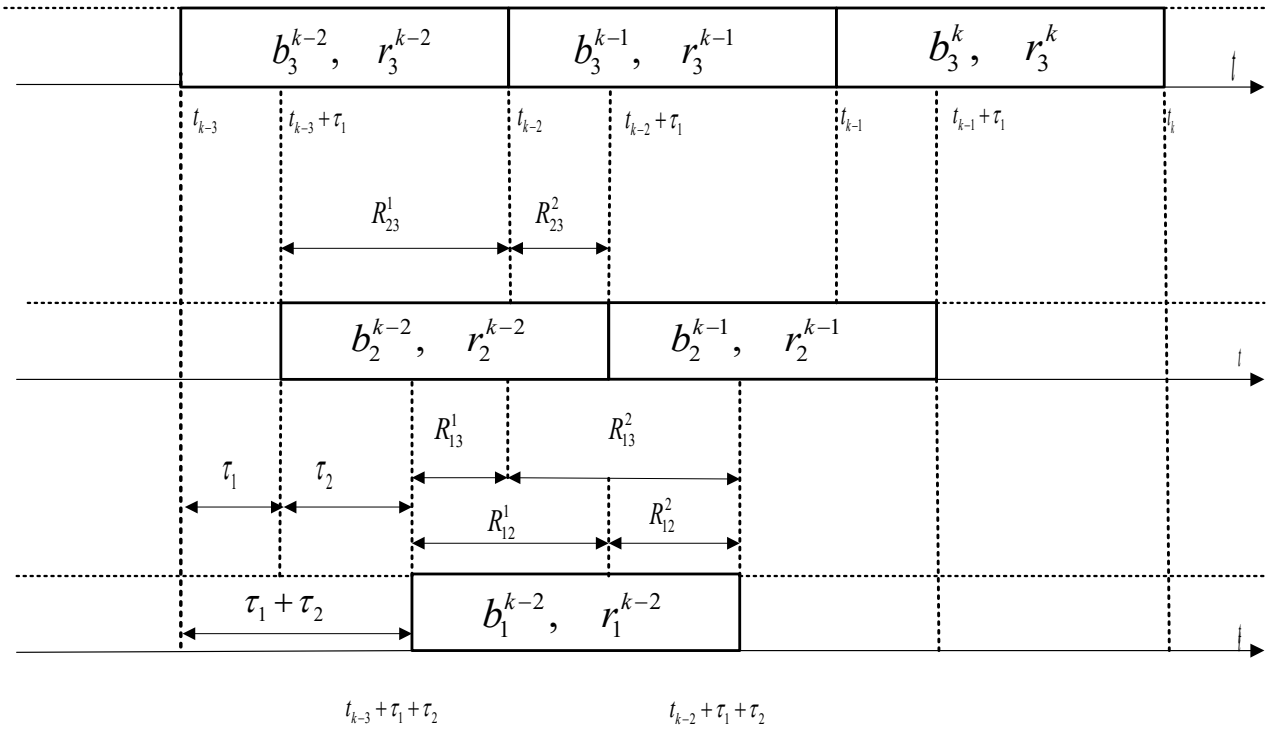


Рис. 2. Графічне представлення моделі (16) – три асинхронні сигнали BPSK

За умов (8), впливом першого найменш потужного на більш потужніші другий і третій сигнали та впливом середнього за потужністю другого сигналу на третій, як було обумовлено вище, можна знехтувати. Тоді по індукції маємо спрощені ППР для випадку взаємного асинхронізму за тактовими точками у вигляді (вважаємо R_{ij} незмінними в часі):

$$r_1^{*k-2} = rect\begin{Bmatrix} -b_1^{k-2} + Arth\Big[th\Big(b_2^{k-2} - Arth\Big(thb_3^{k-2}th2R_{23}^1\Big) - Arth\Big(thb_3^{k-1}th2R_{23}^2\Big)\Big)th2R_{12}^1\Big] + \\ +Arth\Big[th\Big(b_2^{k-1} - Arth\Big(thb_3^{k-1}th2R_{23}^1\Big) - Arth\Big(thb_3^{k}th2R_{23}^2\Big)\Big)th2R_{12}^2\Big] + \\ +Arth\Big(thb_3^{k-2}th2R_{13}^1\Big) + Arth\Big(thb_3^{k-1}th2R_{13}^2\Big) \end{Bmatrix};$$

$$r_2^{*k-2+j} = rect\Big[-b_2^{k-2+j} + Arth\Big(thb_3^{k-2+j}th2R_{23}^1\Big) + Arth\Big(thb_3^{k-1+j}th2R_{23}^2\Big)\Big], \quad j = \overline{0,1}; \tag{17}$$

$$r_3^{*k-2+j} = rect\Big(-b_3^{k-2+j}\Big), \quad j = \overline{0,2}.$$

Тут згідно з рисунками 3, *а*, 3, *б*:

$$\begin{aligned} b_1^{k-2} &= \frac{2}{N_0}\int\limits_{t_{k-3}+\tau_1+\tau_2}^{t_{k-2}+\tau_1+\tau_2} y_t s_1(t)dt; \\ b_2^{k-2+j} &= \frac{2}{N_0}\int\limits_{t_{k-2+j}+\tau_1}^{t_{k-1+j}+\tau_1} y_t s_2(t)dt, \quad j = \overline{0,1}; \quad b_3^{k-2+j} = \frac{2}{N_0}\int\limits_{t_{k-2+j}}^{t_{k-1+j}} y_t s_2(t)dt, \quad j = \overline{0,2}. \end{aligned} \tag{18а}$$

Далі, вважаючи канал стаціонарним:

$$R_{12}^1 = \frac{1}{N_0}\int\limits_{t_{k-3}+\tau_1+\tau_2}^{t_{k-2}+\tau_1} s_1(t)s_2(t)dt, \quad R_{12}^2 = \frac{1}{N_0}\int\limits_{t_{k-2}+\tau_1}^{t_{k-2}+\tau_1+\tau_2} s_1(t)s_2(t)dt;$$

$$R_{13}^1 = \frac{1}{N_0}\int\limits_{t_{k-3}+\tau_1+\tau_2}^{t_{k-2}} s_1(t)s_3(t)dt, \quad R_{13}^2 = \frac{1}{N_0}\int\limits_{t_{k-2}}^{t_{k-2}+\tau_1+\tau_2} s_1(t)s_3(t)dt; \tag{18б}$$

$$R_{23}^1 = \frac{1}{N_0}\int\limits_{t_{k-3}+\tau_1}^{t_{k-2}} s_2(t)s_3(t)dt, \quad R_{23}^2 = \frac{1}{N_0}\int\limits_{t_{k-2}}^{t_{k-2}+\tau_1} s_2(t)s_3(t)dt.$$

Застосовуючи наближення $th(x) \approx sign(x)$; $sign(x \geq 0) = 1$; $sign(x < 0) = -1$, приведемо ППР (17) до вигляду (див. відповідні структурні схеми на рис. 3, *а*, 3, *б*):

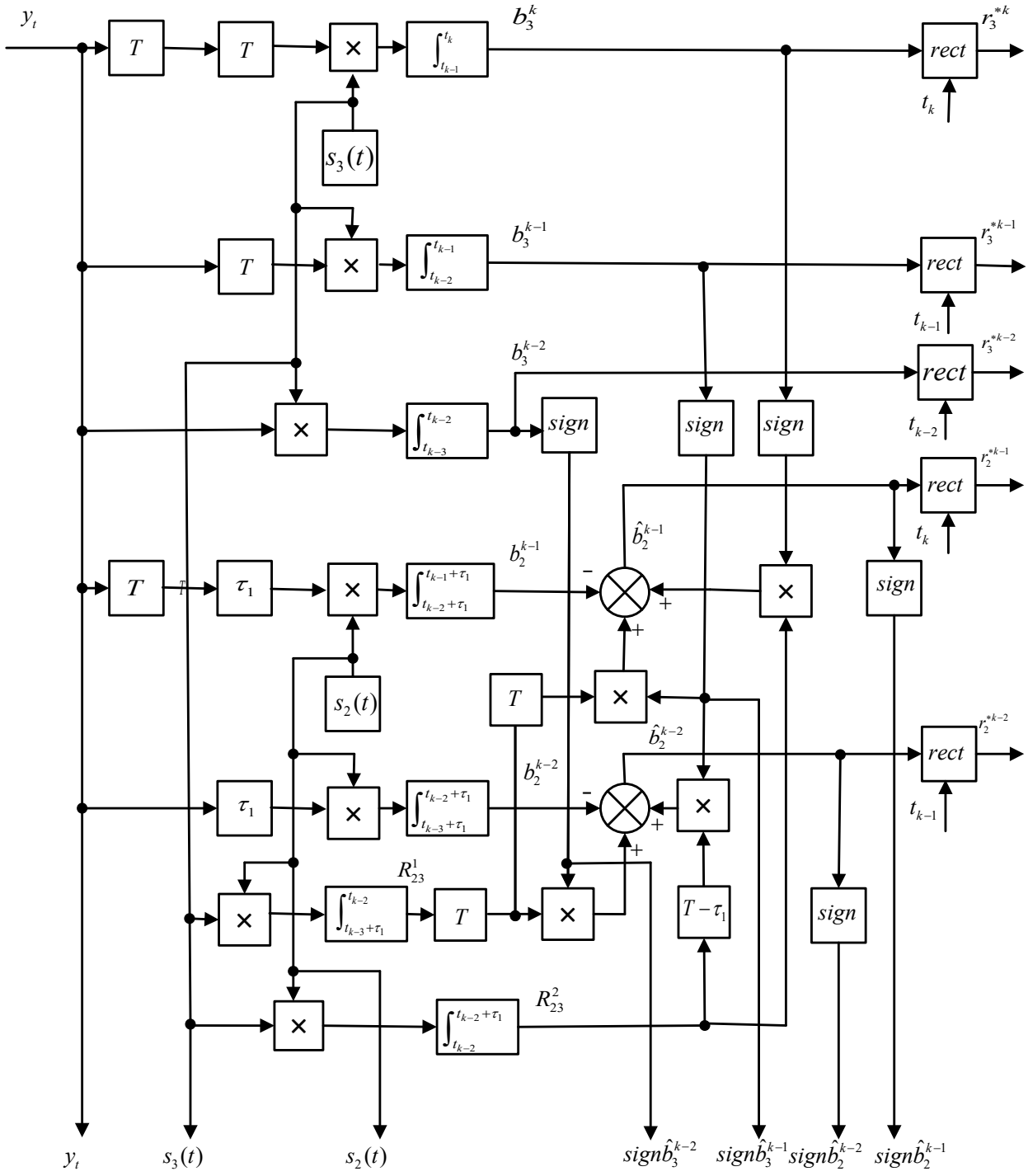


Рис. 3, *а*. Підоптимальний алгоритм розділення трьох асинхронних нерівнопотужних сигналів BPSK (виділення другого та третього сигналів)

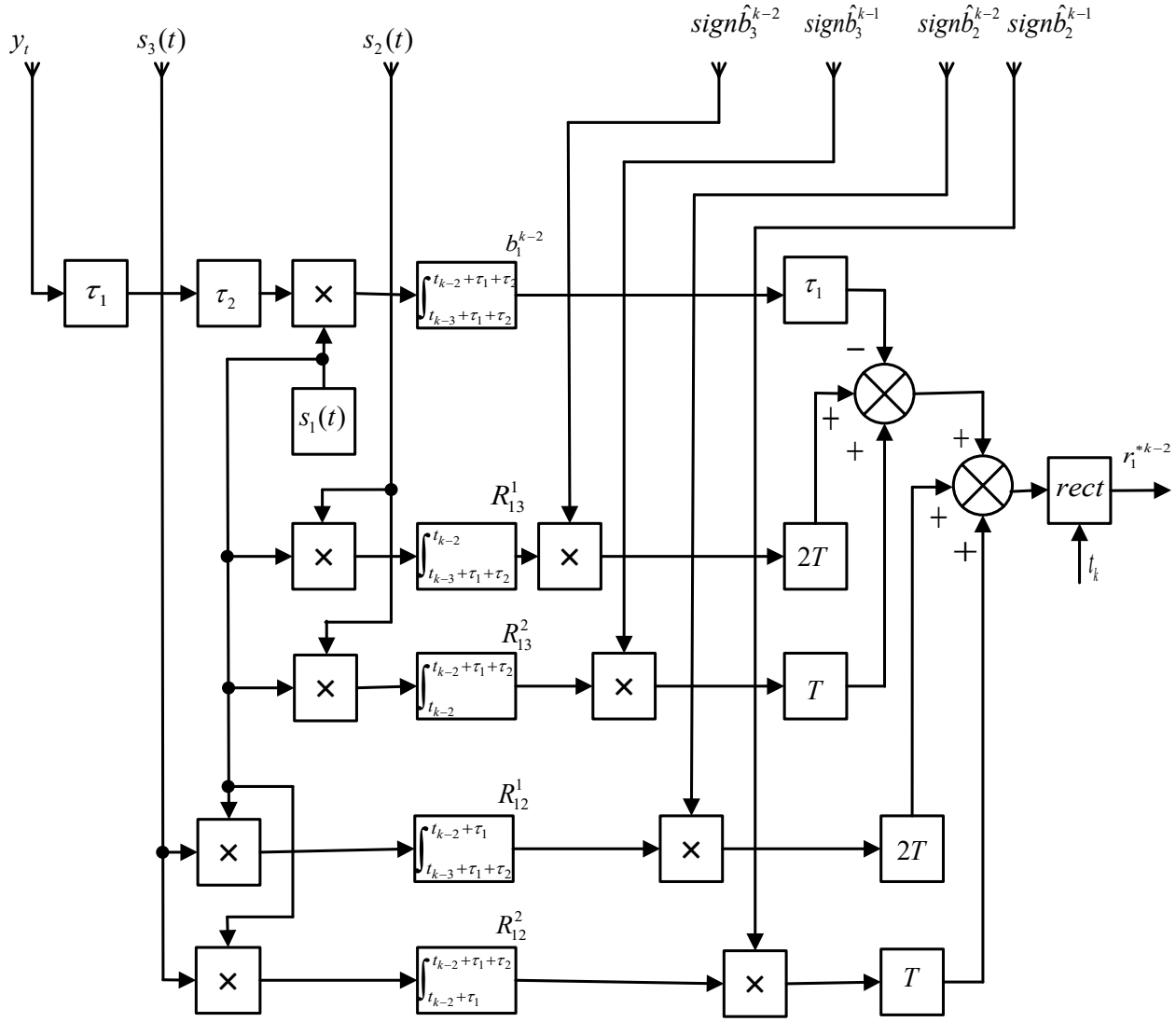


Рис. 3, *б*. Підоптимальний алгоритм розділення трьох асинхронних нерівнопотужних сигналів BPSK (виділення першого сигналу)

$$r_1^{*k-2} = rect\left\{\begin{array}{l} -b_1^{k-2} + 2R_{12}^1 sign\left[b_2^{k-2} - sign\left(b_3^{k-2}\right)2R_{23}^1 - sign\left(b_3^{k-1}\right)2R_{23}^2\right] + \\ \quad + 2R_{12}^2 sign\left[b_2^{k-1} - sign\left(b_3^{k-1}\right)2R_{23}^1 - sign\left(b_3^{k}\right)2R_{23}^2\right] + \\ \quad + sign\left(b_3^{k-2}\right)2R_{13}^1 + sign\left(b_3^{k-1}\right)2R_{13}^2 \end{array}\right\};$$

$$r_2^{*k-2+j} = rect\left[-b_2^{k-2+j} + sign\left(b_3^{k-2+j}\right)2R_{23}^1 + sign\left(b_3^{k-1+j}\right)2R_{23}^2\right], \quad j = \overline{0,1}; \tag{19}$$

$$r_3^{*k-2+j} = rect\left(-b_3^{k-2+j}\right), \quad j = \overline{0,2}.$$

За умови $\tau_1 = \tau_2 = 0$ з (19) у випадку взаємного тактового синхронізму для r_1^* одержуємо наведене раніше ППР (14).

Структурні схеми рисунків 3, *а*, 3, *б* потребують додаткового пояснення. Величини $b_2^{k-2}, R_{23}^1\, R_{23}^2,\ signb_3^{k-2}, signb_3^{k-1}$ зберігаються до моменту прийняття рішення r_2^{*k-2} – до моменту t_{k-1}. Величини $b_2^{k-1}, R_{23}^1\, R_{23}^2, signb_3^{k-1}, signb_3^k$ зберігаються до моменту прийняття рішення r_2^{*k-1} – до моменту t_k. Інтервали формування в часі зазначених величин визначаються виразами (18а), (18б).

2. Оцінювання завадостійкості редуційованих алгоритмів розділення-демодуляції взаємно неортогональних цифрових сигналів

Точний аналіз завадостійкості оптимальних ППР виду (2) вимагає виконання процедур потрійного інтегрування тривимірної гауссівської функції щільності ймовірності зі взаємно залежними межами інтегрування, що визначаються аргументом ППР (2). Якщо ж спостереження має вигляд (16), то процедура обчислення завадостійкості демодуляції першого ЦС навіть із залученням підоптимального ППР (17) потребує принаймні шестивимірного інтегрування, відповідно до кількості взаємно залежних випадкових величин $b_1^{k-1}, b_2^{k-1}, b_2^{k-1}, b_1^{k-2}\ b_3^{k-2}, b_3^{k-1}\ b_3^k$ (див. рис. 2). Водночас, якщо припустити, що при демодуляції найбільш потужного, третього ЦС, компенсація менш потужніших першого та другого згідно з редуційованим ППР (14) не виконується (за умови (8)) і сигнали є взаємно синхронними за тактовими точками (найгірший за завадостійкістю випадок), розрахунки ймовірності помилки $P(r_3^* \neq r_3)$ порівняно з методикою [3] радикально спрощуються:

$$P(r_3^* \neq r_3) = \frac{1}{4}\sum_{r_1=0}^{1}\sum_{r_2=0}^{1}\left\{\overline{F}\left[\sqrt{2h_3^2}\left(1+(-1)^{r_2}\rho_{23}\sqrt{\frac{h_2^2}{h_3^2}}+(-1)^{r_1}\rho_{13}\sqrt{\frac{h_1^2}{h_3^2}}\right)\right]\right\}. \qquad (20а)$$

Далі, припускаючи, що за умов $h_3^2 \geq 4h_2^2 \geq 16h_1^2 \quad h_1^2 >> 1$, коли вплив найслабкішого, першого сигналу не усувається, а вплив третього, найбільш потужного, ідеально компенсується, можемо записати:

$$P(r_2^* \neq r_2) = \frac{1}{2}\sum_{r_1=0}^{1}\left\{\overline{F}\left[\sqrt{2h_2^2}\left(1+(-1)^{r_1}\rho_{12}\sqrt{\frac{h_1^2}{h_2^2}}\right)\right]\right\}. \qquad (20б)$$

У формулах (20а), (20б) доповнення до інтеграла Лапласа:

$$\overline{F}(x) = 1 - \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} exp\left(-\frac{z^2}{2}\right)dz.$$

Розрахунки також доводять, що тактовий асинхронізм між сигналами внаслідок так званого ефекту самокомпенсації призводить до несуттєвого зменшення ймовірності помилки в оцінці більш потужних другого і третього сигналів – менше, ніж удвічі.

Що стосується обчислень імовірностей помилки $P(r_1^* \neq r_1)$ в оцінці ДП найслабкішого сигналу, то за умови вищезазначеного припущення (8) вплив більш потужних другого і третього сигналів на перший буде ефективно компенсуватись, і можна скористатись відомими результатами [3; 12].

Результати розрахунків за формулами (20а), (20б) та залучені з [3; 12] з метою порівняння наведені в таблиці 3 і на рисунках 4 *а*, 4 *б*. Результати розрахунків, наведені в таблиці 3, виконані для типових на практиці ймовірностей помилки на рівнях 10^{-4} або 10^{-6},

що відповідають значенням $h_1^2 = 8{,}39$ *д Б*; $h_1^2 = 10{,}53$ *д Б* в каналі з АБГШ і без сигналів, що заважають, та для нормованих до одиниці коефіцієнтів неортогональності: $\rho \in \{0{,}5; 0{,}7; 0{,}9\}$.

На графіках рисунків 4 *а*, 4 *б* представлено межі потенційної і класичної кореляційної завадостійкості розділення-демодуляції двох взаємно неортогональних сигналів BPSK. На усіх графіках $l^2 = h_1^2/h_2^2$. Нижні унімодальні неперервні криві (P_1) відповідають межам потенційної завадостійкості першого сигналу, фіксованого за миттєвою потужністю $\left(h_1^2 = 8{,}39 \partial Б,\ h_1^2 = 10{,}53 \partial Б;\quad \rho = 0{,}9\right)$. Монотонні криві $(P_2^{\text{кор}})$, одержані із залученням формули (20б), відповідають завадостійкості другого, змінного за потужністю сигналу, коли компенсація впливу першого не виконується. Тут наведені залежності втрат у потенційній завадостійкості $(\hat{P}_1)$ внаслідок апроксимацій в аргументі ППР (4) виду $th(x)th(y) = sign(x)sign(y)$ – верхні унімодальні неперервні криві. Пунктирні криві в лівій частині рисунків характеризують втрати в завадостійкості внаслідок неточностей оцінювання величин взаємних впливів R_{12} на рівнях ± 1 %; ± 5 %. Характерним є те, що для досягнення приблизно однакової завадостійкості розділення-демодуляції обох сигналів відміна в їх миттєвих потужностях повинна лежати в межах 3–6 дБ, залежно від значень ρ взаємного впливу, а відмова від компенсації впливу менш потужного першого сигналу на другий, більш потужний потребує незначного збільшення цієї відміни лише на $(1 \div 1{,}5)$ *дБ*.

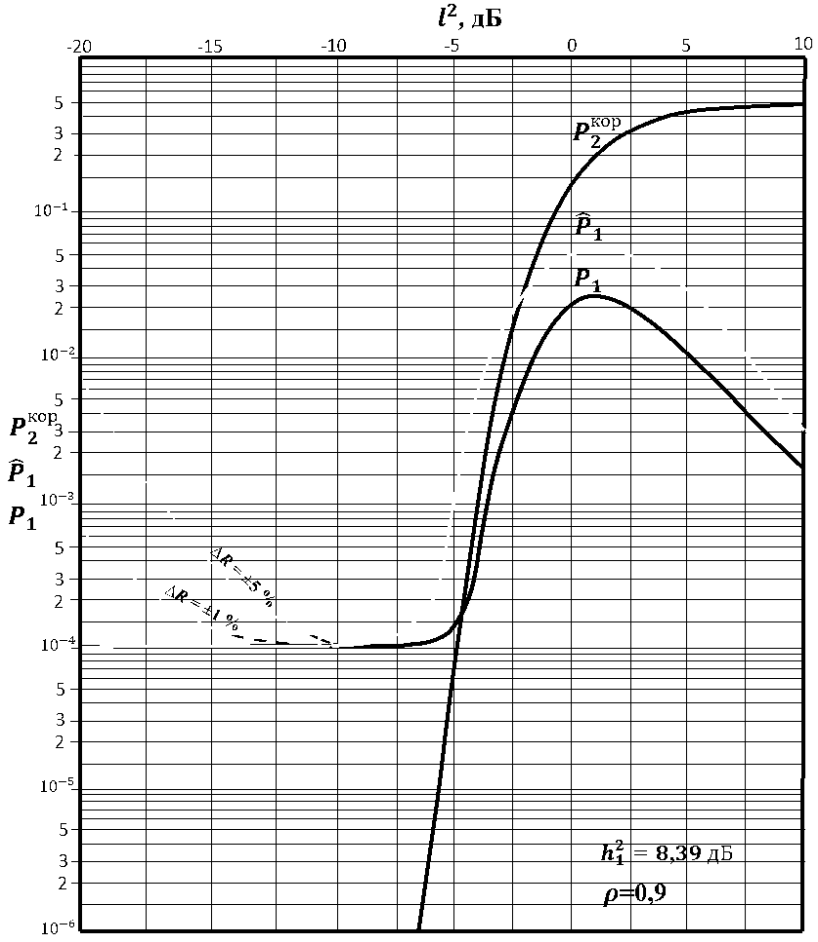


Рис. 4, *а*. Порівняння меж завадостійкості розділення-демодуляції двох взаємно неортогональних сигналів BPSK $(h_1^2 = 8{,}39\ \partial Б, \rho = 0{,}9)$

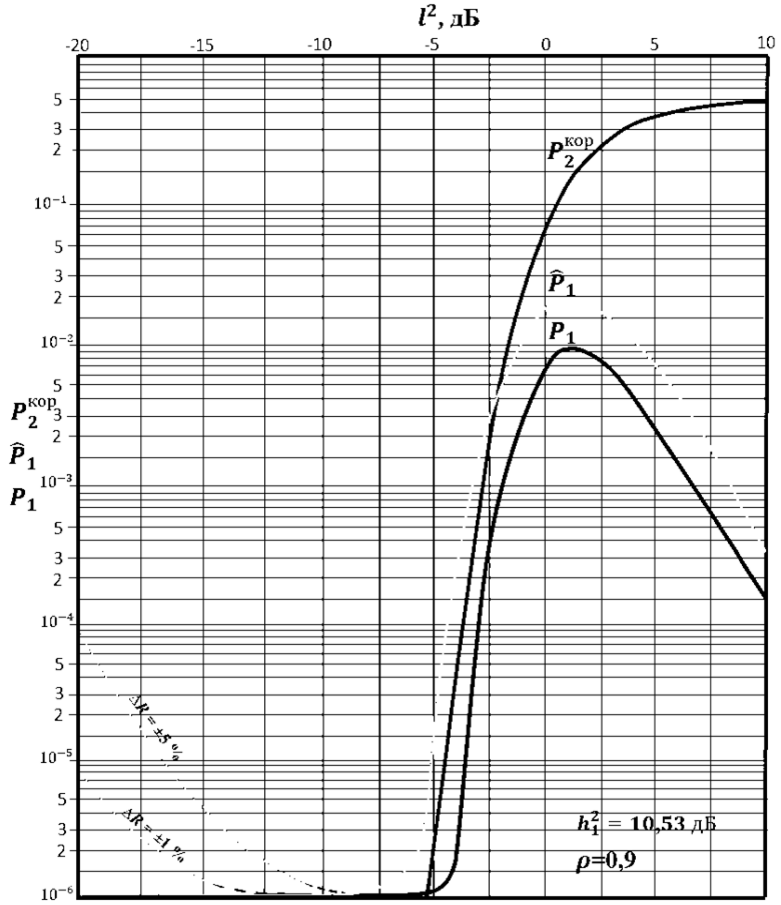


Рис. 4, *б*. Порівняння меж завадостійкості розділення-демодуляції двох взаємно неортогональних сигналів BPSK ($h_1^2 = 10{,}53\ дБ, \rho = 0{,}9$)

У лівій частині таблиці 3 для випадку присутності в спостереженні двох сигналів наведено залежності завадостійкості демодуляції більш потужного сигналу без компенсації впливу першого, менш потужного ($h_1^2 = 8{,}39$ дБ, $h_1^2 = 10{,}53$ дБ; $\rho = 0{,}5; 0{,}7; 0{,}9$).

У правій частині таблиці 3 для випадку присутності в спостереженні трьох сигналів наведено залежності завадостійкості демодуляції більш потужного третього сигналу без компенсації впливу двох менш потужних ($h_1^2 = 8{,}39$ дБ, $10{,}53$ дБ; $h_2^2 = 14{,}39$ дБ, $16{,}53$ дБ, $\rho = 0{,}5; 0{,}7; 0{,}9$).

Із вищенаведених результатів розрахунків витікає, що навіть при оптимальному розділенні взаємно неортогональних сигналів BPSK необхідно забезпечувати відміни в їх миттєвих потужностях в межах 6 дБ, залежно від ступенів взаємної неортогональності (див. рис. 4, *а*, 4, *б*). Як свідчать залежності на цих рисунках, незабезпечення таких відмін в усякому разі є неприйнятним для практичних застосувань – виникає так звана зона пониженої завадостійкості [3; 12], де ефективність розділення-демодуляції взаємно неортогональних сигналів стрімко погіршується. Водночас, за умови забезпечення цих відмін впливом менш потужних сигналів на більш потужні можна нехтувати – це призведе до втрат в енергетиці на одиниці децибел. Відповідна редукція ППР, в свою чергу, суттєво спрощує вихідні оптимальні алгоритми розділення-демодуляції – спостерігається лише лінійне, а не експоненціальне ускладнення редуційованих алгоритмів обробки від кількості взаємно неортогональних сигналів, що підлягають розділенню-демодуляції.

Таблиця 3

Енергетичні витрати на кореляційне виділення сигналів
в редуційованому алгоритмі (14)

N сигн.	2 взаємно неортогональні сигнали BPSK		3 взаємно неортогональні сигнали BPSK	
ρ	$h_1^2 = 8{,}39\ дБ$ $\left(p_1^* = 10^{-4}\right)$	$h_1^2 = 10{,}53\ дБ$ $\left(p_1^* = 10^{-6}\right)$	$h_1^2 = 8{,}39\ дБ$, $h_2^2 = 14{,}39\ дБ$ $\left(p_1^* = p_2^* = 10^{-4}\right)$	$h_1^2 = 10{,}53\ дБ$, $h_2^2 = 16{,}53\ дБ$ $\left(p_1^* = p_2^* = 10^{-6}\right)$
0,5	$h_2^2 = 11{,}7\ дБ$ $\left(p_2^* = 10^{-4}\right)$	$h_2^2 = 12{,}4\ дБ$ $\left(p_2^* = 10^{-4}\right)$	$h_3^2 = 16{,}0\ дБ$ $\left(p_3^* = 10^{-4}\right)$	$h_3^2 = 17{,}4\ дБ$ $\left(p_3^* = 10^{-4}\right)$
	$h_2^2 = 13{,}2\ дБ$ $\left(p_2^* = 10^{-6}\right)$	$h_2^2 = 13{,}9\ дБ$ $\left(p_2^* = 10^{-6}\right)$	$h_3^2 = 17{,}0\ дБ$ $\left(p_3^* = 10^{-6}\right)$	$h_3^2 = 18{,}2\ дБ$ $\left(p_3^* = 10^{-6}\right)$
0,7	$h_2^2 = 12{,}8\ дБ$ $\left(p_2^* = 10^{-4}\right)$	$h_2^2 = 13{,}7\ дБ$ $\left(p_2^* = 10^{-4}\right)$	$h_3^2 = 18{,}0\ дБ$ $\left(p_3^* = 10^{-4}\right)$	$h_3^2 = 19{,}5\ дБ$ $\left(p_3^* = 10^{-4}\right)$
	$h_2^2 = 14{,}0\ дБ$ $\left(p_2^* = 10^{-6}\right)$	$h_2^2 = 15{,}0\ дБ$ $\left(p_2^* = 10^{-6}\right)$	$h_3^2 = 18{,}8\ дБ$ $\left(p_3^* = 10^{-6}\right)$	$h_3^2 = 20{,}1\ дБ$ $\left(p_3^* = 10^{-6}\right)$
0,9	$h_2^2 = 13{,}8\ дБ$ $\left(p_2^* = 10^{-4}\right)$	$h_2^2 = 14{,}9\ дБ$ $\left(p_2^* = 10^{-4}\right)$	$h_3^2 = 19{,}5\ дБ$ $\left(p_3^* = 10^{-4}\right)$	$h_3^2 = 21{,}1\ дБ$ $\left(p_3^* = 10^{-4}\right)$
	$h_2^2 = 15{,}0\ дБ$ $\left(p_2^* = 10^{-6}\right)$	$h_2^2 = 16{,}0\ дБ$ $\left(p_2^* = 10^{-6}\right)$	$h_3^2 = 20{,}1\ дБ$ $\left(p_3^* = 10^{-6}\right)$	$h_3^2 = 21{,}7\ дБ$ $\left(p_3^* = 10^{-6}\right)$

Висновки. Роботоспроможність алгоритмів розділення-демодуляції взаємно неортогональних ЦС без суттєвих втрат у завадостійкості можна забезпечити за обов'язкової умови певних попарних відмінностей в їхніх миттєвих потужностях між будь-якими їхніми сполуками (в межах 6 дБ, залежно від ступенів неортогональності).

З метою редукції оптимальних ППР слід нехтувати впливом менш потужних ЦС на більш потужні. За такої умови експоненціальна залежність складності алгоритмів розділення-демодуляції взаємно неортогональних ЦС від їх кількості спрощується до лінійно залежної.

Алгоритмічна складність підоптимальних алгоритмів розділення-демодуляції за умов $h_i^2 \gg 1 \ \forall\, i$ може бути додатково зменшена шляхом найпростіших апроксимацій виду $thx \approx signx$ в складових аргументів ППР.

Асинхронізм за тактовими точками від 3 до 6 нерівноенергетичних взаємно неортогональних сигналів, що підлягають розділенню-демодуляції, призводить до приблизно лінійно залежного ускладнення редуційованих алгоритмів в 3–5 разів – залежно від кількості таких сигналів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Verdu S. Multiuser Detection. Cambridge University, 1998. 452 p.

2. Michael L. Honig. Advanced in Multiuser Detection. Northwestern University, 2009. 492 p.

3. Єрохін В. Ф. Випадковий множинний доступ при розв'язанні конфліктів на фізичному рівні: навч. посіб. Київ: ІС33І НТУУ «КПІ», 2014. 296 с.

4. Єрохін В., Вакуленко О. Еволюція алгоритмів оптимального розділення двох взаємно неортогональних сигналів двійкової фазової модуляції. *Збірник наукових праць «Information Technology and Sequrity»*. 2022. Vol. 10, Iss. 1 (18). P. 83–97.

5. Dai L., Wang B., Yuan Y., Han S., I C.-L., Wang Z. Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends. *IEEE Commun. Mag*. Sept. 2015. Vol. 53, No. 9. P. 74–81.

6. Wang Y., Ren B., Sun S., Kang S., Yue X. Analysis of nonorthogonal multiple access for 5G. *China Communications*. 2016. Vol. 13, No Supplement 2. P. 52–66.

7. Islam S. M. R., Avazov N., Dobre O. A., Kwak K. S. Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges. *IEEE Commun. Surveys Tuts*. 2017. Vol. 19, No. 2. P. 721–742.

8. Kokilavani M., Siddharth R., Mohamed Riuaz S., Parameswaran Ramesh., Ezhilarasi S., P.T.V. Bhuvaneswari. Downlink Performance Analysis of 5G PD-NOMA System. *IEEE Global Conference on Computing, Power and Communication Technologies (GlobComPT)*. India Habitat Centre, Lodhi Road, New Delhi, India, Sep. 23–25, 2022.

9. Wang Ch.-L., Chen J.-Y., Chen Y.-J. Power Allocation for a Downlink Non-Orthogonal Multiple Access System. *IEEE Wireless VOLUME XX, 2017 2*. Citation information: DOI Communications Letters. Vol. 5. No. 5. P. 532–535. DOI: 10.1109/LWC.2016.2598833.

10. Wei Zh., Ng D. W. K., Yuan J. Power-Efficient Resource Allocation for MC-NOMA with Statistical Channel State Information. *Proc. of 2016 IEEE Global Communications Conference (GLOBECOM)*. Washington, DC, USA. Dec. 2016. P. 1–7. DOI: 10.1109/GLOCOM.2016.7842161.

11. Faeik Al R., Davaslioglu K., Gitlin R. The optimum received power levels of uplink non-orthogonal multiple access (NOMA) signals. *IEEE 18th Wireless and Microwave Technology Conference (WAMICON)*. 2017. P. 1–4.

12. Єрохін В. Ф. Демодуляція конфліктуючих цифрових сигналів. Київ: КВІУЗ – Інститут кібернетики ім. В. М. Глушкова АН України. 1993. 133 с.

DOI: 10.58254/viti.8.2025.06.79

УДК 004.8+004.49

канд. техн. наук Залужний О. В. ORCID: 0000-0002-8722-4087 (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ ВПЛИВУ МЕТОДІВ ВІДБОРУ ОЗНАК НА ЕФЕКТИВНІСТЬ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК

Об'єми даних, що використовуються для навчання моделей машинного навчання систем кіберзахисту, часто вимірюються в гігабайтах та містять десятки ознак, які можуть приймати сотні тисяч значень, окрім того, дані постійно оновлюються та поповнюються в процесі функціонування систем. Збільшення об'єму даних призводить до виникнення певних проблем, серед яких збільшення часу на навчання та тестування моделі, прокляття вимірності, малі вибірки, зашумлені або надмірні ознаки, а також упереджені дані. Відбір ознак (Feature Selection) є фундаментальним для розв'язання таких проблем.

Метою статті є дослідження впливу методів відбору ознак на якість класифікації кібератак моделями машинного навчання для визначення найбільш ефективних підходів до формування набору ознак.

У статті наведено короткий опис та проведено дослідження ефективності використання відомих методів відбору ознак таких як: кореляційний метод, метод на основі статистичного критерію χ^2, статистичний метод ANOVA, метод на основі розрахунку взаємної інформації, метод ReliefF, метод на основі генетичного алгоритму та метод рекурсивного відбору ознак.

Оцінка ефективності методів відбору ознак здійснювалась в поєднанні з різними методами машинного навчання за такими критеріями, як повнота, точність, точність класифікації та параметром F2-scor. Окрім того, в статті наведені графіки залежності кількості пропущених атак і хибних спрацювань від кількості ознак для кожного із досліджуваних методів.

Експериментальні дослідження проведено з використанням інструментів Python та бібліотеки scikit-learn. Вони показали, що застосування методів відбору ознак покращує показники якості роботи моделей машинного навчання та зменшити час на їх навчання. Ефективність кожного із методів залежить від об'єму даних, який потрібно опрацювати, методів машинного навчання з якими використовуються ті чи інші методи відбору ознак, часових та обчислювальних обмежень. Використання алгоритму з χ^2, методів ANOVA та Mutual Information Filter в моделі, що побудована на основі випадкового лісу, дозволяє отримати кращі результати ніж генетичний алгоритм та рекурсивне вилучення ознак. Проте, останні у поєднанні з методом k найближчих сусідів є найефективнішими з усіх досліджуваних комбінацій методів відбору ознак та методів машинного навчання за кількістю детектованих атак та хибних спрацювань.

Ключові слова: *кібербезпека, виявлення кібератак, методи машинного навчання, методи відбору ознак, зменшення розмірності, кореляційний метод відбору ознак, статистичні методи відбору ознак, генетичний алгоритм, рекурсивного вилучення ознак.*

O. Zaluzhnyi. Study on the impact of feature selection methods on the performance of machine learning models in cyberattack detection

Data volumes used to train machine learning models for cyber security systems are often measured in gigabytes and contain dozens of features that can take hundreds of thousands of values. Also, the data is constantly updated and replenished during the operation of the systems. The increase in data volume leads to certain problems, including increased model training and testing time, the curse of dimensionality, small sample sizes, noisy or redundant features, and biased data. Feature selection is fundamental to solving such kinds of problems.

The purpose of this article is to study the impact of feature selection methods on the quality of cyberattack classification by machine learning models in order to determine the most effective approaches to form a features set.

The article provides a brief description and studies the effectiveness of using well-known feature selection methods such as: the correlation method, the method based on the χ^2 statistical criterion, the ANOVA statistical method, the method based on mutual information calculation, the ReliefF method, the method based on a genetic algorithm, and the recursive feature selection method.

The effectiveness of feature selection methods was evaluated in combination with various machine learning methods according to criteria such as Recall, Precision, Accuracy, and F2-score. In addition, the article provides graphs showing the dependence of the missed attacks number and false positives on the number of features for each method.

Experimental studies were conducted using Python and the scikit-learn library. They showed that the feature selection methods' usage improves the machine learning models performance and reduces the time required for their training. The effectiveness of each method depends on the data amount to be processed, the machine learning methods with which certain feature selection methods are used, and time and computational constraints. Using the χ^2 algorithm, ANOVA methods, and Mutual Information Filter in a model based on random forest allows for better results than Genetic Algorithm and Recursive feature elimination. However, the latter, in combination with the k-Nearest Neighbours method, are the most effective of all the

combinations of feature selection methods and machine learning methods studied in terms of the number of detected attacks and false positives.

Keywords: *cybersecurity, cyberattack detection, machine learning methods, feature selection methods, dimensionality reduction, correlation feature selection method, statistical feature selection methods, genetic algorithm, recursive feature elimination.*

Постановка проблеми

Сучасні тенденції розвитку систем кіберзахисту пов'язані з широким застосуванням технологій машинного навчання (МН) для виявлення і запобігання кіберзагрозам. Об'єми даних, що використовуються для навчання моделей часто вимірюються в гігабайтах та містять десятки ознак (Features), які приймають сотні тисяч значень, окрім того дані постійно оновлюються та поповнюються в процесі функціонування систем кіберзахисту. Збільшення об'єму даних призводить до виникнення певних проблем, серед яких збільшення часу на навчання та тестування моделі, прокляття вимірності, малі вибірки, зашумлені або надмірні ознаки, а також упереджені дані. Відбір ознак (Feature Selection) є фундаментальним для розв'язання таких проблем, оскільки відомо, що дозволяє покращити часові показники роботи моделей МН, підвищити повноту та точності прийнятих ними рішень.

Аналіз останніх досліджень і публікацій

Застосування методів машинного навчання в системах кіберзахисту зумовило значний прогрес у сфері виявлення і запобігання кіберзагрозам. Опубліковані численні наукові статті, в яких досліджуються різні підходи та алгоритми для підвищення ефективності таких систем. Зокрема, у роботі [1] проаналізовано результати провідних досліджень, що присвячені виявленню програм-вимагачів за допомогою алгоритмів машинного навчання та глибокого навчання, де зокрема значна увага приділяється підходам до відбору релевантних ознак.

У роботі [2] було проведено ґрунтовні дослідження моделей машинного навчання для виявлення шкідливого програмного забезпечення (ШПЗ), що побудовані з використанням різних методів машинного навчання. Автори підкреслили важливість відбору релевантних ознак для підвищення ефективності детектування ШПЗ, проте не проводили аналізу різних методів відбору ознак.

У статті [3] запропоновано метод відбору ознак на основі ансамблю із чотирьох методів: Information Gain (IG - інформаційний виграш), Gain Ratio (відносний інформаційний виграш), хі-квадрат та алгоритм ReliefF. Досліджено його ефективність для детектування атак типу "розподілена відмова в обслуговуванні" (DDoS). Для аналізу продуктивності системи було використано набір даних NSL-KDD в якому зменшено кількість ознак із 41 до 13 та навчено модель машинного навчання, де використано алгоритм класифікації який побудований на основі дерева рішень.

У роботі [4] запропоновано новий підхід до класифікації шкідливого програмного забезпечення за допомогою методу k-найближчих сусідів (k-Nearest Neighbors, KNN) в поєднанні з середовищем Cuckoo (відокремлене середовище, "пісочниця", для динамічного аналізу та спостереження за поведінкою неперевіреного або потенційно шкідливого коду без ризику для цілісності основної системи). Для автоматизованого відбору ознак запропоновано використання алгоритму Boruta, який побудований на основі алгоритму класифікації випадковий ліс.

Дослідження, що проведені в [5], свідчать про ефективність використання для відбору ознак, при багатокласовій класифікації, методів що ґрунтуються на взаємній інформації.

У роботі [6] автори застосували генетичний алгоритм (Genetic Algorithm, GA) у поєднанні з обгорткою логістичної регресії для відбору ознак у наборах даних UNSW-N15 та KDDCup99, що використовуються при виявленні мережевих вторгнень. Результати досліджень показали, що у поєднанні з класифікатором дерево рішень такий підхід дозволяє правильно виявляти 81,42 % мережевих вторгнень, при цьому хибні спрацювання становлять 6,39 % (було відібрано 20 ознак з 42 у датасеті UNSW-NB15). Що до датасету KDDCup99, то

такий підхід показав результат виявлення 99,90 % і хибні спрацювання склали 0,105 % для 18 ознак.

В роботі [7] застосовано алгоритм Extreme Gradient Boosting (XGBoost) для відбору релевантних ознак в наборі даних UNSWNB15. Використовуючи зменшений простір ознак було навчено та протестовано моделі машинного навчання, що побудовані на основі методу опорних векторів (support vector machine, SVM), KNN, логістичної регресії, штучної нейронної мережі та дерева рішень. У експериментах було розглянуто як бінарну, так і багатокласову класифікацію. Результати показали, що метод відбору ознак на основі XGBoost дозволяє підвищити точність моделі DecisionTree з 88,13 % до 90,85 % для бінарної класифікації.

Таким чином, аналіз літератури показує, що в сучасних системах кіберзахисту активно використовуються технології машинного навчання. Продуктивність таких систем значною мірою залежить від обраних методів машинного навчання та методів відбору релевантних ознак. Незважаючи на те, що за цією тематикою постійно публікуються нові наукові праці, недостатньо дослідженим залишається напрямок, який пов'язаний із проведенням досліджень ефективності методів відбору ознак в поєднанні з різними методами машинного навчання для розв'язання задач класифікації кібератак.

Метою статті є дослідження впливу методів відбору ознак на якість класифікації кібератак моделями машинного навчання для визначення найбільш ефективних підходів до формування набору ознак.

Виклад основного матеріалу дослідження

Короткий опис датасету

Для проведення досліджень було використано загальнодоступний датасет "Internet of Things network intrusion dataset 20" (IoTID20) [8]. Набір даних IoTID20 сфокусовано на виявленні аномальної активності в мережах IoT, проте в деяких роботах його також використовують для розробки Intrusion Detection System (IDS) [9]. Набір даних IoTID20 складається з 83 ознак, що описують мережеву активність, і трьох ознак, які використовуються для маркування класів або типів подій (мітки). Розподіл міток на бінарні, категорійні та підкатегорійні наведено в таблиці 1[8].

Таблиця 1

Бінарні, категорійні та підкатегорійні мітки датасету IoTID20

Binary	Category	Subcategory
Normal, Anomaly	Normal, DoS, Mirai, MITM, Scan	Normal, Syn Flooding, Brute Force, HTTP Flooding, UDP Flooding ARP Spoofing Host Port, OS

Розподіл зразків у наборі даних IoTID20, який використовується для задач виявлення вторгнень, наведено в таблиці 2 відповідно до трьох рівнів класифікації: бінарного (нормальний трафік/атака), категоріального (основні типи атак), а також підкатегоріального (конкретні підтипи атак).

Таблиця 2

Розподіл безпечних та зловмисних зразків у наборі даних IoTID20

Binary label distribution		Subcategory distribution	
Normal	40073	Type	Instances
Anomaly	585710	Normal	40073
		DoS	59391
Category label distribution		Mirai Ack Flooding	55124

Binary label distribution		Subcategory distribution	
Type	Instances	Mirai Brute force	121181
Normal	40073	Mirai HTTP Flooding	55818
DoS	59391	Mirai UDP Flooding	183554
Mirai	415677	MITM	35377
MITM	35377	Scan Host Port	22192
Scan	75265	Scan Port OS	5307

Короткий опис методів машинного навчання, що використовуються для досліджень

Для тестування ефективності методів відбору ознак були використані відомі методи машинного навчання, а саме: дерево рішень (Decision Tree, DT), випадковий ліс (Random Forest, RF), SVM та KNN.

Метод DT

Структурно проста модель, у якій кожен вузол, зверху вниз, відповідає етапу прийняття рішення. Вибір рішення у вузді здійснюється на основі певних умов наприклад, значень ознаки вибірки під час прогнозування. Кожен кінцевий вузол відповідає певній мітці (класу) до якої веде відповідний шлях у дереві рішень [10]. Алгоритм рекурсивно формує дерево зверху вниз, виконуючи розбиття простору ознак у кожному вузлі на основі певної функції домішок (наприклад, ентропії), оцінюючи при цьому, наскільки кожна ознака сприяє розрізненню класів. Розподіл триває до тих пір, доки це дозволяє підвищити точність розмежування класів або поки у вузлі не залишиться надто мало прикладів для подальшого розбиття. Коли процес завершується, кожен кінцевий вузол відповідає певному класу, який визначається більшістю прикладів, що потрапили до цього вузла під час навчання.

Метод

Random Forest – це ансамблевий алгоритм, який використовує концепцію "колективної мудрості" з метою зменшення дисперсії результатів, що отримані за допомогою окремих класифікаторів. Алгоритм формує сукупність дерев рішень, кожне з яких навчається на різних підвибірках навчальних даних, сформованих методом бутстрепу. Для кожного окремого випадку процес класифікації здійснюється кожним деревом у лісі. А потім прогнозований клас визначається на основі принципу більшості голосів [10].

Метод SVM

Основний принцип SVM полягає у побудові гіперплощини або набору гіперплощин в *n*-вимірному просторі, що розділяють об'єкти за класами з максимально можливою відстанню від гіперплощин до найближчих об'єктів кожного класу. Коли дані не є лінійно роздільними у методі використовують функцію втрат в поєднанні з підходом з м'яким рішенням та L2-регуляризацією [10]. Обчислення класифікатора еквівалентні мінімізації виразу:

$$\left[\frac{1}{n}\sum_{i=1}^{n}\max\left(0,1-y_i(\vec{\omega}\cdot\vec{x}_i-b)\right)\right]+\lambda\left\|\vec{\omega}\right\|^2,$$

де $\vec{\omega}$ – це вектор нормалі до гіперплощини;

$\frac{b}{\left\|\vec{\omega}\right\|}$ – зсув площини від початку координат вздовж $\vec{\omega}$;

n – загальна кількість навчальних зразків усіх класів датасету;

x_i – вектор ознак i-го зразка;

y_i – його клас, що визначає, по який бік від гіперплощини знаходиться цей зразок ($y_i \in \{-1,+1\}$);

λ – коефіцієнт регуляризації (контролює баланс між точністю та узагальненням);

$\|\vec{\omega}\|^2$ – квадрат норми вектора нормалі до гіперплощини.

Метод KNN

Метод KNN є непараметричним алгоритмом, який не обмежений фіксованим числом параметрів. Зазвичай вважають, що цей алгоритм взагалі не має параметрів, а реалізує просту функцію від навчальних даних. Насправді в ньому навіть немає справжнього етапу навчання. Просто на етапі тестування, бажаючи отримати вихід *y* для тестового зразка *x*, шукають в навчальному наборі $\boldsymbol{X}$ k-найближчих сусідів $\boldsymbol{x}$ та визначають його клас на основі більшості їхніх міток. Ця ідея працює для будь-якого виду навчання з учителем, за умови, що можна визначити поняття середньої мітки. У разі класифікації усереднювати можна за унітарними кодовими векторами $\boldsymbol{c}$, у яких $\boldsymbol{c}_y = 1$ і $\boldsymbol{c}_i = 0$ для всіх інших *i*. Середнє за такими векторами можна інтерпретувати, як розподіл імовірності класів. Алгоритм KNN, будучи непараметричним, може досягати дуже високої ємності. Припустімо, наприклад, що є завдання багатокласової класифікації та міра продуктивності з бінарною функцією втрат. У такому разі метод одного найближчого сусіда сходиться до подвоєної байєсівської частоти помилок, коли кількість навчальних прикладів наближається до нескінченності. Перевищення над байєсівською помилкою пов'язане з тим, що випадковим чином вибираємо одного з рівновіддалених сусідів. Якщо кількість навчальних прикладів нескінченна, то у всіх тестових точок $\boldsymbol{x}$ буде нескінченно багато сусідів із навчального набору на нульовій відстані. Якби алгоритм дозволяв сусідам проголосувати, а не вибирав випадкового сусіда, то процедура сходилася б до байєсівської частоти помилок. Висока ємність алгоритму KNN дає змогу отримати гарні результати, якщо є великий навчальний набір. Але за це доводиться розплачуватися високою тривалістю обчислень, а за малого навчального набору алгоритм погано узагальнюється. Одне зі слабких місць алгоритму KNN – невміння зрозуміти, що одна ознака є більше характерною, ніж інша [11].

Короткий опис методів відбору ознак, що використовуються

У роботі досліджувались найбільш поширені фільтраційні методи відбору ознак (англ. filter methods), зокрема: кореляційний метод (Correlation Feature Selection, CFS), метод на основі статистичного критерію χ^2, статистичний метод ANOVA (Analysis of Variance – аналіз дисперсії), метод на основі розрахунку взаємної інформації (Mutual Information Filter, MIF) та метод ReliefF. Серед методів обгортки (wrapper methods) були розглянуті: генетичний алгоритм (Genetic Algorithm, GA), де базовим алгоритмом є дерево рішень **(**DT-GA**)**, а також метод рекурсивного відбору ознак **(**Recursive feature elimination, RFE), у якому базовим алгоритмом також є дерево рішень **(**DT-RFE).

Метод CFS

CFS – це простий алгоритм фільтрації, який ранжує підмножини ознак відповідно до кореляційної евристичної функції оцінки. Функція оцінки зміщена в бік підмножин, що містять ознаки, які сильно корелюють з класом і не корелюють між собою. Нерелевантні ознаки ігноруються, оскільки вони матимуть низьку кореляцію з класом. Надлишкові ознаки слід відсіяти, оскільки вони будуть сильно корелювати з однією або кількома ознаками, що залишилися. Прийнятність ознаки буде залежати від того, наскільки вона прогнозує класи в областях простору зразків, які ще не були передбачені іншими ознаками. Евристична функція оцінки підмножини ознак [12]:

$$\text{Merit}_S = \frac{k \cdot \overline{r_{cf}}}{\sqrt{k + k(k-1) \cdot \overline{r_{ff}}}},$$

де Merit_S – це евристична оцінка підмножини ознак *S*, що містить *k* ознак;

$\overline{r_{cf}}$ – середня кореляція ознака-клас $f \in S$;

$\overline{r_{ff}}$ – середня взаємна кореляції між ознаками в підмножині.

Основна мета – знайти баланс між високою кореляцією ознак з класом, і низькою взаємною кореляцією ознак між собою (тобто мінімізувати надмірність).

Фільтраційний метод на основі статистичного критерію χ^2.

В цьому методі тест χ^2 використовується для оцінки кореляції між ознаками та мітками. Статистичний тест χ^2 має нульову гіпотезу, тобто ознака та мітка є незалежним, проти альтернативної гіпотези, тобто вони є залежними. Нульова гіпотеза відхиляється, коли $\text{p}\left(\chi^2_{df} > \chi^2_{statistic}\right) < \alpha$, де рівень значущості $\alpha = 0{,}05$. В іншому випадку нульова гіпотеза не може бути відхилена [13]. Статистика χ^2 має ступінь вільності *degree of freedom – df*), який розраховується як $df = (r-1)\cdot(c-1)$, де *r* – кількість рядків у контингентній таблиці (ознак), *c* – кількість стовпців (міток) .

Основна ідея тесту χ^2 полягає в тому, щоб порівняти спостережувані значення в даних з теоретично очікуваними значеннями і перевірити, чи пов'язані ці значення між собою. Для розрахунку значення χ^2 створюється контингентна таблиця. Формула статистики χ^2 наступна [13]:

$$\chi^2 = \sum_{i=1}^{r} \sum_{j=1}^{c} \frac{(Q_{i,j} - E_{i,j})^2}{E_{i,j}},$$

де $Q_{i,j}$ – спостережувана частота для чарунки i, j;

$E_{i,j}$ – очікуване значення для чарунки i, j, розраховане за умови незалежності змінних.

Теоретично очікуване значення для чарунки i, j, розраховується як:

$$E_{i,j} = \frac{\sum_{k=1}^{c} O_{i,k} \cdot \sum_{k=1}^{r} O_{k,j}}{N},$$

де $\sum_{k=1}^{c} O_{i,k}$ – сума по рядку *i* (загальна кількість спостережень в категорії *i* змінної *x*);

$\sum_{k=1}^{r} O_{k,j}$ – сума по стовпцю *j* (загальна кількість спостережень в категорії *j* змінної *y*);

N – загальна кількість усіх спостережень.

У дослідженнях проводився розрахунок χ^2 та визначення ймовірності $p\left(\chi^2_{df} > \chi^2_{statistic}\right)$, на основі якої ухвалюється рішення про відхилення або прийняття нульової гіпотези. Після чого здійснювалось ранжування ознак та відбір 15 ознак з найкращими показниками.

Статистичний метод ANOVA

Тест дисперсійного аналізу ANOVA використовується для порівняння середніх значень декількох груп у наборі даних та виявлення статистично значущих відмінностей між середніми значеннями різних груп (класів). Статистика для ANOVA – F-статистика, яка обчислюється за такими етапами [14]:

1. Розрахунок варіації між групами:

1.1. Між сумою квадратів (Between sum of squares, BSS):

$$\mathrm{BSS} = \sum_{j=1}^{k} n_j (\overline{x_j} - \overline{x})^2 ,$$

де $\overline{x_j}$ – середнє значення j-ї групи;

n_j – кількість спостережень у j-й групі;

$\overline{x}$ – загальне середнє значення всіх спостережень.

1.2. Середні квадрати між групами (Between mean squares, BMS):

$$\mathrm{BMS} = \mathrm{BSS}/df ,$$

де $df = degree\ off\ \ freedom = k - 1$ (k – кількість груп).

2. Розрахунок варіації всередині груп:

2.1. Сума квадратів всередині груп (Within sum of squares, WSS):

$$\mathrm{WSS} = \sum_{j=1}^{k} (n_j - 1)\sigma_j^2 ,$$

де σ – середньоквадратичне відхилення.

2.2. Середні квадрати всередині груп (Within mean squares, WMS):

$$\mathrm{WMS} = \mathrm{WSS}/df_w ,$$

де $df_w = N - k$, N – кількість спостережень.

Після обчислення F-статистики ознаки сортуються та обирається k найкращих ознак (з найбільшими значеннями F-статистики) [15].

Метод на основі розрахунку взаємної інформації

Маючи взаємну інформацію, можна кількісно оцінити релевантність ознаки на основі того, скільки інформації вона містить про цільовий клас. Таким чином, ми можемо ранжувати ознаки відповідно до отриманої релевантності. Mutual Information Filter дає зважені результати. Для розрахунку взаємної інформації використовується відомий підхід із теорії інформації, який полягає в тому, щоб визначити скільки інформації одна випадкова змінна має про іншу. Обчислення здійснюють за таким виразом [10]:

$$\mathrm{I}(x; y) = \sum_{i=1}^{n} \sum_{j=1}^{n} \mathrm{P}(x_i, y_j) \cdot \log\left(\frac{\mathrm{P}(x_i, y_j)}{\mathrm{P}(x_i) \cdot \mathrm{p}(y_j)} \right),$$

де n – загальна кількість випадків;

x та y – випадкові величини;

x_i та y_i – i-те значення змінної x та y відповідно;

$P(x_i)$ та $P(y_j)$ – ймовірності появи x_i та y_j;

$P(x_i, y_j)$ – об'єднана ймовірність появи x_i та y_j.

Цей метод розглядає ознаки лише окремо, не враховуючи залежності між ними, і, таким чином, є одновимірним підходом.

Метод ReliefF

ReliefF – це популярний алгоритм для відбору ознак, який оцінює, наскільки кожна ознака сприяє розрізненню об'єктів різних класів. Його основна ідея полягає в наступному: для кожного об'єкта x_i у наборі даних алгоритм шукає k найближчих об'єктів того ж класу (так звані *збіги*), а також k найближчих об'єктів для кожного іншого класу (*промахи*) [10].

Далі ReliefF аналізує, наскільки значення кожної ознаки відрізняється між цільовим об'єктом та його сусідами. Якщо ознака має значну різницю між об'єктами різних класів (промахами), це свідчить про її високу інформативність – її вага збільшується. Натомість, якщо така ж відмінність спостерігається між об'єктами одного класу (*збігами*), це означає, що ознака нестабільна в межах класу – її вага зменшується.

Важливо, що ваги оновлюються з урахуванням ймовірності появи кожного класу у вибірці. Це дозволяє врахувати можливу диспропорцію між класами, завдяки чому всі промахи разом мають вагу, співрозмірну з вагами збігів.

У результаті ReliefF формує вектор ваг ознак, який показує їхню значущість для розділення класів. Ознаки з найвищими вагами можуть бути обрані як найбільш релевантні для побудови моделі.

Метод відбору ознак на основі генетичного алгоритму з обгорткою дерева рішень

Генетичний алгоритм – це еволюційний метод, який імітує природні процеси відбору та спадковості. У контексті відбору ознак кожен індивідуум (рішення) подається бінарним вектором, де 1 означає включення певної ознаки до моделі, а 0 – її відхилення. Початкова популяція складається з випадково згенерованих індивідуумів. Далі кожен з них оцінюється за функцією пристосованості, яка базується на точності класифікації (*balanced accuracy*) моделі дерева рішень, навченої на відповідній підмножині ознак із використанням п'ятикратної перехресної перевірки ($cv = 5$).

У кожному поколінні застосовуються оператори схрещування та мутації для створення нових рішень. Вибір батьків здійснюється за принципом турнірної селекції. Найкращі особини зберігаються в наступному поколінні завдяки механізму елітарності. Таким чином, з покоління в покоління оптимізується якість класифікації на основі отриманої комбінації ознак [16].

Метод RFE

Метод RFE – це обгортковий метод відбору ознак, заснований на їх ранжуванні. Він полягає в тому, що послідовно видаляються менш значущі ознаки, використовуючи алгоритм машинного навчання як ядро моделі. Метод був вперше запропонований Guyon та ін. [17] і реалізований у пакеті scikit-learn [18]. У дослідженнях використано метод RFE в обгортці дерева рішень (DT-RFE).

Блок-схема алгоритму DT-RFE наведена на рисунку 1. Спочатку, до навчального набору даних використовується дерево рішень для обчислення важливості ознак і їх ранжування, потім щоразу видаляються найменш значущі ознаки, а решта ознак використовуються для повторного тестування точності класифікації (Accuracy) за допомогою дерева рішень. Точність класифікації обчислюється ітеративно, поки не будуть переглянуті всі ознаки. Врешті-решт отримується ранжування всіх ознак за точністю класифікації.

Короткий опис критеріїв оцінювання ефективності методів відбору ознак

Для аналізу того, наскільки ефективним є той чи інший методу відбору ознак, у цій роботі використовуються такі критеріїв оцінки якості бінарної класифікації як: Recall, Precision, Accuracy та F-score.

Рис. 1. Блок-схема алгоритму DT-RFE

Accuracy (точність класифікації)

Точність класифікації є відсотком правильних прогнозів серед усіх прогнозів і розраховується за наступним виразом (1) [10]:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}, \tag{1}$$

де TP – кількість істинних позитивних результатів;
TN – кількість істинних негативних результатів;
FP – кількість хибнопозитивних результатів;
FN – кількість хибнонегативних результатів.

Ця метрика приймає значення в межах від нуля до одиниці, де одиниця означає, що всі прогнози правильні, а нуль – навпаки. Точність класифікації легко обчислити, хоча одним з її головних недоліків є те, що вона не є достатньо достовірною, якщо дані занадто незбалансовані (кількість зразків кожного класу суттєво відрізняється). Тому, при дослідженнях метрика Accuracy розраховувалась за наступним виразом [20]:

$$\text{Balanced}-\text{accuracy} = \frac{1}{2}\left(\frac{TP}{TP + FN} + \frac{TN}{TN + FP}\right). \tag{2}$$

Формула (2) дозволяє обчислити збалансовану точність та уникнути завищених оцінок на незбалансованих наборах даних. Збалансоване значення точності класифікації – це макро-середнє (macro-average) значення повноти (recall) за класами. Для збалансованих наборів даних цей показник дорівнює звичайній точності класифікації, що розраховується за формулою (1) [20].

Precision (точність позитивних передбачень)

Точність позитивних передбачень (точність) – це показник, який кількісно визначає, скільки випадків, які прогнозуються як позитивні, насправді є позитивними. Він розраховується за формулою [10; 19]:

$$\text{Precision} = \frac{TP}{TP + FP}.$$

Recall (повнота)

Повнота, також відома як чутливість або частота хибнопозитивних результатів моделі. Це метрика, яка кількісно показує, скільки з фактично позитивних зразків були передбачені як позитивні і описується рівнянням [10; 19]:

$$\text{Recall} = \frac{TP}{TP + FN}.$$

F-score

F-score – це зважене гармонійне середнє значення точності та повноти, причому внесок точності в середнє значення зважується за допомогою певного параметра β. Вона визначається за формулою [10; 19]:

$$\text{F}_\beta - \text{score} = \left(1 + \beta^2\right) \cdot \frac{\text{precision} \cdot \text{recall}}{\left(\beta^2 \cdot \text{precision}\right) + \text{recall}}.$$

Щоб уникнути ділення на нуль, коли точність і повнота дорівнюють нулю, використовується еквівалентна формула [10; 19]:

$$\text{F}_\beta - \text{score} = \frac{\left(1 + \beta^2\right) \cdot TP}{\left(1 + \beta^2\right) \cdot TP + FP + \beta^2 \cdot FN}.$$

Коли $\beta = 2$ значення параметра Recall має у чотири рази більший вплив на F-score ніж Precision, що є особливо важливо для задач виявлення кібератак, де пропуск атаки є значно критичнішим за хибне спрацювання.

Як і точність класифікації так і точність позитивних передбачень, повнота та F-score набувають значень в межах від нуля до одиниці.

Аналіз результатів дослідження

Експериментальні дослідження було проведено з використанням інструментів Python та бібліотеки scikit-learn. Обчислення виконувались на системі з 96 ГБ оперативної пам'яті та двоядерним процесором із тактовою частотою 2,3 ГГц на ядро. Для наборів ознак, отриманих методами без вбудованого механізму ранжування, було проведено додаткову оцінку їх значущості за допомогою Permutation Importance.

В таблиці 3 наведено розраховані підчас досліджень значення часу навчання та тестування моделей МН на повному датасеті та на відібраних 15-ти ознаках, значення параметрів: Balanced Accuracy, Precision, Recall та F2-score.

На рисунках 2–8, *а–г* наведено отримані графіки залежності кількості пропущених кібератак та хибних спрацювань від кількості ознак, де:

а – результати обчислень для моделі МН на основі методу SVM;

б – моделі на основі методу RF;

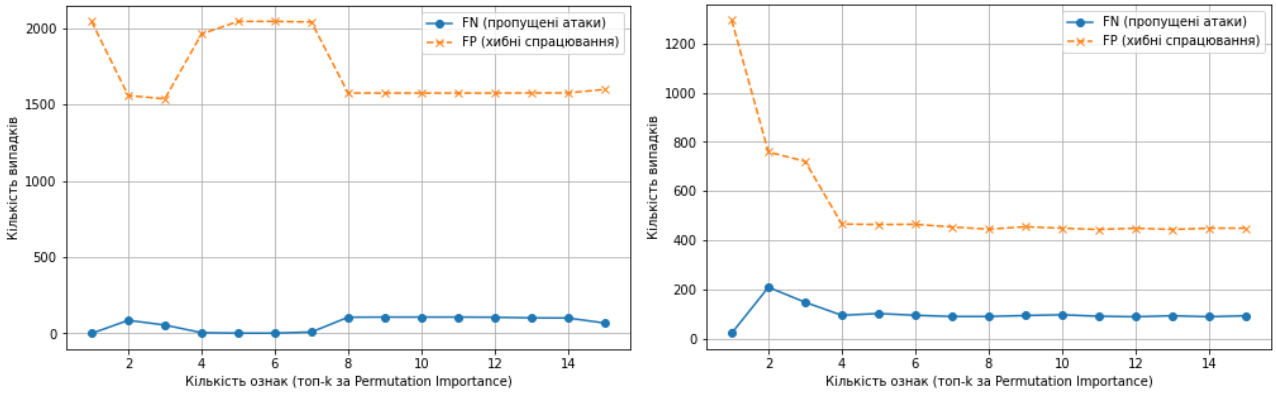
в – моделі на основі методу DT;

г – моделі на основі методу KNN.

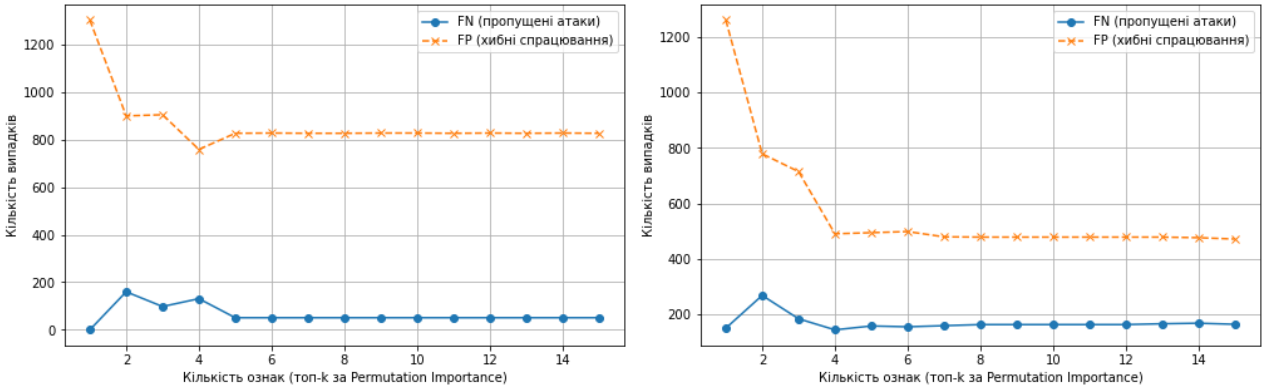
Таблиця 3

Значення показників якості роботи моделей машинного навчання при використанні різних методів відбору ознак

Метод и ML	Параметри оцінки	Усі ознаки	CFS	Алгоритм з χ^2	ANOVA	MIF	Relief	GA	RFE
DT	Час відбору ознак (с)	-	1354	0.06	0.1	32.2	24136	1176	17.9
	Час навчання (с)	0,484	0,078	0,079	0,091	0,185	0,141	0,062	0,152
	Час тестування (с)	0,015	0,01	0,005	0,004	0,005	0,016	0,016	0,004
	Balanced Accuracy	0,965	0,797	0,983	0,983	0,971	0,981	0,965	0,965
	Precision	0,993	0,967	0,981	0,981	0,997	0,984	0,993	0,994
	Recall	0,965	0,797	0,983	0,983	0,971	0,981	0,965	0,965
	F2 score	0,97	0,819	0,983	0,983	0,976	0,981	0,971	0,97
RF	Час навчання (с)	0,672	0,328	0,284	0,313	0,433	0,359	0,219	0,402
	Час тестування (с)	0,063	0,047	0,047	0,064	0,048	0,063	0,031	0,064
	Balanced Accuracy	0,98	0,89	0,991	0,991	0,993	0,986	0,992	0,99
	Precision	0,995	0,966	0,996	0,996	0,999	0,998	0,996	0,999
	Recall	0,98	0,89	0,991	0,991	0,992	0,986	0,992	0,99
	F2 score	0,983	0,903	0,992	0,992	0,994	0,988	0,993	0,992
SVM	Час навчання (с)	74,27	76,72	27,41	173,1	76,83	18,09	19,58	72,94
	Час тестування (с)	40,5	25,73	23,33	21,52	18,87	15,75	18,56	19,17
	Balanced Accuracy	0,635	0,608	0,754	0,753	0,873	0,887	0,893	0,885
	Precision	0,911	0,909	0,82	0,82	0,899	0,872	0,956	0,847
	Recall	0,635	0,608	0,754	0,753	0,873	0,887	0,893	0,885
	F2 score	0,652	0,622	0,764	0,764	0,878	0,884	0,904	0,876
KNN	Час тестування (с)	9,031	4,047	5,741	4,292	2,452	2,422	2,297	2,444
	Balanced Accuracy	0,981	0,882	0,985	0,984	0,989	0,983	0,994	0,99
	Precision	0,988	0,944	0,992	0,992	0,994	0,992	0,995	0,993
	Recall	0,981	0,882	0,985	0,984	0,989	0,983	0,994	0,99
	F2 score	0,982	0,893	0,986	0,986	0,99	0,985	0,994	0,991

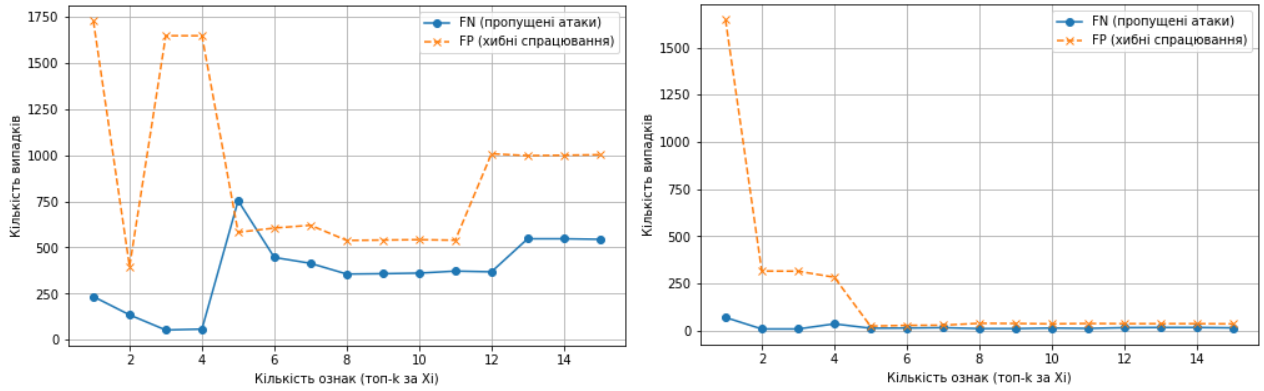


а) *б)*

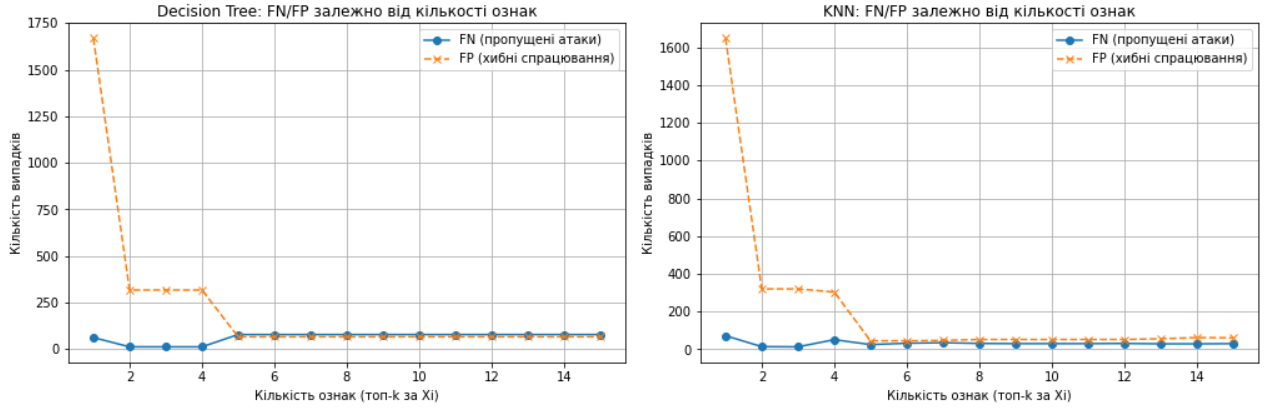


в) *г)*

Рис. 2. Графіки залежності кількості пропущених кібератак та кількості хибних спрацювань від кількості ознак при використанні методу CFS

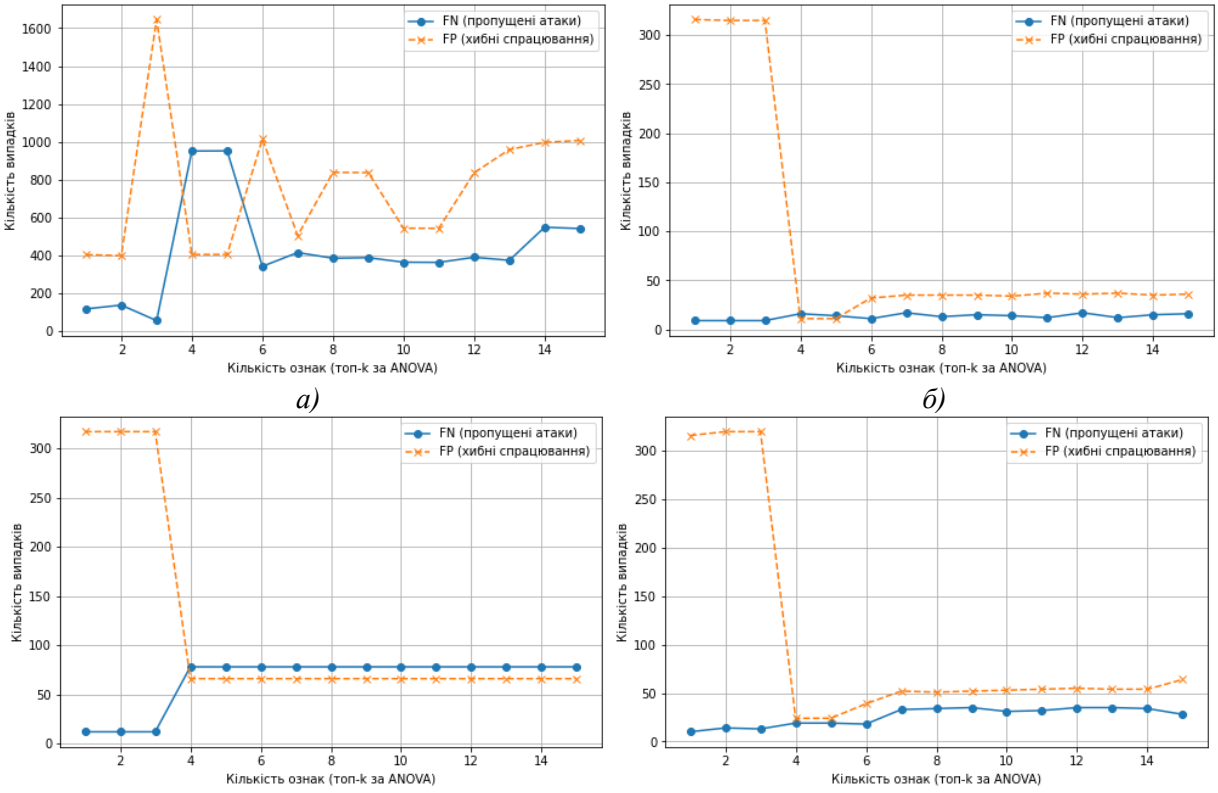


а) *б)*



в) *г)*

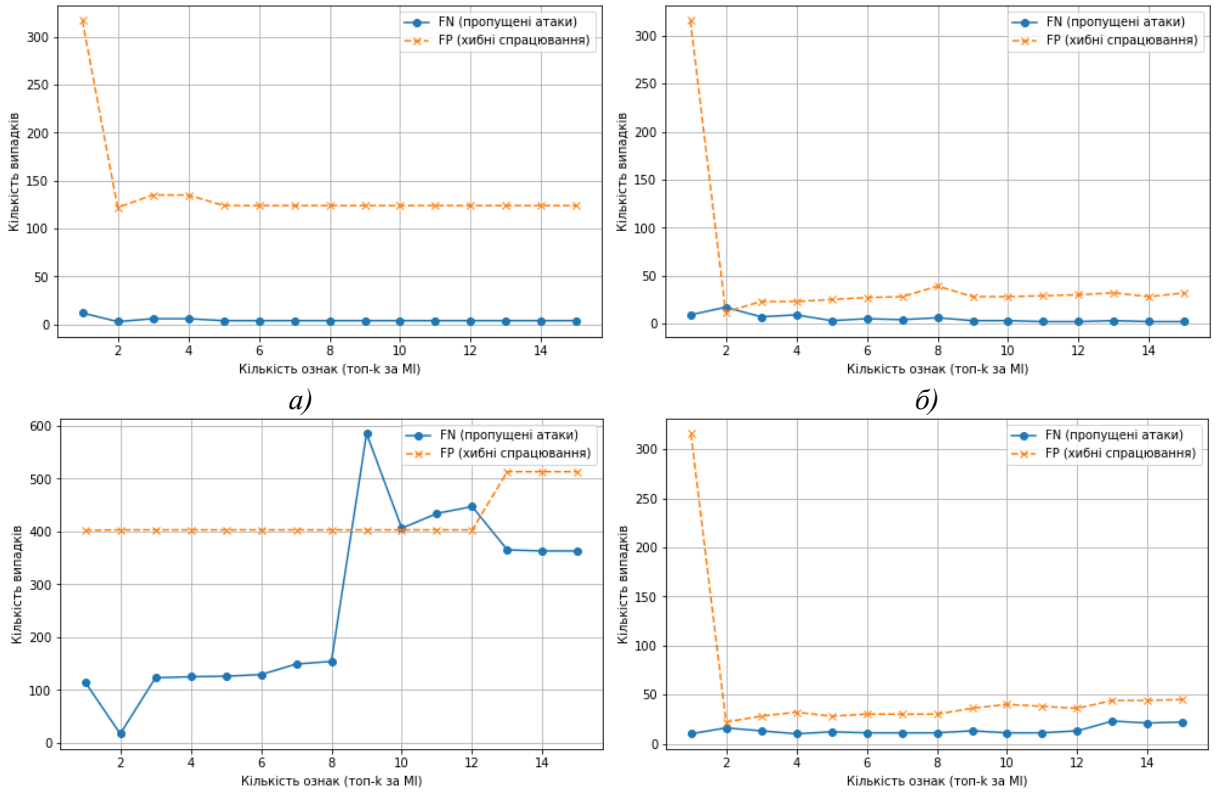
Рис. 3. Графіки залежності кількості пропущених кібератак та кількості хибних спрацювань від кількості ознак при використанні статистичного критерію χ^2



а) *б)*

в) *г)*

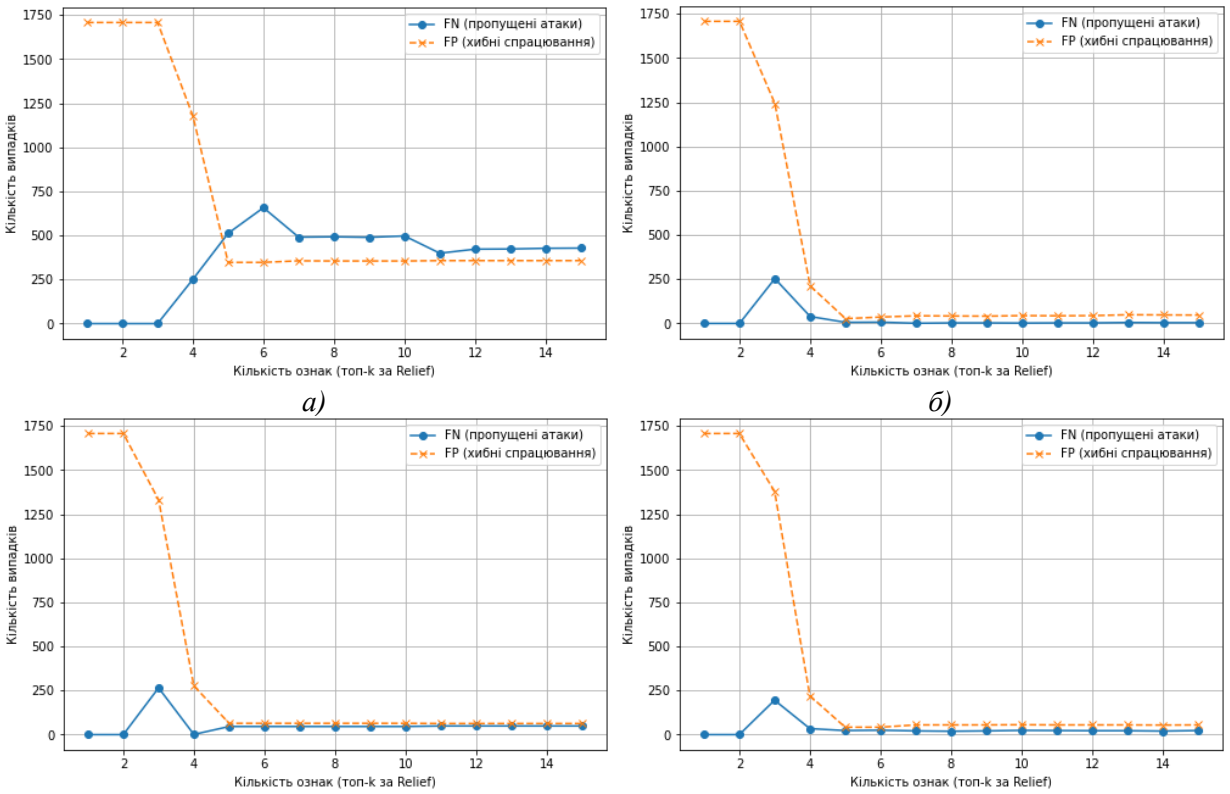
Рис. 4. Графіки залежності кількості пропущених кібератак та кількості хибних спрацювань від кількості ознак при використанні методу ANOVA:



а) *б)*

в) *г)*

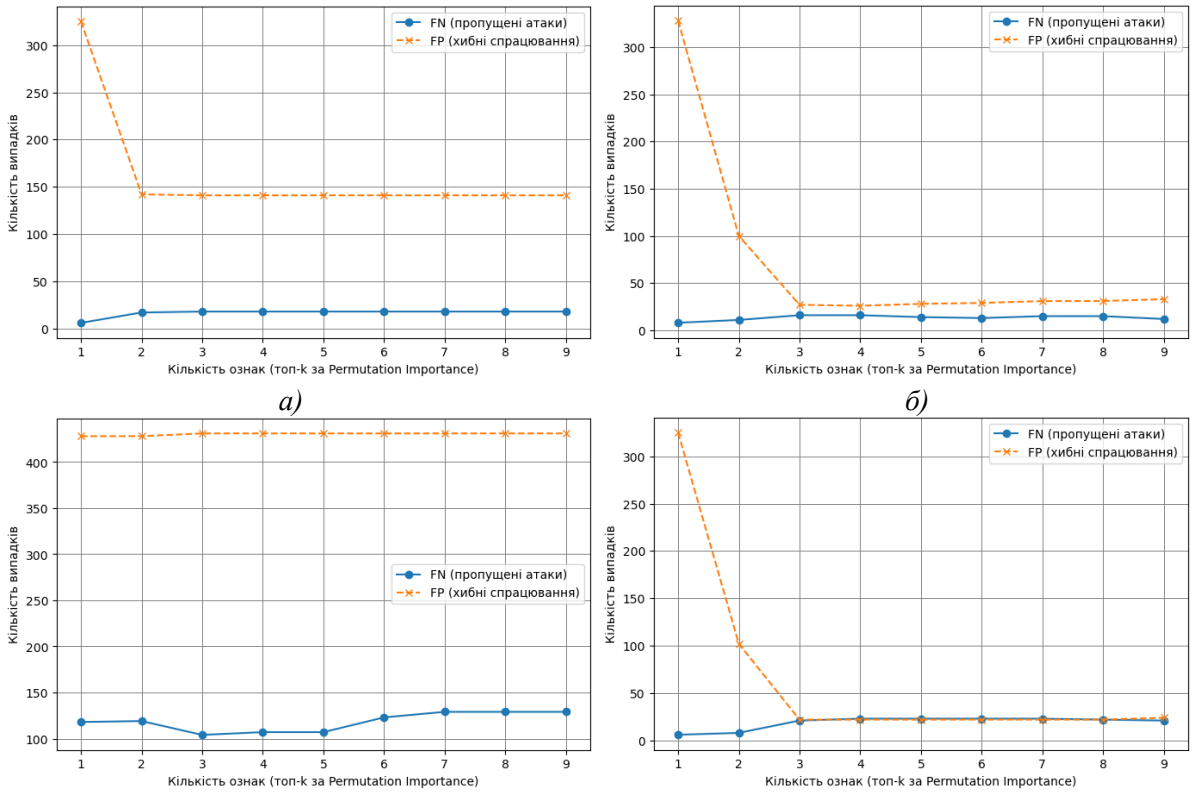
Рис.5. Графіки залежності кількості пропущених кібератак та кількості хибних спрацювань від кількості ознак при використанні методу MIF



а) *б)*

в) *г)*

Рис. 6. Графіки залежності кількості пропущених кібератак та кількості хибних спрацювань від кількості ознак при використанні методу Relief



а) *б)*

в) *г)*

Рис. 7. Графіки залежності кількості пропущених кібератак та кількості хибних спрацювань від кількості ознак при використанні GA

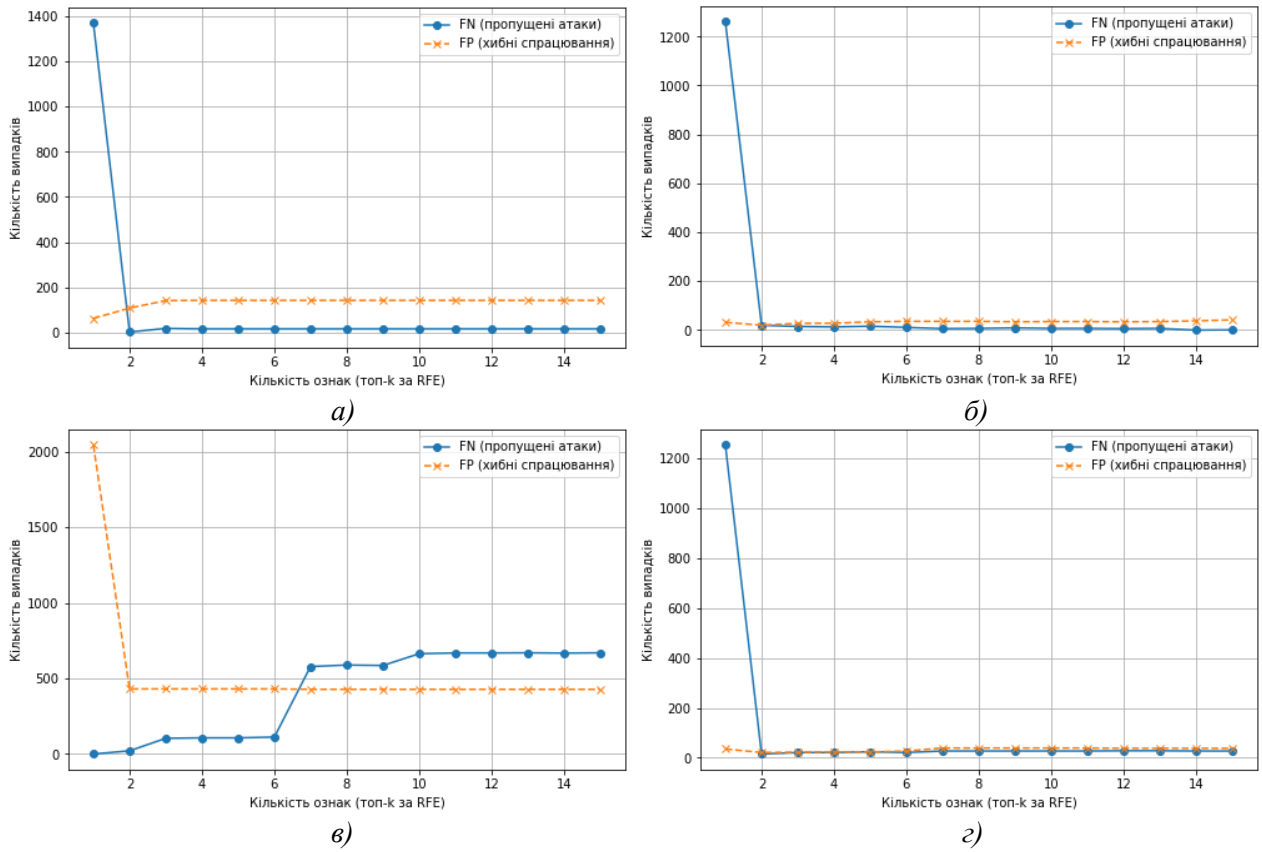


Рис. 8. Графіки залежності кількості пропущених кібератак та кількості хибних спрацювань від кількості ознак при використанні методу RFE

Аналіз результатів показав, що:

1. При використанні методу CFS усі досліджені моделі машинного навчання дають гірший результат за кількістю пропущених атак та кількістю хибних спрацювань ніж при навчанні на повному датасеті. Окрім того, обчислювальна складність цього методу тягне за собою значні затрати часу на відбір ознак, що нівелює виграш від зменшення часу на навчання моделі на меншому наборі ознак.

2. При використанні методу Relief було отримано покращення якості роботи усіх досліджуваних моделей машинного навчання, за усіма показниками, проте, цей метод погано працює на великих наборах даних оскільки має значну обчислювальну складність. Час на відбір 15 ознак із досліджуваного датасету склав більше ніж 6 годин з піковим використанням оперативної пам’яті 87 ГБ.

3. Не ефективною для детектування кібератак є модель на основі методу SVM, що пов’язано з його особливостями. Використання будь яких методів відбору ознак не призвело до значного покращення результатів роботи моделі. Час на навчання та тестування моделі є найвищим із розглянутих методів МН.

4. Найкращих результатів вдалось досягти при використанні алгоритму з χ^2, методів ANOVA та MIF в моделі, що побудована на основі RF. Дещо гірші показники в цьому поєднанні мають методи GA та RFE. Проте використання методів GA та RFE в моделі на основі методу KNN дає найкращий результат з усіх досліджуваних комбінацій методів відбору ознак та методів МН за кількістю детектованих атак та хибних спрацювань. Усі показники якості у такому випадку мають значення що перевищують 99 %.

Висновки

Загалом варто підкреслити, що використання методів відбору ознак дозволяє покращити показники якості роботи моделей машинного навчання, зменшити час на їх навчання. Проте слід зазначити, що ефективність кожного із методів залежить від об'єму та характеру даних, які потрібно опрацювати, методів машинного навчання з якими використовуються ті чи інші методи відбору ознак, часових та обчислювальних обмежень. Наведені в статті результати експериментальних досліджень можуть бути використані для вдосконалення існуючих, або розробки нових моделей машинного навчання, що використовуються в системах кіберзахисту.

Проведений аналіз не є вичерпним і не охоплює усі існуючі методи відбору ознак та їх комбінації, тому напрямками подальших досліджень є аналіз ефективності використання ансамблевих методів відбору ознак та оцінка стабільності різних методів (оцінює, чи залишається обрана підмножина ознак при незначних варіаціях вхідних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. D. W. Fernando, N. Komninos, T. Chen. A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques. *IoT*. 2020. Vol. 1, no. 2. Pp. 551–604. URL: https://doi.org/10.3390/iot1020030.

2. M. S. Akhtar, T. Feng. Evaluation of Machine Learning Algorithms for Malware Detection. *Sensors*. 2023. Vol. 23, no. 2. P. 946. URL: https://doi.org/10.3390/s23020946.

3. Osanaiye O., Cai H., Choo K.-K. R., Dehghantanha A., Xu Z., Dlodlo M. Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking.* 2016. Article number: 130. URL: https://doi.org/10.1186/s13638-016-0623-3.

4. Niveditha S., Prianka Rr., Sathya K., Shreyanth S., Nandhagopal Subramani, Balakrishnan Deivasigamani. Predicting Malware Classification and Family using Machine Learning: A Cuckoo Environment Approach with Automated Feature Selection. *Procedia Computer Science*. 2024. Vol. 235, P. 2434–2451. URL: https://doi.org/10.1016/j.procs.2024.04.230.

5. Xiujuan Wang, Yuchen Zhou. Multi-Label Feature Selection with Conditional Mutual Information. *Computational Intelligence and Neuroscience*. 2022. Article ID 9243893, P. 13. URL: https://doi.org/10.1155/2022/9243893.

6. Khammassi Chaouki, Krichen Saoussen. A GA-LR Wrapper Approach for Feature Selection in Network Intrusion Detection. *Computers & Security*. 2017. Vol. 70. P. 255–277. URL: DOI:10.1016/j.cose.2017.06.005.

7. Mambwe Sydney Kasongo, Sun Yanxia. Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset. *Journal Of Big Data*. 2020. URL: https://doi.org/10.1186/s40537-020-00379-6.

8. Ullah I., Mahmoud Q. H. A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. *Canadian Conference on Artificial Intelligence.* 2020. P. 508–520. URL: https://doi.org/10.1007/978-3-030-47358-7_52.

9. Furqan Rustam, Anca D Jurcut. Malicious traffic detection in multi-environment networks using novel S-DATE and PSO-D-SEM approaches. *Computers & Security*. 2023. № 136 (5): 103564. URL: https://doi.org/10.1016/j.cose.2023.103564.

10. M. C. Barbieri, B. I. Grisci, M. Dorn. Analysis and comparison of feature selection methods towards performance and stability. *Expert Systems With Applications.* 2024. Vol. 249, Part B. URL: https://doi.org/10.1016/j.eswa.2024.123667.

11. Ian Goodfellow, Yoshua Bengio, Aaron Courville. Deep learning. *The MIT Press*. Cambridge, Massachusetts London, England. 2016. 776 p.

12. Mark Hall. Correlation-based feature selection fordiscrete andnumeric class machine learning. *Proceedings of the 17th International Conference on Machine Learning (ICML2000)*. Stanford University, Stanford, CA, USA. 2000. P. 359–366.

13. Handoyo Samingun, Pradianti Nandia, Nugroho Waego, Akri Yusnita. A Heuristic Feature Selection in Logistic Regression Modeling with Newton Raphson and Gradient Descent Algorithm. *International*

Journal of Advanced Computer Science and Applications. 2022. Vol. 13, No. 3. P. 119–126. URL: DOI:10.14569/IJACSA.2022.0130317.

14. Kumar Mukesh, Rath Nitish, Swain Amitav, Rath Santanu. Feature Selection and Classification of Microarray Data using MapReduce based ANOVA and K-Nearest Neighbor. *Procedia Computer Science*. 2015. Vol. 54. P. 301–310. URL: https://doi.org/10.1016/j.procs.2015.06.035.

15. Scikit-learn documentation. SelectKBest. URL: :https://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.SelectKBest.html (дата звернення: 28.10.2025).

16. Xue B., Zhang M., Browne W. N., Yao X. A survey on evolutionary computation approaches to feature selection. *IEEE Trans. Evolutionary Computation*. 2016. Vol. 20, no. 4, P. 606–626. URL: https://doi.org/10.1109/TEVC.2015.2504420.

17. Guyon I., Weston J., Barnhill S., Vapnik V. Gene Selection for Cancer Classification using Support Vector Machines. *Machine Learning*. 2002. Vol. 46. P. 389–422. URL: https://doi.org/10.1023/A:1012487302797.

18. Scikit-learn documentation. Recursive feature elimination. URL: https://scikit-learn.org/stable/modules/feature_selection.html#recursive-feature-elimination (дата звернення: 28.10.2025).

19. Scikit-learn documentation. Precision, recall and F-measure metrics. URL: https://scikit-learn.org/stable/modules/model_evaluation.html#precision-recall-f-measure-metrics (дата звернення: 28.10.2025).

20. Scikit-learn documentation. Balanced accuracy score. URL: https://scikit-learn.org/stable/modules/model_evaluation.html#balanced-accuracy-score (дата звернення: 07.11.2025).

DOI: 10.58254/viti.8.2025.07.96

УДК 355.4:621.396.967

канд. техн. наук Каптур В. А. ORCID: 0000-0003-4200-1151 (ОСЦЕП СВ ЗСУ)

МЕТОДИКА ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ ДЖЕРЕЛА РАДІОВИПРОМІНЮВАННЯ ЗА ОДНИМ ПЕЛЕНГОМ

Вступ. *Вирішення задач локалізації та відображення районів ймовірного місцезнаходження джерел радіовипромінювання в зоні бойових дій є сьогодні ключовими функціями будь-якої системи ситуаційної обізнаності та електронної підтримки. Ситуація за якої значний обсяг інформації, що реєструється відповідними засобами виявлення, просто не використовується і призводить до різкого погіршення якості та достовірності роботи відповідних систем.*

Проблематика. *Відсутність механізмів ефективної утилізації інформації від засобів виявлення за умов наявності обмеженої кількості даних про виявлене джерело радіовипромінювання.*

Мета. *Розробка підходу до визначення місцезнаходження джерела радіовипромінювання в умовах відсутності достатньої для здійснення тріангуляції або трилатерації обсягу інформації від засобів виявлення.*

Матеріали й методи. *В роботі проведено аналіз сучасних методів та підходів до виявлення руху та положення джерел радіовипромінювання в основу яких покладено принцип пасивного радіочастотного спостереження на базі прийому та аналізу існуючих електромагнітних сигналів у навколишньому середовищі. Для оцінки ймовірного значення потужності випромінювання використано загальновідому модель розповсюдження радіохвиль у вільному просторі, а також підхід, що базується на застосуванні накопичення статистичних даних про стріангульовані джерела радіовипромінювання.*

Результати. *Уперше поєднано підхід пеленгаційного спостереження з оцінкою ймовірного значення потужності випромінювання, що базується на моделі поширення сигналу у вільному просторі та накопиченні статистичних даних про раніше локалізовані джерела. На основі запропонованого підходу розроблено методику визначення місцезнаходження джерела радіовипромінювання за одним пеленгом.*

Висновки. *Представлена методика може бути використана для реалізації окремих компонентів систем ситуаційної обізнаності, які базуються на застосуванні даних, що надходять від різноманітних засобів електронної підтримки.*

Ключові слова: *електронна підтримка, ситуаційна обізнаність, радіоелектронна розвідка, джерело радіовипромінювання, пеленг, втрати, локалізація.*

V. Kaptur. Method for determining the location of a source of radio radiation by a single bearing

Introduction. *Solving the problems of localization and mapping the areas of probable location of radio emission sources in the combat zone are today the key functions of any situational awareness and electronic support system. A situation in which a significant amount of information recorded by the appropriate detection sources is simply not used leads to a quick deterioration in the quality and reliability of the operation of the relevant systems.*

Problem. *The absence of mechanisms for effective utilization of information from detection sources in the presence of a limited amount of data on the detected radio emission source.*

Purpose. *Development of an approach to determining the location of a radio emission source in the absence of sufficient information for triangulation or trilateration from detection sources.*

Materials and methods. *The paper analyzes modern methods and approaches to detecting the movement and position of radio emission sources, which are based on the principle of passive radio frequency surveillance based on the reception and analysis of existing electromagnetic signals in the environment. To estimate the probable value of the radio emission power, a well-known model of radio wave propagation in free space was used, as well as an approach based on the application of the accumulation of statistical data on triangulated radio emission sources.*

Results. *For the first time, the direction-finding approach is combined with an estimate of the probable value of the radio emission power, based on a model of signal propagation in free space and the accumulation of statistical data on previously localized sources. Based on the proposed approach, a method for determining the location of a radio emission source by a single bearing is developed.*

Conclusions. *The presented method can be used to implement individual components of situational awareness systems that are based on the application of data coming from various sources of electronic support.*

Keywords: *electronic support, situational awareness, electronic intelligence, radio emission source, bearing, losses, localization.*

Постановка проблеми. Однією з найважливіших задач будь-якої системи електронної підтримки є локалізація та відображення районів ймовірного місцезнаходження джерел радіовипромінювання (ДРВ) (наприклад, безпілотних літальних апаратів, БпЛА). В якості безпосереднього джерела інформації при цьому можуть використовуватись засоби виявлення (сенсори, пеленгатори тощо) різних виробників. Залежно від типу засобу виявлення реалізація зазначеного функціоналу здійснюється різними способами, що включають: розбір інформаційних повідомлень каналів керування, фіксацію сигнатур випромінювання на певних частотах тощо.

Одним із найбільш розповсюджених та очевидних способів детектування точного місцезнаходження ДРВ є тріангуляція радіосигналу двома чи більшою кількістю засобів одного типу. Досягається це завдяки тому, що такі засоби виявлення, як пеленгатори, які мають відповідну антенну решітку, не тільки визначають рівень прийнятого сигналу, але й напрямок, з якого він надійшов (пеленг).

Але доволі часто ДРВ може бути виявлено лише одним засобом. При цьому в результаті можна отримати пеленг, рівень сигналу на приймачі засобу, частотні характеристики ДРВ, однак встановити точне місцеположення за одним пеленгом неможливо. Зазвичай це призводить до того, що значний обсяг інформації, яка реєструється відповідними засобами, просто не використовується системами ситуаційної обізнаності і ніяким чином не бере участі в оцінці стану електромагнітного спектра в тому чи іншому районі ведення бойових дій.

Аналіз останніх досліджень і публікацій. Методи та підходи до виявлення руху і положення ДРВ, а також їх класифікація сьогодні є одним з найбільш досліджуваних напрямків в радіоінженерії. В його основу покладені методи пасивного радіочастотного спостереження, які, в свою чергу, спираються на прийом та аналіз існуючих електромагнітних сигналів у навколишньому середовищі [1]. Такі системи фіксуючи та аналізуючи зміни характеристик сигналу (сили сигналу, частоти, фази та інших параметрів), можуть виявляти рух, присутність та моделі поведінки ДРВ. Основою процедур визначення місцезнаходження ДРВ при цьому складають так звані методи локалізації [2], такі як ToA (time of arrival), TDoA (time difference of arrival), AoA (angle of arrival) та RSS (received signal strength). Характерною спільною ознакою всіх цих методів є застосування методів тріангуляції або трилатерації, що базуються на наявності більш ніж одного приймача. В свою чергу задача визначення місцезнаходження джерела радіовипромінювання в умовах наявності лише одного приймача зазвичай вирішується шляхом переміщення цього приймача в просторі відносно положення ДРВ. Так, наприклад, в [3] запропоновано метод, у якому один приймач на борту БпЛА виконує обертальний рух, щоб отримати послідовні "псевдопеленги" (pseudo-bearing measurements), що дозволяє в подальшому визначати положення радіоджерел без необхідності встановлення кількох статичних приймачів. В іншій роботі [4] досліджено систему, яка переміщує одну всеспрямовану антену у просторі (наприклад, по сферичній поверхні), щоб накопичити кутові вимірювання, а потім оцінити напрям на джерело за рахунок руху. Таким чином, питання розробки нових методів та підходів, щодо визначення місцезнаходження джерела радіовипромінювання за одним пеленгом при застосуванні мереж стаціонарних приймачів залишається актуальним.

Метою статті є розробка методики визначення місцезнаходження ДРВ за одним пеленгом.

Виклад основного матеріалу дослідження. В основу методики визначення місцезнаходження ДРВ за одним пеленгом пропонується покласти принцип визначення ймовірного для кожного засобу виявлення значення потужності випромінювання типового ДРВ, що є характерним для відповідного району ведення бойових дій у відповідному проміжку часу та відповідному частотному діапазоні. Визначення ймовірного значення потужності при цьому має відбуватись або за рахунок співставлення сигнатури зафіксованого сигналу ДРВ із відомими шаблонами сигналів, або ж шляхом розрахунку спираючись при цьому на значення

рівня зареєстрованого сигналу, його частоти та відстані до ДРВ, що були отримані в результаті повноцінних тріангуляцій, в яких брав участь той засіб виявлення, для якого здійснюється визначення ймовірного значення потужності випромінювання типового ДРВ (рис. 1).

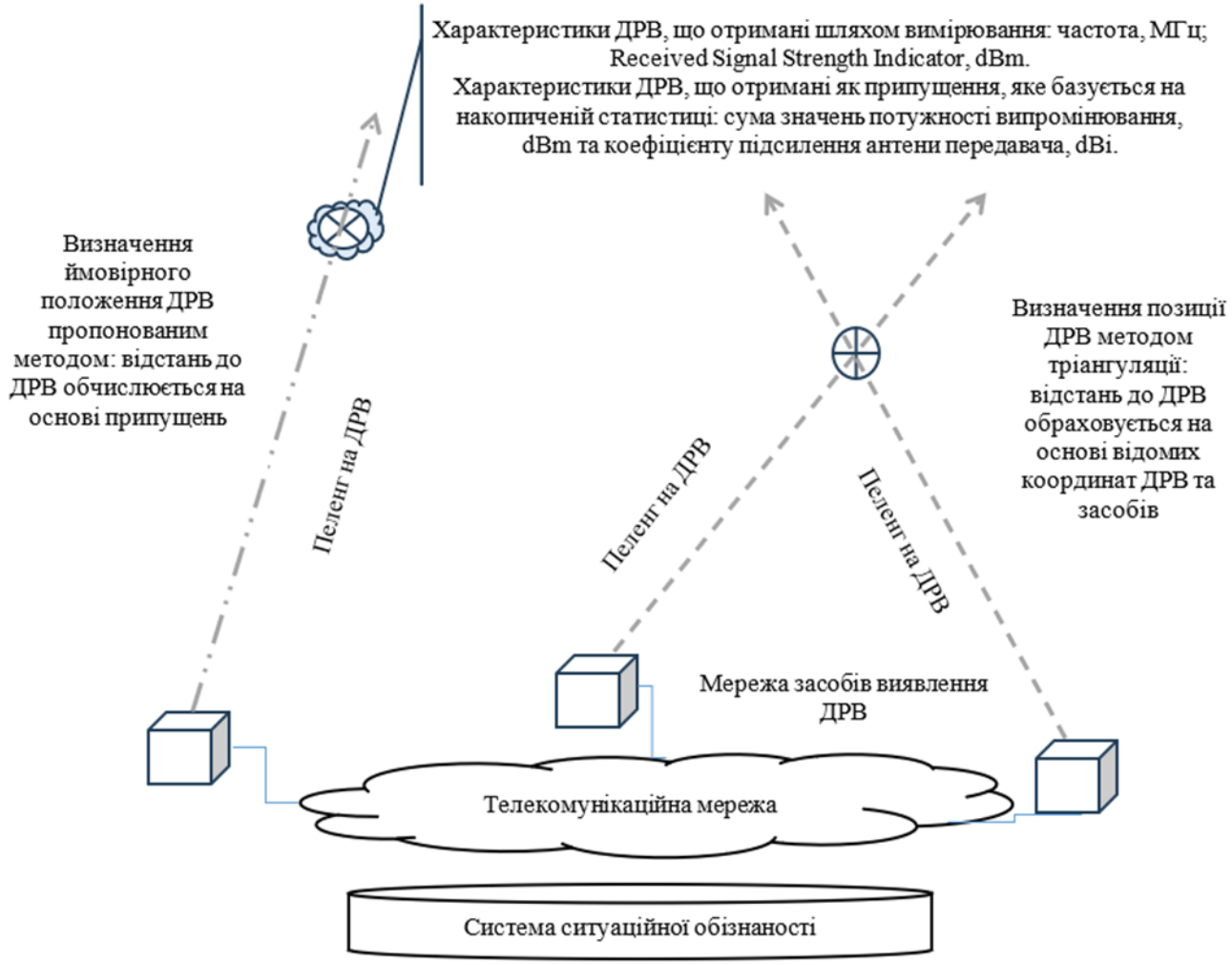


Рис. 1. Загальний принцип визначення місцезнаходження ДРВ за одним пеленгом

Обмеження та припущення. Передбачається наявність інформації про тактико-технічні характеристики засобів електронної підтримки, що використовуються для збору інформації про ДРВ. Однак в межах цієї статті ці застереження будуть проігноровані з метою формування первинної моделі.

На рисунку 2 зображено алгоритм визначення місцезнаходження ДРВ за одним пеленгом.

Вихідними даними для роботи алгоритму (рис. 2) є географічні координати та характеристики засобу виявлення (наприклад, коефіцієнт підсилення приймальної антени), множина сигнатур ДРВ з відомими характеристиками потужності випромінювання та множина повноцінних тріангуляцій з відомими координатами виявлених ДРВ, а також потік подій типу “пеленг” від засобу виявлення.

Під подією типу “пеленг” в межах цієї роботи будемо розуміти дані, що отримані від засобу виявлення (безпосередньо або від сервера чи центральної ноди (вузла) того чи іншого виробника), що містять кут між напрямом від засобу детектування юстованого на північ (магнітну або істинну, залежно від системи координат, що використовується в системі

електронної підтримки) до виявленого джерела радіовипромінювання з врахуванням похибки визначення позиції (відхилення від значення пеленгу).

Ядром алгоритму (рис. 2) є безперервний цикл обробки подій від засобів виявлення. Вихід з циклу (та алгоритму в цілому) відбувається лише за умов примусового або позапланового завершення роботи системи, в межах якої реалізовано цей алгоритм.

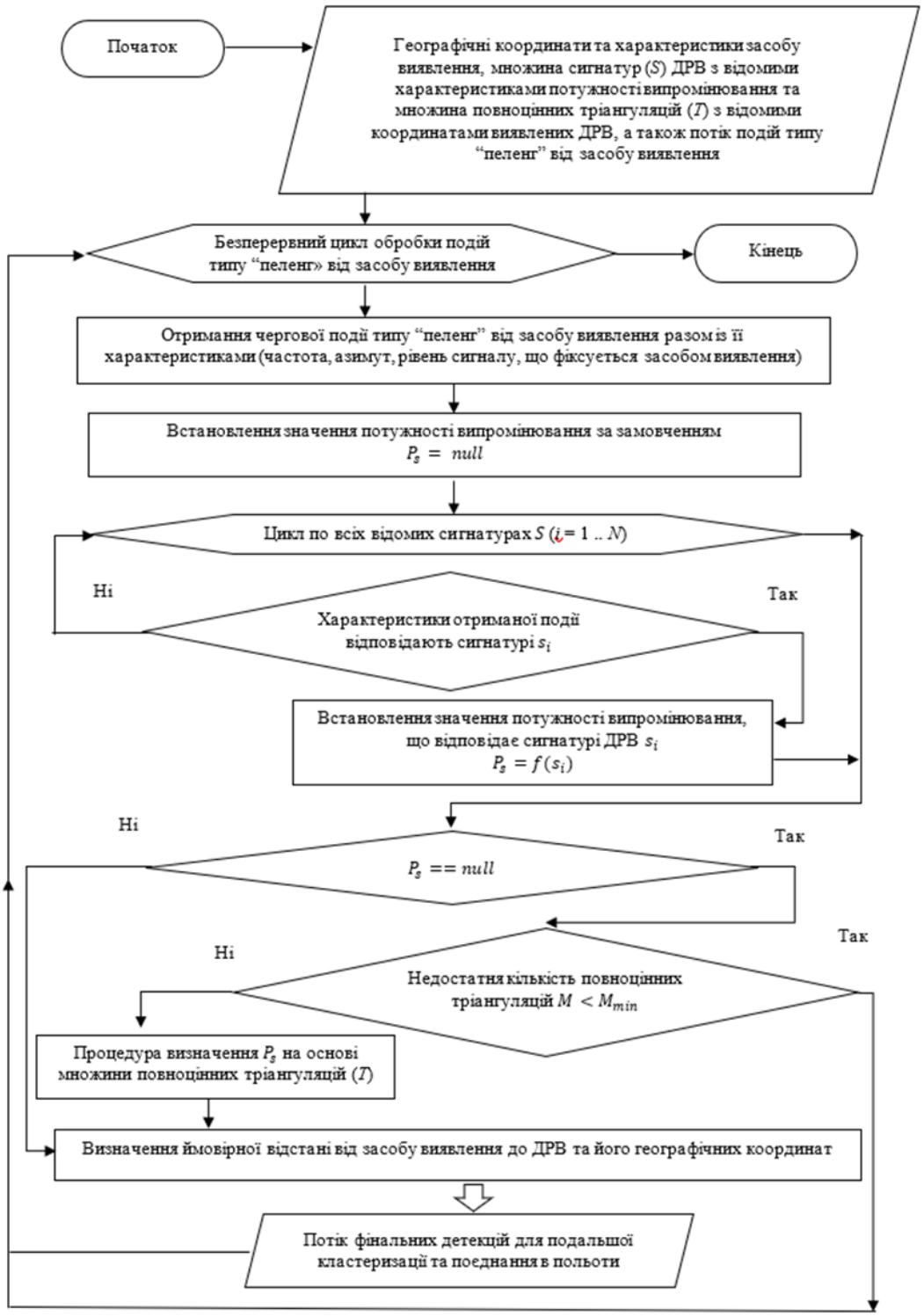


Рис. 2. Алгоритм визначення місцезнаходження ДРВ за одним пеленгом

На кожній черговій ітерації циклу здійснюється отримання чергової події типу "пеленг" від засобу виявлення разом із її характеристиками (частота, азимут, рівень сигналу, що фіксується засобом виявлення). Всі інші типи подій (наприклад, тріангульована детекція, виявлення тощо) в межах цього алгоритму ігноруються.

Першою операцією після отримання чергової події є встановлення ймовірного значення потужності випромінювання за замовченням у невизначене значення ($P_s = null$). Тут і далі під потужністю випромінювання будемо розуміти ймовірну потужність з якою ДРВ здійснює випромінювання, і яка складається з потужності передавача та коефіцієнта підсилення передавальної антени, що використовується ДРВ (1):

$$P_s = P_t + G_t, \tag{1}$$

де P_t – потужність передавача ДРВ, dBm; G_t – коефіцієнт підсилення передавальної антени ДРВ, dBi.

Далі в межах циклу (рис. 2), що послідовно перебирає всі відомі сигнатури з множини $S\{s_1, s_2, \dots, s_N\}$ здійснюється оцінка чи характеристика отриманої події, відповідають черговій сигнатурі s_i, де i = 1 ... *N*. У разі, якщо таку сигнатуру знайдено ймовірна потужність випромінювання встановлюється у значення, що відповідає сигнатурі ДРВ s_i ($P_s = f(s_i)$).

У разі, якщо на попередньому кроці значення ймовірної потужності випромінювання не було визначено, здійснюється оцінка можливості застосування процедури визначення P_s на основі множини повноцінних тріангуляцій (*T*). Виклик цієї процедури відбувається лише у випадку, коли кількість повноцінних тріангуляцій, в яких брав участь відповідний засіб виявлення, є більшою або рівною за мінімально встановлену кількість ($M \geq M_{\min}$). В іншому випадку відповідна подія типу "пеленг" ігнорується і не може бути використаною для визначення місцезнаходження ДРВ.

Якщо відповідне ймовірне значення потужності випромінювання було визначено або шляхом співставлення із відповідною множиною сигнатур, або через застосування процедури визначення потужності, на основі множини повноцінних тріангуляцій, на наступному кроці алгоритму здійснюється визначення ймовірної відстані від засобу виявлення до ДРВ та його географічних координат з подальшим передаванням цієї інформації до загального потоку фінальних детекцій для подальшої кластеризації та поєднання в польоти.

На рисунку 3 наведено процедуру визначення P_s на основі множини повноцінних тріангуляцій (*T*). Вихідними даними для роботи процедури є географічні координати та характеристики засобу виявлення, що отримані з головного алгоритму (рис. 1), а також множина повноцінних тріангуляцій з відомими координатами виявлених за участю цього засобу ДРВ.

Процедура базується на визначенні середнього по кожному сенсору значенню P_s, що визначено шляхом зворотного підрахунку, спираючись на значення частоти та рівня сигналу, що фіксується засобом виявлення, що отримані для кожної повноцінно тріангульованої детекції в якій приймав участь відповідний засіб за певний період часу (задану глибину (кількість) детекцій), а також на характеристики самого засобу (зокрема, коефіцієнт підсилення приймальної антени засобу виявлення).

У разі, якщо в базі даних недостатньо відомостей для обрахунку середнього значення на задану глибину (кількість) детекцій $M_{\min}$ – відповідні припущення щодо візуалізації можливих джерел випромінювання за цим засобом не обраховуються.

Слід зазначити, що на рис. 3 наведено найпростіший з можливих варіантів реалізації процедури. Для покращення точності додатково може бути застосовано відкидання значень p_j, що відхиляються від середнього значення на певне значення (наприклад, перевищують середньоквадратичну похибку, що обчислена на основі попереднього ряду значень). Однак в межах цієї статті зазначені варіанти не розглядаються, а підкислюється лише загальний

принцип – застосування даних про повноцінні тріангуляції для своєрідного "навчання" моделі шляхом підрахунку очікуваної (ймовірної) потужності ДРВ.

Визначення відстані d_j від засобу виявлення до точки тріангуляції t_j здійснюється за допомогою формули гаверсинуса [5] із використанням координат сенсора та тріангульованої позиції.

В свою чергу визначення значення ймовірної потужності випромінювання ДРВ p_j для тріангуляції t_j (рис. 3) здійснюється на основі тієї чи іншої моделі розповсюдження радіохвиль (моделі визначення втрат). Слід зазначити, що обрання моделі також залежить від конкретної реалізації системи, особливостей розташування засобу виявлення та характеристик його антенної системи. Однак у межах цієї статті ми будемо розглядати лише найпростіший випадок – модель розповсюдження радіохвиль у вільному просторі (справедлива для випадків коли і джерело і приймач в зоні прямої видимості). В цьому випадку значення ймовірної потужності випромінювання ДРВ p_j може бути визначено за формулою [6; 7] (2):

$$p_j = RS_j + 20\log(f_j) + 20\log(d_j) - G_r + 32.44\,, \tag{2}$$

де RS_j– RSSI (Received Signal Strength Indicator), сила сигналу, що було зафіксовано засобом виявлення в межах *j*-ї тріангуляції, dBm; f_j – частота, на якій засобом виявлення було зафіксовано сигнал в межах *j*-ї тріангуляції, МГц; d – відстань від засобу виявлення до точки тріангуляції t_j, км; G_r – максимальний коефіцієнт підсилення антени приймача засобу виявлення (для резонансної частоти та головного напрямку випромінення).

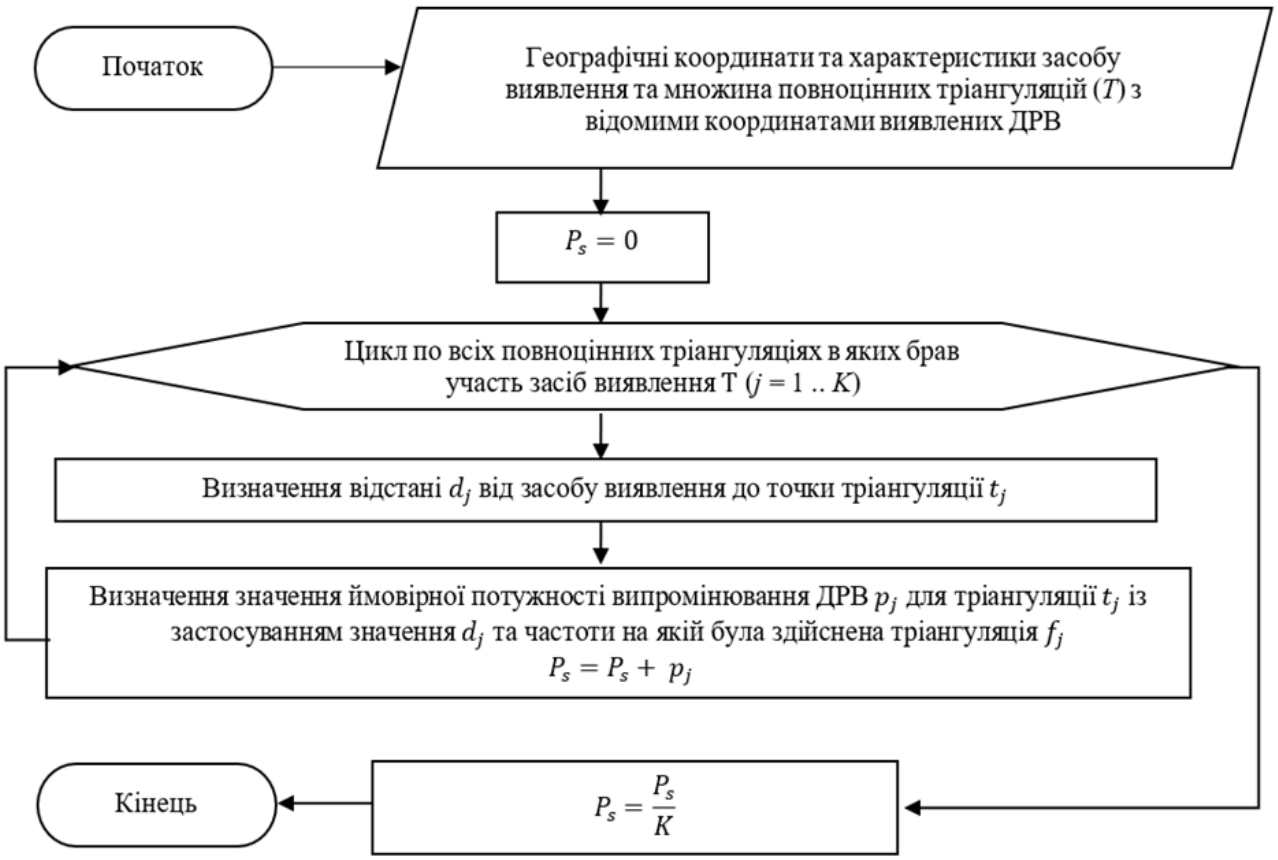


Рис. 3. Процедура визначення P_s на основі множини повноцінних тріангуляцій

Слід зазначити, що формула (2) є коректною якщо частоти передавача та приймача співпадають. Отже потрібно, щоб засіб виявлення працював у смузі роботи ДРВ. В іншому випадку засіб виявлення може детектувати позасмугове випромінення і розрахунок не буде коректним. Також слід зазначити, що якщо частота відрізняється від оптимальної для даної антени та/або напрямок на ДРВ не є головним напрямком випромінення, необхідно враховувати зменшення підсилення в вертикальній та горизонтальній площинах.

Очевидно, що отримавши в результаті роботи вищезазначених алгоритмів (рис. 2 та рис. 3) припущення щодо ймовірної потужності ДРВ та використавши формулу (2) можна отримати ймовірне значення відстані від засобу до ДРВ.

$$d = \frac{10^{P_S - RS - 20\log(f) - G_r - 32.44}}{20}, \quad (3)$$

де P_s – ймовірна потужність з якою ДРВ здійснює випромінювання, dBm; RS – RSSI (Received Signal Strength Indicator), сила сигналу, що було зафіксовано засобом виявлення в межах відповідної події типу "пеленг", dBm; f – частота, на якій засобом виявлення було зафіксовано сигнал у межах відповідної події типу "пеленг", МГц; G_r – максимальний коефіцієнт підсилення антени приймача засобу виявлення (для резонансної частоти та головного напрямку випромінення).

Отримане ймовірне значення відстані, від засобу до ДРВ, можна легко перерахувати у координати потенційного джерела випромінювання із застосуванням тієї ж самої формули гаверсинуса, а відповідні координати в подальшому можуть бути кластеризовані до того чи іншого активного польоту, надаючи змогу відображати відповідні фіксації ДРВ в цілісному вигляді в межах тієї чи іншої системи ситуаційної обізнаності.

Висновки й перспективи подальших досліджень

Запропоновано методику визначення джерела радіовипромінювання за одним пеленгом, що базується на застосуванні ймовірного значення потужності випромінювання для визначення підрахунку ймовірного значення відстані від засобу до джерела через застосування тієї чи іншої моделі розповсюдження радіохвиль.

Наведений приклад базується на застосуванні моделі розповсюдження радіохвиль у вільному просторі та визначенні потужності на основі множини повноцінних тріангуляцій, що були зроблені за участю відповідного засобу виявлення.

Отримані результати можуть бути використані у складі більш комплексних алгоритмів систем ситуаційної обізнаності військового та цивільного призначення. Відображення місцеположення джерел радіовипромінювання, яке отримане на основі пропонованого алгоритму, в таких системах має супроводжуватись позначенням того, що відповідні розрахунки зроблено на основі низки припущень про потужність ДРВ, тип на направленість його антени тощо, що суттєвим чином може вплинути на точність визначення потенційного місцезнаходження такого джерела.

З цією метою подальші дослідження мають бути зосереджені на формалізації процедур поєднання відповідних визначень положень джерела радіовипромінювання в таку сутність як "політ БпЛА".

Також, для оцінки ефективності запропонованого підходу, рекомендовано розробити імітаційну модель, що дозволила б на основі історичних даних, які отримані з реальних засобів виявлення, формувати відповідну гіпотезу про потужність ДРВ. Подальші дослідження мають бути спрямовані на вдосконалення "опорних" показників, що можуть вплинути на точність детектування, таких як глибина детекцій тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cui G., Liu J., Li H., Himed B. Signal detection with noisy reference for passive sensing. *Signal Process.* 2015. No. 108. P. 389–399.

2. He W.-N., Huang X.-L. Deterministic Localization for Fully Automatic Operation: A Survey and Experiments. *Sensors*. 2024. Vol. 24, no. 13. P. 4128. DOI: https://doi.org/10.3390/s24134128.

3. Chen F., Rezatofighi S. H., Ranasinghe D. C. GyroCopter: Differential Bearing Measuring Trajectory Planner for Tracking and Localizing Radio Frequency Sources. *IEEE Robotics and Automation Letters.* 2024. DOI: 10.1109/LRA.2024.3525549.

4. Eliyahu G., Maor A. M., Meshar R., Mukamal R., Weiss A. J. Single Transmitter Direction Finding Using a Single Moving Omnidirectional Antenna. *Sensors.* 2022. Vol. 22, no. 23. P. 9208. DOI: https://doi.org/10.3390/s22239208.

5. Інман Джеймс. Navigation and Nautical Astronomy: For the Use of British Seamen. L., C. & J. Rivington, 1835.

6. Friis H. T. A Note on a Simple Transmission Formula. *IRE Proceedings.* 1946. Vol. 34, No. 5. P. 254–256.

7. Ensatellite. Free Space Path Loss: Derivation from Friss transmission equation. URL: https://ensatellite.com/fspl/?utm_source=chatgpt.com (дата звернення: 30.08.2025).

DOI: 10.58254/viti.8.2025.08.104

УДК 004.421.2

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 ЗАСТОСУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Псевдовипадкові послідовності відіграють ключову роль у сучасних інформаційно-комунікаційних та обчислювальних системах. Напрямки наукових досліджень питань створення та обробки псевдовипадкових послідовностей є невід'ємною складовою розвитку озброєння та військової техніки оскільки у в цій сфері псевдовипадкові послідовності використовуються для забезпечення захищених каналів зв'язку, прихованої передачі інформації, формування завадостійких сигналів, а також у системах радіолокації та навігації. Застосування таких послідовностей дозволяє підвищити точність та стійкість до впливу засобів радіоелектронної боротьби. Особливої ваги набуває проблема генерації якісних псевдовипадкових послідовностей набуває в умовах сучасних бойових дій. Інформаційна перевага та стійкість систем зв'язку до перехоплення чи глушіння визначають ефективність управління військами і застосування окремих високотехнологічних зразків озброєння.

Використання псевдовипадкових послідовностей у технологіях розширеного спектра забезпечує не лише підвищену завадостійкість радіоканалів, але й ускладнює виявлення та дешифрування сигналів з боку противника. Це має безпосереднє значення також для безпілотних авіаційних комплексів, навігаційних систем та високоточних засобів ураження. Крім того, псевдовипадкові послідовності є основою для криптографічних алгоритмів, що забезпечують захист службової інформації, командно-штабних даних та телеметрії озброєння.

Генератори псевдовипадкових послідовностей знаходять застосування в автоматизованих системах управління військами, інформаційних мережах та спеціалізованому програмному забезпеченні військового призначення.

Таким чином, з огляду на тенденції цифровізації та інтелектуалізації озброєння, вимоги до швидкодії, статистичної якості та криптографічної стійкості псевдовипадкових послідовностей, дослідження середовища використання псевдовипадкових послідовностей є актуальним завданням, що напряму пов'язане з підвищенням ефективності функціонування сучасних і перспективних зразків озброєння та військової техніки, а також із забезпеченням інформаційної та кібернетичної безпеки у воєнній сфері.

Ключові слова: *генератор псевдовипадкових послідовностей, криптозахист, статистичні тести, генерація ключів, інформаційно-комунікаційні системи.*

V. Kuzavkov, A. Tlustyi. Analysis of the application of pseudorandom sequences in weapon systems

Pseudorandom sequences play a key role in modern information-communication and computational systems. Research directions devoted to the generation and processing of pseudorandom sequences are an integral component of the development of weaponry and military equipment, since in this domain pseudorandom sequences are employed to provide secure communication channels, covert information transfer, formation of interference-resistant signals, as well as in radar and navigation systems. The use of such sequences makes it possible to increase accuracy and robustness against the effects of electronic warfare means. This problem of generating high-quality pseudorandom sequences acquires particular importance in the conditions of contemporary armed conflict. The information advantage and the resilience of communication systems to interception or jamming determine the effectiveness of troop command and the employment of certain high-technology weapon systems.

Application of pseudorandom sequences in spread-spectrum technologies provides not only enhanced interference resistance of radio channels, but also complicates detection and decryption of signals by the adversary. This is directly relevant for unmanned aerial systems, navigation systems, and precision strike means. Moreover, pseudorandom sequences form the basis of cryptographic algorithms that protect operational information, command-and-control data, and telemetry of weapon systems.

Pseudorandom sequence generators are used in automated command-and-control systems, information networks, and specialized military software solutions.

Thus, in view of trends toward digitization and increased autonomy of weapon systems, and given the stringent requirements for throughput, statistical quality, and cryptographic strength of pseudorandom sequences, investigation of the operating environment and generation methods for pseudorandom sequences is an urgent task directly related to improving the performance of current and prospective weapon systems, as well as to ensuring information and cyber security in the military domain.

Keywords: *pseudorandom sequence generator, cryptographic protection, statistical tests, key generation, information-communication systems.*

Постановка проблеми

Проблематика генерації та застосування псевдовипадкових послідовностей (ПВП) тривалий час перебуває у фокусі наукових досліджень, що обумовлено їх ключовою роллю в інформаційній безпеці та цифрових комунікаційних технологіях. Попри значний науковий прогрес, відсутня систематизована оцінка ролі та ефективності ПВП у військових системах, де вони використовуються для захищеного зв’язку, радіолокації, навігації, формування завадостійких сигналів і криптографічного захисту даних. Наявні дослідження зосереджені переважно на окремих аспектах – статистичній якості, криптографічній стійкості чи апаратних реалізаціях генераторів, тоді як інтегральний підхід до аналізу сфер застосування ПВП у комплексних зразках озброєння відсутній. Це зумовлює необхідність цілісного вивчення можливостей та обмежень ПВП у воєнно-технічних системах для підвищення їхньої ефективності та інформаційної безпеки.

Аналіз публікацій за темою дослідження

У працях українських дослідників [1; 3] наголошується на важливості ПВП для систем військового зв’язку, де основна увага приділяється забезпеченню завадостійкості та захисту службової інформації. Ці підходи корелюють із закордонними дослідженнями [2; 4], у яких ПВП розглядаються як базис для побудови систем зв’язку з розширеним спектром, що гарантують прихованість передавання та стійкість до впливу радіоелектронних засобів противника.

Особливе місце у науковій літературі займають дослідження, спрямовані на створення генераторів криптографічно стійких ПВП. Рекомендації NIST [5; 9] визначають сучасні вимоги до генераторів випадкових чисел, підкреслюючи необхідність як високих статистичних характеристик, так і захисту від можливих криптоаналітичних атак. Значний внесок у цій сфері зробили роботи, що аналізують математичні властивості послідовностей: періодичність, рівномірність розподілу, кореляційні характеристики та лінійну складність [6; 7; 14; 15].

Паралельно активно досліджуються апаратні методи генерації випадкових чисел, які базуються на фізичних процесах, зокрема на хаотичних коливаннях та шумових сигналах [8; 10; 19]. Такі підходи дозволяють отримати справді випадкові послідовності, однак їх впровадження вимагає значних обчислювальних і технічних ресурсів.

Окремий напрям становлять роботи, присвячені застосуванню ПВП у криптографії. Дослідження [24–26] висвітлюють використання генераторів псевдовипадкових чисел у протоколах автентифікації, цифрових підписах, алгоритмах формування ключів та протоколах післяквантової криптографії. Це дозволяє зробити висновок, що саме криптографія є сферою, де до ПВП висуваються найжорсткіші вимоги.

Метою статті є систематизація та обґрунтування сфер застосування ПВП у інформаційно-комунікаційних системах спеціального призначення, визначення їх ролі у забезпеченні криптографічної стійкості та функціональної ефективності технологій передачі, обробки й захисту даних

Виклад основного матеріалу

Визначення та класифікація псевдовипадкових послідовностей

Псевдовипадкові послідовності (ПВП) визначаються як послідовності чисел або бітів, що генеруються детермінованими алгоритмами, але за своїми статистичними властивостями наближаються до істинно випадкових [6].

Класифікація ПВП формують базис для їх подальшого дослідження і дає змогу встановити відповідність певного виду послідовності конкретним сферам застосування у військовій та цивільній техніці. Класифікація ПВП може здійснюватися за різними ознаками (табл. 1).

Таблиця 1

Класифікація ПВП

№ з/п	Критерій класифікації	Класи (Типи) ПВП
1	За призначенням та сферою застосування	Звичайні ПВП Криптографічно стійкі ПВП Сигнальні ПВП (PN-послідовності)
2	За методом генерації	Лінійні генератори Нелінійні генератори Гібридні генератори
3	За структурою та довжиною періоду	Короткоперіодичні Довгоперіодичні
4	За якістю випадковості	Нестійкі ПВП Високоякісні ПВП
5	За способом реалізації	Детерміновані (алгоритмічні) Апаратні
6	У контексті застосувань	Криптографічно стійкі Некриптографічні
7	За структурою генератора	Лінійні конгруентні РЗЛЗЗ -послідовності Хаотичні відображення, гібридні методи

Класифікація псевдовипадкових послідовностей

У науковій та технічній літературі ПВП класифікують за кількома критеріями:

За призначенням та сферою застосування: звичайні ПВП – *застосовуються у моделюванні, чисельних методах, статистиці, машинному навчанні,* криптографічно стійкі ПВП – *розроблені для задач захисту інформації, генерації ключів, формування стійких до атак потоків даних* [8], синальні ПВП (PN-послідовності) – *застосовуються у системах зв’язку, радіолокації та навігації для розширення спектра сигналу та підвищення завадостійкості* [9].

За методом генерації: лінійні генератори *(лінійні конгруентні, регістри зсуву з лінійним зворотним зв’язком)* нелінійні генератори *(алгоритми на основі хаотичних відображень, криптографічних примітивів),* гібридні генератори *(поєднання кількох методів для підвищення статистичної якості).*

За структурою та довжиною періоду: короткоперіодичні – *придатні для обмежених завдань (наприклад, тестових симуляцій),* довгоперіодичні – *забезпечують стійкість до передбачення та можливість використання у складних системах (наприклад, військових мережах зв’язку).*

За якістю випадковості: нестійкі ПВП – *мають виявлені кореляції, що робить їх непридатними для криптографії,* високоякісні ПВП – *проходять усі тести NIST та відповідають вимогам до генераторів випадкових чисел у безпечних системах* [7].

ПВП також поділяють на детерміновані (алгоритмічні), які формуються за допомогою математичних виразів або рекурентних співвідношень, та апаратні, що базуються на фізичних процесах, котрі моделюють випадковість [8].

У контексті криптографії та військових застосувань важливим є поділ ПВП на криптографічно стійкі та некриптографічні. Перші володіють високим рівнем непередбачуваності та захищеності від атак, другі ж використовуються у задачах моделювання чи тестування, де вимоги до безпеки є нижчими [9].

Також ПВП класифікують за структурою генератора: на основі лінійних конгруентних методів, регістрів зсуву з лінійним зворотним зв’язком (РЗЛЗЗ), хаотичних відображень, гібридних методів тощо [10].

Класифікація ПВП демонструє широкий спектр можливостей застосування ПВП. Вибір конкретного класу залежить від вимог до системи: у моделюванні та чисельних обчисленнях

першочерговим є швидкодія, тоді як у військових системах зв’язку та криптографії – криптостійкість і захищеність від передбачення. Саме ця різноманітність підходів до класифікації дозволяє адаптувати ПВП до потреб різних галузей, включаючи сферу озброєнь і військової техніки.

Ключові математичні властивості

Ефективність псевдовипадкових послідовностей (ефективність використання ПВП), зокрема у військовій техніці та засобах зв’язку, безпосередньо залежить від їхніх математичних властивостей. Саме вони визначають, наскільки послідовність наближена до істинно випадкової та чи може вона бути використана для криптографічного захисту, моделювання або формування сигнальних структур. До таких властивостей слід віднести: періодичність; рівномірність розподілу; незалежність (відсутність кореляцій); автокореляційні властивості; лінійна складність; ентропія та непередбачуваність; стійкість до статистичного аналізу. Розглянемо ці показники окремо.

Будь-який детермінований генератор ПВП породжує послідовність скінченої довжини, яка з часом повторюється. Довжина циклу називається періодом. Для практичних застосувань необхідно, щоб період був достатньо довгим і перевищував потреби системи. У криптографії вимагаються надзвичайно довгі періоди [11].

Іншою фундаментальною вимогою до ПВП є рівномірність розподілу значень у заданому діапазоні. Це означає, що з імовірністю, наближеною до випадкової, усі можливі стани генератора повинні зустрічатися з однаковою частотою. У випадку бітових послідовностей – кількість нулів і одиниць має бути збалансованою [12].

Для того щоб ПВП були корисними в задачах захисту інформації та передачі сигналів, вони повинні задовольняти вимогу статистичної незалежності: жоден елемент послідовності не повинен передбачатися на основі попередніх. Наявність кореляцій робить послідовність вразливою до аналізу та атак, що є критичною загрозою у військових системах зв’язку [13].

У багатьох прикладних сферах, зокрема у радіолокації та навігації, важливою є форма автокореляційної функції ПВП (рис. 1). Ідеальна послідовність повинна мати низькі бічні пелюстки автокореляції та різке зростання у точці нульового зсуву. Такі властивості забезпечують чітке розрізнення сигналів і зменшують рівень перешкод [14].

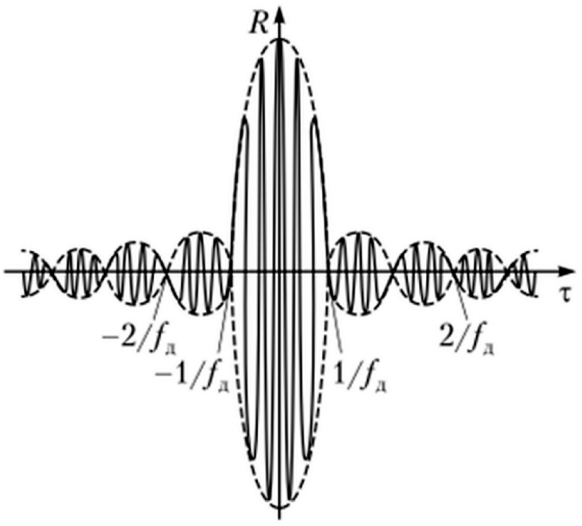


Рис. 1. Графік нормованої автокореляційної функції лінійно-частотно модульованого імпульсу

Лінійна складність визначається як мінімальна довжина регістра зсуву, здатного відтворити дану послідовність. Для безпечних ПВП лінійна складність повинна бути високою, інакше існує ймовірність відтворення генератора та передбачення подальших значень [15].

Ентропія визначає ступінь «невпорядкованості» послідовності та гарантує, що прогнозування наступного елемента практично неможливе. Висока ентропія є необхідною умовою для використання ПВП у криптографії. У військових застосуваннях ця властивість безпосередньо пов'язана з кіберстійкістю та захистом від засобів радіоелектронної розвідки [13].

Придатність визначається за допомогою статистичних тестів. Цей набір найчастіше визначається сукупністю нормативних документів та стандартів, серед яких ключовими є NIST SP 800-22, NIST SP 800-90, ISO/IEC 18031, FIPS 140-2/3, а також національні стандарти (ДСТУ ISO/IEC 18031:2015). Це дозволяє визначити, чи відповідають їхні властивості вимогам реальних систем. Послідовності, що не проходять таких тестів не можуть застосовуватися у критичних задачах [15].

Таким чином, сукупність ключових математичних властивостей ПВП формує основу для їхньої придатності до різних сфер використання. У військових системах особливе значення мають довгий період, рівномірність розподілу, висока лінійна складність та низька кореляція, що дозволяє забезпечувати прихованість, завадостійкість та криптографічну стійкість.

Наступним аспектом роботи є розгляд основних методів генерації ПВП.

Методи генерації псевдовипадкових послідовностей (ПВП) визначають їхню якість, довжину періоду та придатність для різних застосувань. У загальному випадку генератор описується рекурентним співвідношенням:

$$X_{n+1} = f\left(X_{n,}X_{n-1,\dots}X_{n-k+1}\right), \tag{1}$$

де f – функція переходу;

k – порядок генератора [6].

У науковій літературі розрізняють: лінійні методи, не лінійні, гібридні та апаратні.

Реалізація лінійних методів можлива на основі лінійних конгруентних генераторів та РЗЛЗЗ.

При застосуванні лінійних конгруентних генераторів виконується правило:

$$X_{n+1} = (aX_n + c)\mathrm{mod}\, m, \tag{2}$$

де a – множник (ціле число, зазвичай > 1);

c – приростання (ціле число, може бути 0);

X_{n+1} – поточне значення послідовності (ціле число);

m – модуль (ціле число, зазвичай > 0);

$\mathrm{mod}\, m$ – операція взяття залишку від ділення на m.

Вираз (2) є класичним прикладом лінійного конгруенційного генератора, який використовується для створення псевдовипадкових послідовностей.

При правильному виборі параметрів забезпечується максимальний період m [16].

Формула визначає наступне значення послідовності X_{n+1} як залишок від ділення суми $aX_n + c$ на m.

Наприклад:

якщо $X_n = 5$, $a - 3$, $c = 7$, $m - 10$, то $X_{n+1} = (3 \cdot 5 + 7)\mathrm{mod}10 = 22,\ \mathrm{mod}10 = 2$.

У випадку використання РЗЛЗЗ правило виглядає наступним чином:

$$S_{n+k} = (C_1 S_{n+k-1} \oplus C_2 S_{n+k-2} \oplus \dots \oplus C_k S_n, \tag{3}$$

де $\oplus$ – операція XOR, $Ci \in \{0,1\}$ – коефіцієнти з характеристичного многочлена. (ЛЗРЗЗ) утворюють m-послідовності з максимальним періодом $2k-1$ [17].

Операція XOR ("виключене АБО") – це бінарна логічна операція, яка повертає 1, якщо вхідні біти різні, і 0, якщо однакові.

Таблиця 2

Істинності для операції XOR

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Властивості операції XOR:

комутативність $A \oplus B = B \oplus A$;

асоціативність $(A \oplus B) \oplus C = A \oplus (B \oplus C)$;

ідентичність $A \oplus 0 = A$;

інверсія $A \oplus A = 0$.

Вираз (3) описує рекурентне правило для генерації послідовності в ЛЗРЗЗ, де S_n, S_{n+1},…, S_{n+k} – елементи бінарної послідовності (зазвичай 0 або 1), які представляють стан регістру у момент часу n;

C_1, C_2,…, C_k – коефіцієнти характеристичного многочлена, де кожен $Ci \in \{0,1\}$. Ці коефіцієнти визначають, які попередні стани послідовності впливають на наступний стан. Зазвичай $C_k = 1$ (щоб многочлен був нормалізованим).

k – довжина регістру (кількість бітів або ступінь характеристичного многочлена).

В тому числі вираз (3) показує, що новий стан S_{n+k} обчислюється як результат операції XOR усіх попередніх станів S_{n+k-1}, S_{n+k-2},… S_n, помножені на відповідні коефіцієнти Ci.

Якщо $Ci = 0$, відповідний член ігнорується (тобто не бере участі в операції XOR).

У контексті ЛЗРЗЗ: операція XOR використовується для комбінування бітів із зворотного зв'язку, визначеного коефіцієнтами Ci. Наприклад: якщо $C_1 = 1$ і $C_2 = 1$, то $S_{n+2} = S_{n+1} \oplus S_n$ (зсуваємо і додаємо через операцію XOR).

Нелінійні методи складаються з нелінійних конгруентних генераторів:

$$X_{n+1} = (aX_n^2 + bX_n + c) mod\ m. \quad (4)$$

Вираз (4), де додано квадратичний або вищий член для руйнування лінійності та підвищення ентропії, хаотичних генераторів, базується на нелінійних відображеннях типу:

$$X_{n+1} = rX_n(1 - x_n), \quad X_n \in (0,1), \quad r \in (3.57, 4),$$

де r – параметр хаосу криптографічних генераторів котрі будуються на односторонніх функціях:

$$X_{n+1} = H(X_n \parallel s) \text{ [18]}, \quad (5)$$

де $H(\cdot)$ – криптографічна геш-функція (SHA-2, SHA-3);

s – додатковий параметр, який може виступати в ролі солі (salt) початкового значення (*seed*) або ключа, що визначає результат роботи алгоритму.

Інший варіант – використання потокових шифрів, де ключовий потік виступає ПВП [9].

Вираз (5) складається з кількох компонентів, які потрібно інтерпретувати:

X_n – поточне значення послідовності (може бути числом, рядком бітів або байтів, залежно від контексту);

X_{n+1} – наступне значення послідовності, яке обчислюється;

H – функція, ймовірно, геш-функція (наприклад, SHA-256, MD5), яка перетворює вхідні дані в фіксований вихідний геш;

$\|$ – операція конкатенації (об'єднання), яка з'єднує два елементи (наприклад, X_n і s) в один рядок або послідовність бітів.

Цей вираз описує ітеративний процес генерації послідовності, де кожне наступне значення X_{n+1} залежить від попереднього X_n і фіксованого s, об'єднаних через конкатенацію та оброблених геш-функцію H.

Наприклад: початкове $X_0 = 1001$, $s = 1100$, H – функція, що повертає 8 бітів;

$X_1 = (10011100 = 10101010$ (уявімо, що геш дає цей результат);

$X_2 = (10101010 \| 1100 = H(101010101100)$, і так далі.

Гібридні методи складаються з комбінованих генераторів (приклад – операція XOR-комбінація двох РЗЛЗЗ:

$$s_n = s_n^{(1)} \oplus s_n^{(2)}, \tag{6}$$

де $s_n^{(1)}, s_n^{(2)}$ – виходи двох незалежних регістрів; та методи комбінованих конгруентних генераторів:

$$(X_{n+1} = (a_n X_n \bmod m_1 - a_2 X_n \bmod m_2) \bmod (m_2 - 1), \tag{7}$$

що дозволяє значно подовжити період та зменшити кореляції [16].

Окреме місце займають апаратні методи які реалізуються через фізичні процеси (шум, хаотичні осцилятори).

У спрощеному вигляді формула апаратного генератора може описуватися як:

$$X_{n+1} = \mathrm{Q}(\eta_n), \tag{8}$$

де η_n – виміряний шумовий сигнал;

$Q(\cdot)$ – процедура квантування до бітової форми [19].

Таким чином, формалізація кожного методу через математичні співвідношення дозволяє систематизувати підходи до генерації ПВП. Лінійні методи забезпечують простоту, нелінійні – криптографічну стійкість, гібридні – баланс властивостей, а апаратні – фізичну випадковість та високу швидкодію.

Різноманіття методів генерації зумовило появу великої кількості типів (ПВП), кожен з яких має власні характеристики: довжину періоду, спектральні властивості, рівень кореляції та криптографічну стійкість.

На практиці особливе місце посідають наступні класи (табл. 3).

Таблиця 3

Класифікація ПВП

Класи псевдовипадкових послідовностей					
Максимально довгі послідовності	Голд послідовності	Послідовності Kasami	Збільшені сімейства	Хаотичні послідовності	Криптографічні ключові потоки

Максимально довгі послідовності *m*-послідовності генеруються регістрами зсуву з лінійним зворотним зв'язком (РЗЛЗЗ) за характеристичним многочленом, що є примітивним над полем GF(2). Їх період дорівнює:

$$T = 2^n - 1, \tag{9}$$

де n – довжина регістра.

Властивості *m*-послідовностей: рівномірний розподіл нулів і одиниць (різниця не більше ніж на 1), двозначна автокореляційна функція (10) [20]:

$$\mathrm{R}(\tau) = \begin{cases} 1 & \text{при } \tau = 0 \\ -\frac{1}{2^n - 1} & \text{при } \tau \neq 0 \end{cases}. \tag{10}$$

Голд-послідовності отримуються як операція XOR двох різних *m*-послідовностей з однаковим періодом $2^n - 1$. Їх кількість *N* становить приблизно $2^n = 1$.

Математично виражається як:

$$g_i(t) = s_i(t) \oplus s_2(t + i), \tag{11}$$

де s_1 ,s_2 – m-послідовності;

i – зсув.

Перевагою є обмеженість значень кореляційної функції (наприклад, $-1, -t(n)$, $t(n) - 2$, що дозволяє використовувати їх у багатокористувальних системах CDMA [21].

Послідовності Kasami формуються на основі підмножини *m*-послідовностей та характеризуються ще кращими властивостями кореляції.

Для малої підмножини довжина періоду становить:

$$T = 2^n - 1, \tag{12}$$

а кількість послідовностей *N* дорівнює $2^{n}/_{2}$.

Дані послідовності знаходять застосування у стільникових мережах, супутникових каналах та військових системах зв'язку завдяки низькому рівню взаємної кореляції [22].

Збільшені сімейства такі як:

Коди Уолша: формуються за допомогою матриці Адамара:

$$H_1 = [1],\ H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}. \tag{13}$$

Усі послідовності взаємно ортогональні, що дозволяє застосовувати їх у каналах множинного доступу з ортогональним розділенням [23].

Коди Баркера – короткі послідовності довжиною N, для яких автокореляційна функція задовольняє умову:

$$\mathrm{R}(\tau) \leq 1,\ \tau \neq 0. \tag{14}$$

Використовуються у радіолокації завдяки мінімізації бічних пелюсток кореляційної функції [24].

Хаотичні послідовності формуються за допомогою хаотичних карт, наприклад, логістичного відображення:

$$x_{n+1} = rx_n(1 - x_n), x_n \in (1,0). \quad (15)$$

Властивості: непередбачуваність; висока ентропія; можливість регулювати спектральні характеристики.

Хаотичні ПВП все частіше використовуються у криптографії та системах безпілотної техніки [19].

У сучасних системах захисту інформації застосовуються криптографічні генератори, які формують ключові потоки.

Приклад – генератор на основі блочного шифру, що математично представлено формулою (16):

$$S_i = E_k(IV + i), \quad (16)$$

де $E_k(\cdot)$ – шифрування за ключем;

K – ключ шифрування;

IV – ініціалізаційний вектор.

Такі послідовності не тільки володіють статистичними властивостями ПВП, але й гарантують стійкість до атак [9].

Таким чином, типи ПВП різняться за своїми властивостями та областями застосування. m-послідовності та їх узагальнення (Голд, Kasami) ефективні у зв’язку та радіолокації; коди Уолша і Баркера – у сигнальних системах; хаотичні – у сучасних криптографічних протоколах; а криптографічні потоки – в інформаційній безпеці. Це підкреслює важливість грамотного вибору типу послідовності залежно від завдання, що безпосередньо пов’язано з військовою технікою та системами зв’язку.

Серед галузей застосування псевдовипадкових послідовностей найбільший інтерес у дослідників викликає криптографія.

У криптографії ПВП є основою генераторів ключових потоків, шифрів із секретним розподілом ключів та протоколів автентифікації, де необхідна висока ентропія й непередбачуваність [25; 26].

У криптографії справжня випадковість (наприклад, з фізичних джерел, як шум діодів) є ідеальною, але важко генерувати в великих обсягах. Тому використовують ПВП – послідовності, створені детермінованими алгоритмами, які виглядають випадковими, але повторюються при однакових початкових умовах. Вони повинні бути криптостійкими, тобто:

неможливість прогнозування наступного елемента послідовності навіть за умови знання довільної кількості попередніх;

стійкість до криптоаналітичних атак, зокрема методів зворотного відновлення алгоритму;

наявність максимального періоду та відповідність основним статистичним критеріям випадковості, що забезпечує можливість практичного застосування методу.

Генерація криптографічних ключів.

У симетричних криптографічних системах (зокрема, AES, DES) ключ виступає у вигляді бінарної послідовності значної довжини (зазвичай 128–256 бітів), яка визначає процеси шифрування та дешифрування інформаційних потоків.

Формування такого ключа ґрунтується на використанні псевдовипадкових послідовностей (ПВП), що генеруються на основі початкового значення (seed), котре може поєднувати пароль користувача із додатковими параметрами, наприклад, сіллю (salt). З метою

підвищення криптографічної стійкості до отриманої ПВП застосовується криптографічна геш-функція $H(\cdot)$, зокрема SHA-256, у результаті чого формується ключ.

Практичним прикладом є протоколи захисту бездротових мереж (наприклад, WPA2), де ключі формуються з паролів користувача шляхом використання алгоритму PBKDF2, що інтегрує ПВП для забезпечення додаткової ентропії та протидії словниковим атакам.

Ключовим аспектом є те, що без застосування ПВП криптографічні ключі мали б передбачувану структуру, що значно знижувало б рівень захисту і робило систему вразливою до несанкціонованого доступу.

Створення одноразових шифрів.

Одноразові шифри реалізуються шляхом використання псевдовипадкової послідовності, як ключа для операції XOR з повідомленням:

$$C = M \oplus K, \tag{17}$$

де M – вихідне повідомлення;

K – ключ у вигляді ПВП;

C – зашифрований текст [27].

Важливою умовою є те, що ключ повинен мати довжину, ідентичну довжині повідомлення, та використовуватися лише один раз. Порушення цієї вимоги призводить до значного зниження криптографічної стійкості [27; 28].

Прикладом практичного застосування даного принципу є потокові шифри, у яких для кожного пакета даних генерується нова послідовність ключових бітів. Історично застосовувався алгоритм RC4, який сьогодні вважається компрометованим, тоді як сучасні рішення базуються на безпечніших генераторах, таких як Salsa20 та його похідні [28].

Сутність методу полягає у тому, що за умови використання дійсно випадкового, секретного та одноразового ключа забезпечується абсолютна криптографічна стійкість, що теоретично унеможливлює розкриття повідомлення без знання ключа [29].

Вектори ініціалізації та nonce.

Використання векторів ініціалізації та одноразових числових значень (*nonce*) є фундаментальним механізмом забезпечення криптографічної стійкості сучасних систем шифрування [30].

Вектор ініціалізації IV являє собою коротку псевдовипадкову послідовність, яка поєднується з ключем шифру для запобігання появі ідентичних вихідних блоків у різних сеансах. У симетричних алгоритмах, зокрема в режимах Cipher Block Chaining (CBC) та Counter Mode (CTR), додавання IV до ключа забезпечує унікальність криптографічного перетворення для кожного блоку даних [31].

Поняття (*nonce*) передбачає використання унікальної псевдовипадкової послідовності для кожного повідомлення або транзакції в межах криптографічного протоколу. Наприклад, у режимі AES-GCM nonce виступає основою для генерації ключового потоку, що гарантує неможливість повторного застосування однакових параметрів при шифруванні [30; 32].

Фактично, механізм можна подати у виді:

$$IV \oplus K \Rightarrow K^*, \tag{18}$$

де IV – вектор ініціалізації;

K – основний ключ;

K^* – унікальний ключ для поточного блоку чи сеансу.

Практичним прикладом є протокол Transport Layer Security (TLS), що використовується для захищеного передавання даних в Інтернеті: у ньому для кожного сеансу формується унікальний nonce, який генерується псевдовипадковою послідовністю. Це забезпечує захист від атак, що базуються на повторному використанні зашифрованих даних.

Сутність цього підходу полягає в тому, що за відсутності векторів ініціалізації або nonce повторювальні повідомлення залишалися б вразливими для статистичного аналізу, що значно знижувало б рівень безпеки криптографічних систем [30; 32].

Використання солей (*salts*) при гешуванні паролів. Сіль визначається як псевдовипадкова послідовність, яка додається до пароля перед обчисленням його геш-значення. Це дозволяє сформувати унікальний вхідний рядок для криптографічної функції гешування. Процес описується співвідношенням:

$$h = H(P \parallel s), \tag{19}$$

де P – пароль користувача.

У практичних реалізаціях (наприклад, алгоритми *bcrypt*, *Argon2*) кожному користувачу в системі призначається власна унікальна сіль, завдяки чому навіть ідентичні паролі відображаються у різні геші. Це унеможливлює застосування заздалегідь обчислених таблиць відповідностей та ускладнює словникові атаки.

Сутність даного підходу полягає у підвищенні криптографічної стійкості систем автентифікації за рахунок індивідуалізації результатів гешування та мінімізації ризику компрометації баз даних паролів.

Генерація підписів і випадкових чисел.

У криптографічних системах використання псевдовипадкових послідовностей відіграє ключову роль у забезпеченні надійності цифрових підписів та протоколів обміну ключами. Зокрема, у схемах цифрового підпису, таких як ECDSA та RSA, псевдовипадкові значення застосовуються як *nonce* для запобігання компрометації секретних ключів [33].

У протоколах встановлення спільних параметрів, наприклад, у Diffie–Hellman, псевдовипадкові послідовності використовуються для генерації тимчасових ключів, що забезпечує унікальність та стійкість процесу обміну [34].

Прикладом практичного застосування даного підходу є система Bitcoin, де nonce використовується під час процесу майнінгу. Його роль полягає у варіюванні вхідних даних блоку для пошуку хешу з необхідними криптографічними властивостями, що відповідають встановленому рівню складності [35].

Загалом, використання псевдовипадкових послідовностей гарантує непередбачуваність криптографічних операцій і виключає можливість атак на основі повторів, тим самим підвищуючи безпеку системи [36].

Загальні висновки

Проведений аналіз засвідчив, що псевдовипадкові послідовності мають багатовекторне застосування у військових системах: від формування сигнальних структур у радіозв'язку та радіолокації до забезпечення криптографічних протоколів і процедур автентифікації. Різні класи ПВП демонструють відмінні характеристики – одні орієнтовані на високу швидкодію та простоту реалізації, інші забезпечують підвищений рівень непередбачуваності й стійкість до атак. Узагальнення підходів показало, що ефективність ПВП визначається не лише математичними властивостями, але й їхньою здатністю адаптуватися до вимог конкретних підсистем озброєння. Перспективним напрямом є розробка комбінованих і гібридних генераторів, які поєднують криптографічну стійкість, статистичну якість і технічну ефективність для практичного застосування у складних воєнно-технічних комплексах.

Напрямком подальшого розвитку наукової діяльності доцільно обрати розробку методів генерації створення ПВП для їх застосування у військовій сфері, зокрема в засобах радіозв’язку та електронно-комунікаційних системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Малахов О. А. Системи захищеного військового зв’язку. Київ: НУОУ, 2020.

2. Zhang Z., Zhang Y., Xu Z., Wang J. Design and analysis of spreading sequences for secure communications. *IEEE Access.* 2018. Vol. 6. P. 23518–23528. DOI: 10.1109/ACCESS.2018.2833166.

3. Боднар В. П. Захист інформації у системах військового призначення. Харків: ХНУРЕ, 2021.

4. Ding Z., Poor H. V. Design of multi-antenna spectrum sharing systems for wireless communications. *IEEE Transactions on Signal Processing.* 2015. Vol. 63, No. 4. P. 1003–1015. DOI: 10.1109/TSP.2014.2384197.

5. Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on post-quantum cryptography. NISTIR 8105. National Institute of Standards and Technology, 2016.

6. Niederreiter H., Winterhof A. Applied number theory. Springer, 2015.

7. Gentle J. E. Random number generation and Monte Carlo methods. Springer Science & Business Media, 2013.

8. Bucci M., Luzzi R., Trifiletti A. A high-speed oscillator-based true random number source for cryptographic applications on a smart card IC. *IEEE Transactions on Computers.* 2010. Vol. 59, No. 11. P. 1543–1554. DOI: 10.1109/TC.2010.125.

9. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST SP 800-90A Rev.1. National Institute of Standards and Technology, 2015.

10. Stipčević M., Koç Ç. K. True random number generators. In: Open Problems in Mathematics and Computational Science. Springer, 2014. P. 275–315. DOI: 10.1007/978-3-319-10683-0_13.

11. Li C., Babu P., Palomar D. P. Optimization methods for designing sequences with low autocorrelation sidelobes. *IEEE Transactions on Signal Processing.* 2014. Vol. 62, No. 7. P. 1711–1726. DOI: 10.1109/TSP.2014.2300837.

12. Möller T., Miller D. Uniform distribution measures of pseudorandom sequences in Monte Carlo integration. *Journal of Computational Physics.* 2016. Vol. 307. P. 50–68. DOI: 10.1016/j.jcp.2015.12.038.

13. Li C., Zhang Y., Wang C., Hanzo L. Physical layer security in military wireless networks. *IEEE Transactions on Vehicular Technology.* 2020. Vol. 69, No. 10. P. 11739–11752. DOI: 10.1109/TVT.2020.3016035.

14. Katz D. J. Sequences with low correlation. In: Л. Budaghyan, F. Rodríguez-Henríquez (eds.). *Arithmetic of Finite Fields. WAIFI 2018. Lecture Notes in Computer Science*, vol. 11321. Springer, 2018. P. 149–172.

15.Li C. A survey on complexity measures for pseudo-random sequences. *Cryptography.* 2024. Vol. 8, No. 2. P. 25. DOI: 10.3390/cryptography8020025.

16. L’Ecuyer P. History of uniform random number generation. *ACM Transactions on Modeling and Computer Simulation.* 2017. Vol. 28, No. 1. P. 1–35. DOI: 10.1145/3121434.

17. Wang X., Hu J. A new LFSR-based pseudorandom number generator. *International Journal of Computer Mathematics.* 2012. Vol. 89, No. 16. P. 2141–2152. DOI: 10.1080/00207160.2012.669457.

18. Kocarev L., Stojanovski T. Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine.* 2011. Vol. 1, No. 3. P. 6–21. DOI: 10.1109/7384.963463.

19. Sunar B., Martin W. J., Stinson D. R. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on Computers.* 2012. Vol. 56, No. 1. P. 109–119. DOI: 10.1109/TC.2006.257.

20. Canteaut A. LFSR-based Stream Ciphers. MPRI Lecture Notes, 2016.

21. Devrari A. et al. Sequential logic circuit Gold codes: LFSR-based gold code generator chip. *Microprocessors and Microsystems.* 2024. DOI: 10.1016/j.micpro.2024.104825.

22. Jiang W. On the generalized large set of Kasami sequences. *Applied Algebra in Engineering, Communication and Computing.* 2010. Vol. 21. P. 377–389. DOI: 10.1007/s00200-009-0105-3.

23. Wang S. et al. A Walsh-Hadamard coded spectral-efficient full-frequency-diversity COFDM. *IEEE Transactions on Communications.* 2010. Vol. 58, No. 7. P. 1966–1976. DOI: 10.1109/ TCOMM.2010.07.090116.

24. Suesser-Rechberger B., et al. Performance of Walsh-Hadamard codes used for timing recovery in a DVB-S2x multibeam scenario. CSNDSP 2016. DOI: 10.1109/CSNDSP.2016.7573985.

25. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. CRC Press, 2021.

26. Bernstein D. J., Lange T. Post-Quantum Cryptography. Springer, 2017.

27. Cerruti U., Fogliato R., Trovò F. One Time Pad and the Short Key Dream. *arXiv preprint.* 2021. arXiv:2108.06981.

28. Nabil M. A new-one-time-pad stream cipher. *International Journal of Wireless and Mobile Computing.* 2020. Vol. 18, No. 1. P. 46–56. DOI: 10.1504/IJWMC.2020.104364.

29. Ji Z., Xu J., Huang C., Yuen C. Random Shifting Intelligent Reflecting Surface for OTP Encrypted Data Transmission. *arXiv preprint.* 2020. arXiv:2010.14268.

30. Kampanakis P. et al. Practical Challenges with AES-GCM and the need for a nonce misuse-resistance option. NIST Workshop on Block Cipher Modes of Operation, 2024.

31. Gueron S. Compound-CTR: Counter Mode for Long Messages and a Long Nonce. *ACM Conference Paper.* 2022. DOI: 10.1145/3510548.3519545.

32. Li H., Wang Y., Ma Y., Jia W., Bai L. AEAD Modes for ZUC Family Stream Ciphers. *arXiv preprint.* 2021. arXiv:2111.05117.

33. Osaki S., Kunihiro N. Bias from Uniform Nonce: Revised Fourier Analysis-based Attack on ECDSA. SAC Workshop 2024. DOI: 10.1007/978-3-031-82852-2_9.

34. National Institute of Standards and Technology. Cryptographic Nonce. 2024.

35. Benkoczi R. et al. Quantum Bitcoin Mining. *Philosophical Transactions of the Royal Society A.* 2022. Vol. 380, No. 2229. P. 20210199. DOI: 10.1098/rsta.2021.0199.

36. Trail of Bits. ECDSA: Handle with Care. Trail of Bits Security Blog. 2020.

DOI: 10.58254/viti.8.2025.09.117

УДК 004.056

канд. техн. наук Мазулевський О. Є. ORCID: 0000-0002-6042-2577 (ВІТІ ім. Героїв Крут)
д-р філософії Зарубенко А. О. ORCID: 0000-0002-7616-6416 (ВІТІ ім. Героїв Крут)
канд. техн. наук Коваленко І. Г. ORCID: 0000-0002-6827-5196 (ВІТІ ім. Героїв Крут)

ВИЯВЛЕННЯ КРИТИЧНИХ ЗМІН У ДИНАМІЦІ КІЛЬКОСТІ КІБЕРІНЦИДЕНТІВ ЯК ІНДИКАТОРА ПРОГНОЗУВАННЯ ВИНИКНЕННЯ КРИЗОВИХ СИТУАЦІЙ В ОБОРОННОМУ ВІДОМСТВІ

У статті представлено науково обґрунтований підхід до оцінювання поточного стану кіберстійкості оборонного відомства, заснований на аналізі статистичних даних щодо кількості зареєстрованих кіберінцидентів. Запропонований підхід передбачає використання методів лінійної алгебри та статистичного аналізу для виявлення закономірностей та динамічних змін у розвитку кіберзагроз. Такий підхід дозволяє визначати моменти критичних відхилень, що можуть свідчити про зниження рівня кіберстійкості або підвищення ймовірності настання кризових ситуацій у кіберпросторі. Отримані результати створюють наукове підґрунтя для подальшого вдосконалення процесів оцінювання стану кіберзахисту, прогнозування ризиків та формування ефективної системи прийняття рішень у сфері кібербезпеки оборонного сектору.

Особливу увагу приділено розробленню алгоритмічного підходу до визначення критичних моментів у часових рядах показників кіберінцидентів, що дає змогу швидко реагувати на зміни у рівні загроз та адаптувати заходи кіберзахисту відповідно до поточної ситуації. У роботі підкреслено важливість інтеграції аналітичних методів до системи моніторингу кібербезпеки з метою підвищення ефективності виявлення та запобігання кібератакам.

Дослідження є першим етапом у формуванні комплексного методу оцінювання кіберстійкості та прогнозування ризиків для оборонного відомства відповідно до законодавчо визначеної зони відповідальності, що передбачає подальшу розробку механізмів протидії кризовим явищам у кіберпросторі. Практична значущість результатів полягає у створенні основи для підвищення ефективності управлінських рішень, забезпеченні завчасного виявлення загроз, мінімізації негативних наслідків кібератак та підтриманні належного рівня ситуаційної обізнаності керівного складу Міністерства оборони та Збройних Сил України.

Ключові слова: *кіберстійкість, кібербезпека, криза в галузі кібербезпеки, кіберінцидент.*

O. Mazulevsky., A. Zarubenko, I. Kovalenko. Identification of critical changes in the dynamics of the number of cyber incidents as an indicator for forecasting the occurrence of crisis situations in the defense department

The article presents a scientifically grounded approach to assessing the current state of cyber resilience of the defense agency, based on the analysis of statistical data regarding the number of recorded cyber incidents. The proposed methodology employs methods of linear algebra and statistical analysis to identify patterns and dynamic changes in the development of cyber threats. This makes it possible to determine moments of critical deviation that may indicate a decrease in cyber resilience or an increased likelihood of crisis situations in cyberspace. The obtained results provide a scientific foundation for improving cyber defense assessment processes, risk forecasting, and the development of an effective decision-making framework in the field of cybersecurity for the defense sector.

Special attention is devoted to developing an algorithmic approach for identifying critical moments within time series of cyber incident indicators, enabling timely response to variations in the threat landscape and the adaptive adjustment of cybersecurity measures according to current conditions. The study emphasizes the importance of integrating analytical methods into information security monitoring systems to enhance the efficiency of detecting and preventing cyberattacks.

This research represents the first stage in the development of a comprehensive methodology for assessing cyber resilience and forecasting risks for the defense agency in accordance with its legally defined area of responsibility. It also establishes a basis for further development of mechanisms to counteract crisis phenomena in cyberspace. The practical significance of the results lies in strengthening the effectiveness of managerial decision-making, ensuring early threat detection, minimizing the negative consequences of cyber incidents, and maintaining an adequate level of situational awareness among the leadership of the Ministry of Defense and the Armed Forces of Ukraine.

Keywords: *cyber resilience, cybersecurity, cybersecurity crisis, cyber incident.*

Вступ

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційних технологій, які проникають у всі сфери життєдіяльності, зокрема у військову, кібербезпека набуває статусу критично важливого чинника стабільного функціонування будь-якої

організації. Захист інформаційних ресурсів від загроз у кіберпросторі є необхідною передумовою ефективної діяльності, оскільки порушення кібербезпеки може призвести до значних фінансових і репутаційних втрат, зупинки процесів управління чи навіть до втрати людських життів у разі військових структур. З огляду на постійне зростання кількості та складності кібератак, перед фахівцями у сфері кібербезпеки постає завдання не лише оперативного реагування на інциденти, а й прогнозування потенційних кризових ситуацій в галузі кібербезпеки з метою мінімізації їх наслідків. У даній статті представлено один із етапів уперше розробленого процесу виявлення та прогнозування виникнення кризових явищ на основі статистичного аналізу даних про зафіксовані кіберінциденти та визначення числової оцінки поточного рівня кіберстійкості оборонного відомства для забезпечення належної ситуаційної обізнаності його керівництва.

Аналіз останніх досліджень та публікацій. Відповідно до [1] передбачено створення ситуаційного центру Кабінету Міністрів, а також ситуаційних центрів центральних органів виконавчої влади, обласних і Київської міської державних адміністрацій, інших державних органів та установ сектору безпеки й оборони, зокрема Міністерства оборони України.

Водночас у вітчизняному науковому та інформаційному просторі відсутні публікації, що висвітлюють методологічні підходи до виявлення потенційно можливих кризових ситуацій у кіберпросторі на основі аналізу статистичних даних. Єдиним нормативним документом, який частково стосується цього питання, є [2]. Проте зазначений документ регламентує лише взаємодію суб’єктів у процесі ліквідації вже наявних кризових ситуацій, не охоплюючи аспектів їх попередження чи прогнозування.

У зв’язку з цим, в тезах доповіді [3] запропоновано розпочати розробку та у даній статті представлено фрагмент *Методу прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних*.

Мета статті. Метою статті є представлення підходу оцінювання поточного стану кіберстійкості оборонного відомства з урахуванням ситуації у кіберпросторі на основі статистичного аналізу зафіксованих кіберінцидентів.

Виклад основного матеріалу дослідження

У процесі участі у війні (військових конфліктах) країна та суспільство зазнають стрімкого розвитку в різних галузях, що є запорукою вдалого протистояння ворогу. Однією з основних ознак розвитку сучасного суспільства (зокрема військової організації країни) під час війни є зростання залежності від якості й надійності інформаційно-комунікаційних систем (ІКС), які застосовуються в діяльності в усіх галузях життя: від країни як механізму державності, включно із воєнною організацією, так громадянина як носія державності. Відповідне посилення високорівневої спрямованості розвитку інформаційних ресурсів зумовлює необхідність підвищення вимог до рівня їх інформаційної безпеки, а особливо в умовах військового протиборства.

Проблема ускладнена особливістю глобальної мережі Інтернет, з якою інтегровано більшість ІКС і використанням загальнодоступного програмного забезпечення, призводять до накопичення випадкових і непередбачуваних впливів.

Зазначимо, що ІКС, які мають підключення до Інтернет, розглядаються в ракурсі необхідності захисту ресурсів таких систем від кібератак у процесі реалізації базових технологічних процесів отримання, зберігання, транспортування, оброблення та відображення інформації [4].

Обумовимо, що деякі терміни будуть використовуватися відповідно до [5]:

інформаційна безпека та кібербезпека в інформаційно-комунікаційних системах (інформаційна безпека в ІКС, ІБ в ІКС) − сукупність організаційних, правових, інженерно-технічних заходів, спрямованих на захист інформації та кіберзахист ІКС;

інцидент безпеки інформації – подія або низка несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії

людського фактору) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці ІКС, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку інформації, що обробляється в таких ІКС.

Введемо термін: кіберстійкість ІКС – стан ІКС, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз.

Інші терміни вживаються в значеннях, які наведені в Законах України [6; 7], Державному Стандарті України [8].

Згідно зі статтею 8 Закону України «Про основні засади забезпечення кібербезпеки України» [6] Міністерство оборони України є одним із основних суб’єктів національної системи кібербезпеки і відповідно до компетенції здійснює заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі. Тому, слід мати можливість оцінити стан кіберстійкості ІКС оборонного відомства і державних органів (установ) для прийняття зважених управлінських рішень в мирний час та під час функціонування в особливий період.

Далі, розглянемо отримання даних для проведення оцінки поточного стану системи з урахуванням ситуації у кіберпросторі. Для формування вірної картини стану кіберстійкості доречним буде проведення регулярного моніторингу результатів роботи засобів кіберзахисту в ІКС. Моніторинг реалізується шляхом збору статистичних даних виявлених кіберінцидентів засобами кіберзахисту та за допомогою роботи аналітиків кібербезпеки.

Для оцінки в Міноборони слід збирати дані за базові елементи національної системи кібербезпеки, а саме від державного сектору України, Збройних Сил України та Міністерства оборони України, за можливості інших елементів.

Для проведення оцінки поточного стану з урахуванням ситуації у кіберпросторі стану кіберстійкості Міноборони використовуються наступні показники, які показують рівень напруженості ситуації в кіберпросторі: узагальнений індекс напруженості ситуації у кіберпросторі; індекси напруженості ситуації у кіберпросторі для Державного сектору, ЗС України та Міноборони (усі окремо); узагальнений індекс змін кількості виявлених кіберінцидентів; індекси змін кількості виявлених кіберінцидентів для Державного сектору, ЗС України та Міноборони (усі окремо); композитний показник кіберстійкості (розраховується з урахуванням оцінки забезпеченості кібербезпеки в ІКС відомства, буде запропоновано у подальших дослідженнях).

Визначення узагальненого індексу напруженості ситуації у кіберпросторі і узагальненого індексу змін кількості виявлених кіберінцидентів проводиться на основі статистичних даних кількості виявлених кіберінцидентів у відповідальних підрозділах із кібербезпеки в ІТС та змін кількості кіберінцидентів у поточний момент із врахуванням даних за певний минулий період часу.

Індекс кількості виявлених інцидентів кібербезпеки розраховується для оцінки зміни виявленої активності проти ІКС різної приналежності. Дані, які надходять, мають відповідати Переліку категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України [9]. Приклад таксономії переліку категорій та типів кіберінцидентів наведено на сайті CERT-UA [10]. Перелік розроблявся для впровадження структуризації даних для обміну інформацією щодо кіберінцидентів в установах усіх форм власності.

Дані зі звітів по різними типам кіберінцидентів заносяться до таблиці. Для проведення статистичного аналізу необхідно мати вибірку даних не менше визначеного періоду, наприклад за 90 діб. На далі розмір вибірки може змінюватися з наданням обґрунтування.

На основі вибірки розраховуються наступні показники: перцентранк поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу напруженості ситуації у кіберпросторі); середнє геометричне

перцентранка поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу напруженості ситуації у кіберпросторі); кількість верхніх крайніх значень перцентранка поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу змін кількості виявлених кіберінцидентів); кількість нижніх крайніх значень перцентранка поточних показників за всіма типами кіберінцидентів (використовується для знаходження узагальненого індексу змін кількості виявлених кіберінцидентів).

Розглянемо розрахунок індексу напруженості ситуації у кіберпросторі. Узагальнений індекс напруженості ситуації у кіберпросторі розраховується на основі вибору максимального із індексів напруженості ситуації у кіберпросторі для окремих елементів, зокрема для ІКС Міноборони, ЗСУ, Держсектору, розрахунок яких розглянемо далі в матеріалах статті.

Розрахунок індексу напруженості ситуації у кіберпросторі для різних відомств проводиться за однаковими принципами але за своїми статистичними даними взятими зі звітів по напрямкам шляхом визначення перцентранку для кожного дня.

Перцентранк – перцентильний ранг значення у масиві даних (зворотна функція перцентиля). *Перцентиль* – значення ознаки, яке відокремлює кожну соту частину впорядкованого ряду, указує на відносне місце визначеного значення в загальному розподілі впорядкованої множини.

Функція розрахунку перцентраку обчислює перцентильний ранг значення (x) у масиві даних $\{A\}$. Формула для обчислення виглядає наступним чином:

$$P(x)=(r-1)/(N-1), \tag{1}$$

де $P(x)$ – перцентильний ранг значення x;

r – ранг значення x у впорядкованому масиві $\{A\}$;

N – загальна кількість елементів у масиві $\{A\}$.

Порядок розрахунку:

1. Впорядкування масиву: спочатку впорядковується масив даних $\{A\}$ у порядку зростання.

2. Визначення рангу: знаходиться ранг r значення x у впорядкованому масиві. Ранг – це позиція значення x у масиві $\{A\}$, починаючи з першого найменшого значення.

3. Обчислення перцентильного рангу: використовуючи формулу (1), де N – загальна кількість елементів у масиві, обчислюється перцентильний ранг значення x.

Обчислення проводиться для кожного типу кіберінцидентів (КІ) за визначений період і буде визначати множину $\{_{date}Perc\}$ набору перцентранків кожного відліку (за датою).

Наступним етапом розрахунків є знаходження середнього геометричного перцентранка поточних показників за всіма типами кіберінцидентів, що і буде значенням *індексу напруженості ситуації у кіберпросторі для елементу спостереження* (МО України, ЗС України, Держсектору). Для цього скористаємося класичною формулою розрахунку середнього геометричного: *середнє геометричне* (середнє пропорційне) декількох додатних чисел дорівнює кореню, ступінь якого дорівнює кількості чисел, із добутку даних чисел. Значення узагальнюється на довільну кількість чисел більших нуля. Середнє геометричне E чисел a_1, $a_2 \ldots a_E$ дорівнює кореню E-го ступеня із добутку даних чисел. Середнє геометричне E чисел a_1, $a_2 \ldots a_E$ дорівнює

$$Risk\_index = \sqrt[E]{\prod_{e=1}^{E} a_e}\ , \tag{2}$$

де E – кількість додатніх значень перцентранка за типами кіберінцидентів; a_e –додатні значення перцентранка за типами кіберінцидентів.

Індекс напруженості ситуації у кіберпросторі розраховується для кожного напряму спостереження, а саме для Міноборони, Збройних Сил України, державного сектору України.

Узагальнений індекс напруженості ситуації у кіберпросторі, як зазначалося вище, визначається вибором максимального значення серед індексів напруженості кожного напрямку спостереження.

Максимальне значення використовується з розуміння того, що відсутність проведення (виявлення) кіберінцидентів в одному із напрямів спостереження не є основою для припущення послаблення напруженості у кіберпросторі.

Індекс змін кількості виявлених кіберінцидентів. Подальшим етапом обробки статистичних даних є *знаходження верхніх крайніх та нижніх крайніх значень перцентранку кількості кіберінцидентів за типами, для кожного напрямку.* Порогові значення визначаються емпіричним шляхом (в подальшому можуть змінюватися для детального налаштування моделі прогнозування). На першому етапі прийнято рішення про фіксацію таких випадків:

для фіксації низького рівня кількості кіберінцидентів виражених перцентранком за типами при зменшенні менше ніж порогове значення;

для фіксації високого рівня кількості кіберінцидентів виражених перцентранком за типами при перебільшенні більше ніж порогове значення.

Використання декількох рівнів порогових значень може застосовуватися для визначення ступеню впливу та побудови більш точних моделей виявлення кіберінцидентів та прогнозування різних типів кібератак (кібервпливів) і в подальшому настання, на їх основі, кризових ситуацій. Для кожного окремого напряму розраховується значення кількості значень подолання порогових значень, в яких значення перераховані від більш суворих до більш м'яких.

Для кожного напряму визначимо кількість спрацювань по кожному пороговому значенню у матриці кількості подолань порогів $[{}_{date}B]$ згідно з виразом:

$$ {}_{date}B = \begin{bmatrix} |\forall \{{}_{date}Perc_{k=1..|{}_{date}Perc|}\} \leq MinPor_{p=1..P}|; \\ |\forall \{{}_{date}Perc_{k=1..|{}_{date}Perc|}\} \geq MaxPor_{p=1..P}|; \end{bmatrix}, $$

де ${}_{date}Perc_{k=1..|{}_{date}Perc|}$ – усі елементи множини значень перцентранків кількості кіберінцидентів за визначену дату;

MinPor – матриця значень мінімальних порогових значень;

MaxPor – матриця значень максимальних порогових значень.

Отже, в матриці кількості подолання порогів $[{}_{date}B]$ визначаються кількість зменшень відносно мінімальних порогів в першому рядку та кількість перебільшень максимальних порогів в другому рядку.

Подолання порогового значенням перцентранку кількості кіберінцидентів за типами дає змогу побачити аномальну активність/безактивність зловмисників. Перевищення покаже ймовірний початок нової атаки (етапу атаки), а заниження про завершення атаки (етапу атаки) і підготовку до нової атаки (етапу атаки). Як відомо, кібератака складається із декількох етапів, про що можливо дізнатися із різних підходів вивчення кібератак. Так, наприклад, «Cyber Kill Chain» від Lockheed Martin поділяє кібератаку на 7 етапів [11], а «MITRE ATT&CK» на 14 «тактик» із описом конкретних «технік» [12] для реалізації різних типів кібератак.

Не всі етапи кібератаки призводять до підвищення значень кількості кіберінцидентів, не всі атаки використовують послідовність класичних моделей та можуть бути проведені в повному обсязі набору дій в моделі для досягнення поставлених цілей (у разі дії не фінансово вмотивованих зловмисників, а політично чи примусово…). Або кібератаки різного типу

можуть бути етапами однієї більшої скоординованої кібератаки. Наприклад, останнім часом, ворогом, (через використання APT-угрупувань, Advanced Persistent Threat) під час проведення атак на інфраструктуру державного сектору для відволікання уваги фахівців кібербезпеки та/або переведення телекомунікаційного обладнання в критичні режими функціонування, проводяться атаки розподіленої відмови в обслуговуванні (DDoS) з залученням контрольованих «хактивістів» (політично або ідеологічно вмотивованих кіберзлочинців здебільшого із низьким рівнем підготовки) країни агресора під різними вигаданими (надуманими) приводами. Отже, «хактивісти» вважають це проведенням окремого «акту впливу» (помсти, покарання), а насправді є інструментом на черговому етапі для більш скоординованої кібератаки.

Індекс змін кількості виявлених кіберінцидентів розраховується окремо за кожним напрямом Міноборони, Збройних Сил України, державного сектору України, тощо. Для його знаходження використаємо раніше визначену матрицю кількості подолання порогів [$_{date}B$] відповідно для кожного напряму:

$$divIncidents = ({}_{date}B_{1,1} + {}_{date}B_{2,1}) * q,$$

де $_{date}B_{1,1}$ – елемент матриці $[_{date}B]$, який показує кількість подолання мінімального порогу (1 рядок 1 стовпець);

$_{date}B_{2,1}$ – елемент матриці $[_{date}B]$, який показує кількість подолання найстрогішого максимального порогу (2 строка 1 стовпець);

q – рівнозважений коефіцієнт впливу подолання порогового значення.

Значення рівнозваженого коефіцієнту впливу спрацювання порогового значення визначається як: $q = 100\% / 21 \approx 4.76$, де 21 – кількість типів кіберінцидентів в таксономії [10]. Значення рівнозваженого коефіцієнту впливу спрацювання порогового значення в подальшому можливо змінювати використовуючи наукові підходи, наприклад, методом парних порівнянь.

Узагальнений Індекс змін кількості виявлених кіберінцидентів визначається як максимальне значення серед індексів змін кількості виявлених кіберінцидентів кожного напряму спостереження.

Максимальне значення використовується з розуміння того, що відсутність проведення (виявлення) кіберінцидентів в одному з напрямів спостереження не є основою для припущення послаблення напруженості у кіберпросторі.

У подальшому для загальної картини варто розрахувати композитний показник кіберстійкості. Але для його оцінки потрібно оцінити результати впровадження заходів та засобів кіберзахисту в інфраструктурі відомств. Розгляд способу згаданої оцінки буде розглянуто в подальших дослідженнях.

В загальному, розробка *Методу прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних* оборонного відомства, ґрунтується на трьох послідовних етапах:

оцінювання забезпеченості системи кібербезпеки нормативно-правовими документами, їх змістовому наповненню та наявності технічних засобів кіберзахисту (є напрямом подальших досліджень);

аналіз поточного стану на основі статистичних даних щодо кількості та типів зафіксованих кіберінцидентів (розглянуто у даній статті);

прогнозування можливих кризових ситуацій у кіберпросторі з метою своєчасного реагування та мінімізації їх наслідків (є напрямом подальших досліджень).

Реалізація зазначеного методу сприятиме підвищенню спроможності оборонного відомства протидіяти кіберзагрозам шляхом запровадження ефективних заходів попередження та реагування.

Висновки й перспективи подальших досліджень

Запропонований у статті підхід до оцінювання поточного стану кіберстійкості оборонного відомства дає змогу підвищити рівень ситуаційної поінформованості щодо характеру та інтенсивності впливу противника (зловмисників) у кіберпросторі, а також слугує індикатором можливого наближення кризових ситуацій у сфері кібербезпеки. Представлений спосіб є складовою частиною "Методу прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних", подальша розробка й удосконалення якого визначають напрям наступних досліджень.

Впровадження оцінки поточного стану та прогнозування виникнення кризових ситуацій дозволить виявити прогалини в організації та забезпеченні кібербезпеки, ідентифікувати ознаки формування кризових ситуацій, що, в свою чергу, підвищить рівень готовності відомства до реагування на них, чим буде досягнуто мінімізації наслідків кіберінцидентів та забезпечення стабільного функціонування ІКС. Таким чином, розробка і практичне застосування зазначеного Методу становлять важливий крок до зміцнення кіберстійкості оборонного відомства в умовах зростаючої активності кіберзлочинців, державно-вмотивованих APT-груп і появи нових загроз у кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Питання мережі ситуаційних центрів: Постанова Кабінету Міністрів України від 11.07.2023 № 705. URL: https://zakon.rada.gov.ua/laws/show/705-2023-%D0%BF#Text (дата звернення: 24.11.2025).

2. Порядок взаємодії суб’єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки, затверджений Національним координаційним центром кібербезпеки 22.09.2022. URL: https://www.rnbo.gov.ua/ua/Diialnist/5765.html (дата звернення: 24.11.2025).

3. Мазулевський О., Денесюк Р. Прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних // Тези доповідей Науково-практичної конференції «Інформаційно-аналітичне забезпечення органів військового управління: Проблемні питання та шляхи їх вирішення» НУОУ, 28.11.2024 р. С. 74–75.

4. Терейковський І., Корченко А. Інтелектуалізовані методи захисту інформації: нейронні мережі в захисті інформації : навч. посіб. КПІ ім. Ігоря Сікорського, 2022. 175 с.

5. Основні засади забезпечення інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах: затверджено Наказом Міністерства оборони України від 18.04.2024 № 248.

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 24.11.2025).

7. Про захист інформації в інформаційно-комунікаційних системах: Закон України (зі змінами) від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/ laws/show/80/94-%D0%B2%D1%80#Text.

8. Державний Стандарт України ISO/IEC 27000:2023. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Наказ ДП «УкрНДНЦ» від 17.08.2023 № 210.

9. Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021 (від 28.10.2021 № 16/320/21).

10. Перелік категорій кіберінцидентів. URL: https://cert.gov.ua/recommendation/ 16904 (дата звернення: 24.11.2025).

11. The Cyber Kill Chain® framework. Lockheed Martin. 2024. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата звернення: 24.11.2025).

12. Globally-accessible knowledge base of adversary tactics and techniques MITRE ATT&CK®. 2024. URL: https://attack.mitre.org/ (дата звернення: 24.11.2025).

DOI: 10.58254/viti.8.2025.10.124

УДК 621.39(06):004.056.55:623(06)

Максимов І. О. ORCID: 0000-0002-1285-2564 (НУОУ)
Загоровець О. В ORCID: 0009-0008-2566-9217 (ВІТІ ім. Героїв Крут)

АНАЛІЗ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Інформаційно-комунікаційні системи військового призначення відіграють ключову роль у забезпеченні планування, координації та оперативного управління підрозділами Збройних Сил України в умовах ведення бойових дій. Одним з найважливіших завдань у таких системах є забезпечення достовірності та стійкості до перехоплення критично важливої інформації. Це зумовлює актуальність дослідження приховування інформації, зокрема стеганографічних, криптографічних та комбінованих методів забезпечення достовірності інформації.

У контексті зростаючих загроз, з боку засобів радіоелектронної боротьби та кібератак противника, виникає необхідність оцінки ефективності та практичного застосування кожного з методів. Проблематика дослідження полягає в тому, що окреме використання стеганографічного або криптографічного методів має низку обмежень, які можуть бути подолані шляхом їх інтеграції у вигляді комбінування.

Метою статті є систематизація та порівняльний аналіз сучасних методів приховування інформації в інформаційно-комунікаційних системах військового призначення, а також обґрунтування доцільності застосування комбінованого методу як найбільш ефективного для захисту обміну та змісту інформаційних повідомлень в умовах сучасного інформаційного протиборства.

У ході дослідження застосовано методи порівняльного аналізу, критичного огляду літературних джерел та системного узагальнення. У статті проаналізовано основні види стеганографічних і криптографічних методів, охарактеризовано їхні ключові переваги та недоліки, представлено структурну схему комбінованого методу та проведено оцінку ефективності за основними критеріями: стійкість до виявлення, ресурсоємність, швидкість передачі, можливість застосування в бойових умовах.

Результати дослідження свідчать про те, що комбіновані методи забезпечують багаторівневий захист даних, що суттєво ускладнює перехоплення, аналіз або модифікацію інформаційного потоку. Вони дозволяють знизити ризики виявлення самої передачі повідомлення та забезпечити захист його змісту навіть у разі компрометації каналу зв'язку. Обґрунтовано доцільність широкого впровадження комбінованих методів приховування інформації в інформаційно-комунікаційні системи військового призначення з урахуванням рівня управління, умов бойової обстановки та потенційних загроз.

Перспективним напрямом подальших досліджень є розроблення методики оцінювання достовірності інформації в ІКС ВП на основі визначення показників із врахуванням сучасних методів приховування інформації в інформаційно-комунікаційних системах військового призначення

Ключові слова: *інформаційно-комунікаційна система, приховування інформації, стеганографія, криптографія, комбіновані методи, конфіденційність, достовірність.*

I. Maksymov, O. Zahorovets. Methods of information hiding in military communication and information systems: analysis and prospects

Military information and communication systems play a key role in ensuring the planning, coordination, and operational command of the Armed Forces of Ukraine units in combat conditions. One of the most critical tasks in such systems is to ensure the authenticity and resistance to interception of mission-critical information. This underscores the relevance of researching information hiding, particularly steganographic, cryptographic, and combined methods for ensuring information integrity.

In the context of growing threats from enemy electronic warfare and cyberattacks, the need arises to evaluate the effectiveness and practical application of each method. The research problem lies in the fact that the separate use of steganographic or cryptographic methods has a number of limitations that can be overcome through their integration in a combined approach.

The purpose of the article is to systematize and comparatively analyze modern methods of information hiding in military information and communication systems, as well as to substantiate the expediency of using a combined method as the most effective for protecting the exchange and content of information messages in the conditions of modern information warfare.

The study employed methods of comparative analysis, critical literature review, and systemic generalization. The article analyzes the main types of steganographic and cryptographic methods, characterizes their key advantages and disadvantages, presents a block diagram of the combined method, and evaluates its effectiveness based on key criteria: resistance to detection, resource intensity, transmission speed, and applicability in combat conditions.

The research results indicate that combined methods provide multi-layered data protection, which significantly complicates the interception, analysis, or modification of the information flow. They allow for reducing the risks of detecting the message transmission itself and ensure the protection of its content even if the communication channel is compromised. The feasibility of widespread implementation of combined information hiding methods in military information and communication systems is substantiated, taking into account the command level, combat environment conditions, and potential threats.

A promising area for further research is the development of a methodology for assessing information integrity in military information and communication systems, based on defining indicators that consider modern methods of information hiding.

Keywords: *information and communication system, information hiding, steganography, cryptography, combined methods, confidentiality, authenticity.*

Постановка проблеми. Аналіз досвіду застосування інформаційно-комунікаційних систем військового призначення (ІКС ВП) в умовах бойових дій на території України свідчить про критичне значення захищеного обміну інформацією для успішного виконання бойових завдань. Особливої актуальності набуває використання комплексних методів приховування інформації, що включають як криптографічне шифрування даних, так і стеганографічне приховування самого факту передачі повідомлень.

Широкомасштабне вторгнення продемонструвало системне застосування противником комплексних методів радіоелектронної боротьби, кібератак та засобів радіоелектронної розвідки, що призводить до дезорганізації системи управління військами та порушення ієрархічної структури проходження критично важливої інформації. Встановлено, що російські підрозділи радіоелектронної боротьби (РЕБ) цілеспрямовано блокують канали обміну даними між штабами та підрозділами, створюють завади для супутникової навігації, а також здійснюють масоване придушення радіозв’язку на тактичному та оперативному рівнях. Одночасно з цим зафіксовано численні випадки використання російськими кіберпідрозділами стеганографічних методів для прихованої передачі шкідливого коду та команд управління зловмисним програмним забезпеченням (ПЗ) [1].

Варто зазначити, що російська федерація активно застосовувала методи захисту та приховування інформації ще до початку широкомасштабного вторгнення. Яскравим прикладом стала кібератака "NotPetya" у 2017 році, коли технології стеганографії використовувались для інтеграції шкідливого коду в оновлення бухгалтерського програмного забезпечення, а криптографічні механізми забезпечували захист каналів управління шкідливим ПЗ. Після повномасштабного вторгнення було зафіксовано нові випадки застосування комплексних підходів приховування інформації, зокрема: впровадження шкідливого програмного забезпечення "Armageddon" через вбудований у зображення код, який активувався при перегляді контенту на інформаційних ресурсах; використання стеганографії в поєднанні з асиметричним шифруванням у модифікованих документах MS Office, які розповсюджувалися через фішингові атаки на урядові установи; приховування шифрованих команд управління для ботнет-мереж у метаданих зображень, розміщених на публічних ресурсах, що дозволяло обходити системи виявлення мережевої активності.

У 2022 році було задокументовано діяльність хакерської групи Worok, яка використовувала стеганографію для приховування шкідливого коду в графічних файлах формату PNG. Такий код активувався після обробки зображення зараженою системою та дозволяв отримувати контроль над пристроєм жертви без виявлення з боку традиційних засобів кіберзахисту [2].

Підрозділи Збройних Сил України активно впроваджують багаторівневі методи захисту та приховування інформації для підвищення безпеки власних комунікацій. Практичне застосування включає інтеграцію шифрованих повідомлень у голосові пакети протоколів реального часу (Real-time Transport Protocol, RTP), використання цифрових водяних знаків у медіафайлах із додатковим криптографічним захистом та спеціалізовані застосунки для прихованої передачі координат, інформації розвідки та оперативних даних. Комплексні

програмні рішення на основі OpenStego, DeepSound та rSteg у поєднанні з сучасними криптографічними протоколами стали важливими інструментами у забезпеченні достовірності та цілісності військових комунікацій.

Противник активно використовує технології Deep Packet Inspection (DPI) для виявлення фактів прихованої передачі даних навіть у зашифрованому трафіку, а також засоби криптоаналізу для спроб дешифрування перехоплених повідомлень. Сучасні методи стегоаналізу дозволяють виявляти статистичні аномалії, що виникають при вбудовуванні додаткової інформації в цифрові контейнери. Зафіксовано випадки цілеспрямованого глушіння каналів зв’язку та модифікації інформаційних потоків з метою пошкодження прихованих повідомлень і криптографічних ключів.

Аналіз останніх досліджень і публікацій. Аналіз наукових праць у сфері захисту інформації свідчить, що значна увага дослідників приділяється фундаментальному вивченню окремих методів приховування. Зокрема, праці українських вчених [3–5] містять ґрунтовний розгляд теоретичних і практичних основ стеганографії. Водночас криптографічні підходи, їхні математичні принципи та застосування детально висвітлено у роботі [6]. Ці публікації створюють міцний теоретичний базис, проте розглядають криптографію та стеганографію переважно як самостійні дисципліни.

Світова наукова спільнота активно розвиває інноваційні та вузькоспеціалізовані рішення спрямовані на створення доказово безпечних алгоритмів [7], підвищення пропускної спроможності каналів прихованої передачі [8] та розробку нових підходів безконтейнерної стеганографії [9]. Попри високу наукову цінність, ці роботи є розрізненими і не пропонують комплексного аналізу, який би дозволив адаптувати та систематизувати сучасні досягнення для потреб військових систем зв’язку.

У роботах [10] та [11] розглядаються комбіновані крипто-стеганографічні підходи, проте проведений аналіз має переважно фрагментарний характер та обмежується прикладами застосування без розробки системної методології для порівняльної оцінки їх ефективності. Питання комплексного застосування цих методів, особливо в контексті специфічних вимог до ІКС ВП, висвітлено недостатньо, що унеможливлює обґрунтований вибір оптимального методу для конкретних бойових завдань та умов функціонування.

Таким чином, існує потреба у проведенні системного аналізу методів приховування інформації, який би враховував їхні переваги й недоліки саме в контексті військового застосування.

Метою роботи є проведення порівняльного аналізу методів приховування інформації в інформаційно-комунікаційних системах військового призначення, визначення їх основних переваг та недоліків для удосконалення захисту військових комунікацій в умовах інформаційного протиборства.

Виклад основного матеріалу дослідження. Одним із найбільш поширених і перспективних методів до приховування інформації є стеганографія. Він базується на прихованні повідомлень у цифрових носіях, таких як зображення, аудіо- чи відеофайли, наявність котрих залишається непомітною для сторонніх осіб.

Актуальність використання стеганографічних методів значно зросла у зв’язку із збільшенням загроз в умовах сучасної інформаційної боротьби під час планування та виконання завдань підрозділами Збройних Сил України. Основні принципи цих методів охоплюють комплексний підхід для впровадження, збереження та захисту прихованих даних, забезпечуючи прозорість та безпеку обміну інформацією.

В основі стеганографії лежить принцип приховування самого факту існування таємного повідомлення шляхом його інтеграції у звичайні, на перший погляд, файли. Такі файли-носії називаються контейнерами, якими можуть виступати цифрові зображення, аудіо- та відеозаписи або навіть текстові документи.

Ключовою вимогою, що визначає ефективність будь-якого стеганографічного методу, є непомітність (прозорість) втручання. Для досягнення непомітності використовують надлишковість даних у цифрових контейнерах. При цьому внесені зміни не повинні візуально погіршувати якість зображення, спотворювати звучання аудіофайлу чи бути помітними для читача тексту (контейнер має залишатися функціонально та візуально ідентичним до оригіналу) [5].

Вибір конкретного методу приховування залежить від балансу між обсягом даних, необхідним рівнем стійкості до виявлення та типом контейнера. Залежно від способу роботи з контейнером, методи поділяють на просторові, частотні та адаптивні.

Розглянемо основні типи стеганографічних методів, які використовуються для приховування інформації.

1. Стеганографія у зображеннях:

1) метод Least Significant Bit (LSB) – здійснює заміну найменш значущих біт у зображенні на біти прихованої інформації [9] згідно з виразом (1):

$$C` = (C \wedge \neg 1) \vee m, \tag{1}$$

де C – вихідне значення байта контейнера;

$C`$ – нове значення байта контейнера після вбудовування;

m – один біт секретного повідомлення;

$\wedge$ – побітова операція ‘‘І’’;

$\vee$ – побітова операція ‘‘АБО’’;

$\neg$ – побітова операція ‘‘НЕ’’;

2) метод Spread Spectrum (SS) – приховує дані шляхом розподілу їх серед великої кількості пікселів за випадковим алгоритмом [9], створюючи результуючий сигнал $T(t)$, що передається в канал зв’язку та наведено у виразі (2):

$$T(t) = S(t) \cdot C(t), \tag{2}$$

де $S(t)$ – вихідний інформаційний сигнал;

$C(t)$ – псевдовипадкова кодова послідовність, швидкість значно вища за швидкість S(t);

3) метод Discrete Cosine Transform (DCT) – вбудовує приховані дані у частотні компоненти зображення (зокрема у JPEG-файлах), змінюючи амплітуду низькочастотних коефіцієнтів для стійкості до стиснення [12] згідно з формулою (3):

$$X[k] = \alpha(k) \sum_{n=0}^{N-1} x[n] \cos\left(\frac{\pi(2n+1)k}{2N}\right), \tag{3}$$

де $x[n]$ – вхідна послідовність даних, де n ==0, 1, …, $N-1$;

N – кількість елементів у послідовності;

$\alpha(k)$ – коефіцієнт нормалізації представлений виразом (4):

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{N}} & \text{якщо } k = 0 \\ \sqrt{\frac{2}{N}} & \text{якщо } k > 0 \end{cases}. \tag{4}$$

2. Стеганографія в аудіо:

1) метод ехо-модуляції (ЕМ) – приховує дані шляхом додавання слабкого відлуння до аудіосигналу, змінюючи затримку та амплітуду для мінімального впливу на сприйняття звуку [13]. Модифікований сигнал (із вбудованим ехом) у момент часу *t* представлено у виразі (5):

$$s'(t) = s(t) + \alpha \cdot s(t - d), \tag{5}$$

де $s(t)$ – вихідний аудіосигнал у момент часу *t*;

α – амплітуда еха, де $0 < \alpha < 1$. Вона має бути нижчою за поріг сприйняття слухача;

d – затримка еха в часі;

2) метод Phase Coding (PhC) – вбудовує інформацію шляхом модифікації початкової фази аудіосигналу, що робить зміни практично непомітними для людського вуха [14] відповідно до виразу (6):

$$\phi_i^{`}(f) = \begin{cases} \phi_{i-1}(f) + \frac{\pi}{2}, & \text{якщо } m = 1 \\ \phi_{i-1}(f) - \frac{\pi}{2}, & \text{якщо } m = 0 \end{cases}; \tag{6}$$

3) метод Spread Spectrum Audio Steganography (SSAS) – розподіляє приховані дані по всьому частотному спектру аудіофайлу, що забезпечує високу стійкість до спотворень та атак [15] згідно з виразом (7):

$$S(t) = A(t) + \alpha \cdot \big(M(t) \cdot C(t)\big), \tag{7}$$

де $A(t)$ – вихідний аудіосигнал;

$M(t)$ – сигнал секретного повідомлення;

$C(t)$ – псевдовипадкова послідовність, швидкість набагато вища за швидкість $M(t)$;

α – коефіцієнт амплітуди (регулює гучність прихованого сигналу).

3. Стеганографія в тексті:

1) метод синонімічної стеганографії – приховує інформацію шляхом заміни слів у тексті на їхні синоніми, зберігаючи зміст, але модифікуючи структуру повідомлення;

2) метод Whitespace Steganography (WS) – використовує непомітні для читача пробіли, табуляції та переноси рядків для кодування прихованих даних у текстовому файлі;

3) метод зміни порядку слів – модифікує текст, переставляючи слова або фрази так, щоб це не змінювало сенс, але дозволяло передавати додаткову інформацію [16].

У таблиці 1 наведено найбільш поширені методи стеганографії, що застосовуються для приховання інформації в цифрових зображеннях, аудіофайлах і текстових документах.

Таблиця 1

Методи стеганографії в зображенні, аудіо та тексті

Тип носія	Методи стеганографії	Переваги	Недоліки
Зображення	LSB	Мінімальна зміна зображення	Легко виявляється статистичним аналізом
	SS	Висока стійкість до атак	Висока складність реалізації
	DCT	Найменш помітний для аналізу	Потребує обчислювальних ресурсів
Аудіо	ЕМ	Висока стійкість до виявлення	Потребує точного налаштування параметрів

Тип носія	Методи стеганографії	Переваги	Недоліки
	PhC	Важко виявити зміни	Висока складність реалізації
	SSAS	Захист від шумів та спотворень	Потребує великого обсягу даних
Текст	Синонімічна стеганографія	Використовує заміну слів на синоніми	Обмежена кількість інформації для приховування
	WS	Легке впровадження, малопомітність	Легко виявляється при аналізі форматування
	Зміна порядку слів	Висока стійкість до виявлення	Може викликати зміни в змісті

Стеганографічні методи приховування інформації мають як переваги, так і недоліки, що визначають їх ефективність у різних умовах. До основних переваг можна віднести непомітність передачі даних, оскільки прихована інформація інтегрується у цифрові контейнери так, що її існування важко виявити навіть за умов активного моніторингу. Також ці методи відзначаються гнучкістю у застосуванні, оскільки можуть використовувати різні типи контейнерів. Важливою перевагою є можливість їх поєднання з криптографічними технологіями, що дозволяє забезпечити як захист змісту повідомлення, так і приховування самого факту передачі даних. За умов правильного вибору алгоритму та контейнера, такі методи є досить стійкими до пасивних атак.

Одним із ключових недоліків є її висока чутливість до активних атак. При модифікації контейнера, шляхом стиснення або змін параметрів інформаційного повідомлення, може відбутись втрата прихованих даних, оскільки обсяг прихованої інформації залежить від розміру та типу обраного контейнера. Ефективність методу значною мірою залежить від відповідності контейнера умовам використання, що ускладнює його універсальність.

Існує базова схема процесу використання стеганографічних методів для приховування додаткової інформації, яка включає етапи вбудовування інформації у носій, передачу через стегоканал та подальше вилучення прихованого повідомлення на приймальному боці. Процес є двостороннім та потребує використання ключа як на етапі вбудовування, так і при вилученні інформації, що підвищує рівень захищеності передачі.

Стеганографічні методи мають значний потенціал для забезпечення конфіденційності в інформаційно-комунікаційних системах військового призначення. Їх практичне застосування потребує ретельного аналізу можливих загроз, обмежень та правильного вибору контейнера й алгоритму для досягнення максимальної ефективності.

Криптографічні методи є фундаментальним інструментом забезпечення конфіденційності та цілісності даних в ІКС ВП, головним завданням яких є перетворення інформації в шифротекст, що гарантує захист змісту повідомлення навіть у разі його перехоплення.

У сучасних системах застосовують симетричні та асиметричні методи криптографічних перетворень.

Симетричні криптографічні методи базуються на використанні одного й того ж секретного ключа як для шифрування, так і для дешифрування даних. Головною особливістю цих методів з сучасним стандартом симетричного шифрування є алгоритм Advanced Encryption Standard (AES), який широко використовується для захисту великих обсягів даних.

До основних переваг симетричних методів відносять високу швидкість роботи та відносно низькі вимоги до обчислювальних ресурсів, що дозволяє їх використовувати для шифрування файлів, баз даних та потокового трафіку, тощо. Основним недоліком є забезпечення безпечної передачі (розподіл) ключів, які мають бути відомі лише відправнику і отримувачу та збереження їх в таємниці від зловмисника [4].

Асиметричні криптографічні методи вирішують проблему розподілу ключів, використовуючи відкритий та закритий ключі, які математично пов’язані між собою.

Відкритий ключ вільно поширюється і використовується для шифрування даних, а закритий ключ зберігається в таємниці його власником і є єдиним засобом для дешифрування інформації, яка була зашифрована відповідним відкритим ключем. До асиметричних методів належать алгоритми Rivest–Shamir–Adleman (RSA) та Elliptic Curve Cryptography (ECC), які є основою для технологій цифрового підпису [6].

Основним недоліком асиметричних алгоритмів є висока обчислювальна складність та низька швидкість обробки великих обсягів даних.

У сучасних ІКС ВП, як правило, використовується гібридний підхід, що поєднує переваги обох методів. Асиметрична криптографія застосовується на початковому етапі для безпечної передачі симетричного ключа, після чого весь подальший обмін великими обсягами даних шифрується за допомогою швидкого симетричного алгоритму. Таке поєднання дозволяє ефективно протидіяти широкому спектру атак, але, попри високу надійність, супроводжується ризиком компрометації ключів, залежністю від продуктивності системи та потребою у своєчасному оновленні криптографічних протоколів.

Комбіновані методи приховування інформації поєднують криптографічні та стеганографічні підходи для підвищення рівня безпеки передачі інформаційних повідомлень. Сучасні методи комбінування можуть включати: шифрування перед стеганографією, подвійне приховування або розподіл секрету, що дозволяє досягти вищої безпеки та надійності передачі інформаційних повідомлень.

Основними характеристиками комбінованих методів є:

1. Ступінь прихованості (високий рівень прихованості забезпечується використанням ефективних алгоритмів стеганографії, які мінімізують помітність змін у цифровому контейнері);
2. Криптостійкість (залежить від складності використаного алгоритму шифрування);
3. Ресурсомісткість (застосування комбінованих технологій може збільшувати вимоги до обчислювальних ресурсів та впливати на швидкість обробки даних);
4. Стійкість до атак (визначає здатність методу протистояти розкриттю та спробам виявлення прихованої інформації).

На рисунку 1 подано структурну схему процесу комбінованого методу приховування інформації, який поєднує стеганографічні та криптографічні підходи.

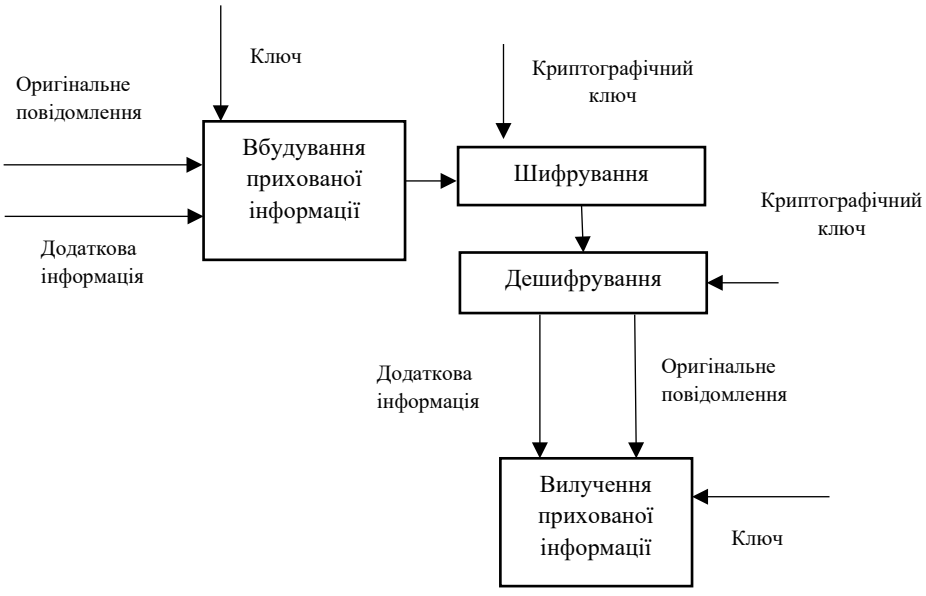


Рис. 1. Структурна схему процесу комбінованого методу приховування інформації

Перевагою комбінованих методів є подвійний рівень безпеки, оскільки інформація не лише шифрується, а й приховується, що ускладнює її перехоплення та аналіз. Такі методи забезпечують захист від аналізу трафіку, оскільки приховують сам факт передавання конфіденційних інформаційних повідомлень. Однак їх застосування може бути обмежене високими вимогами до продуктивності та складністю реалізації, особливо в системах з обмеженими ресурсами.

В таблиці 2 наведено порівняння методів приховування інформації їх переваги та недоліки

Таблиця 2

Порівняння методів приховування інформації

Метод	Переваги	Недоліки	Ключові характеристики
Стеганографія	Прихованість каналу передачі; Стійкість до виявлення засобами розвідки	Низька пропускна спроможність; Чутливість до зміни контейнера; Вразливість до стегоаналізу	Використовує для приховування зображення, аудіо, текст тощо
Криптографія	Надійний захист змісту; Гарантія цілісності даних; Автентифікація відправника	Складність правильної реалізації та масштабованість; Складність управління ключами; Високі обчислювальні витрати	Шифрування інформації, яка передається через відкриті канали зв’язку
Комбінований метод	Багаторівневий захист; Конфіденційність при виявленні; Максимальна стійкість	Складність реалізації; Високі вимоги до ресурсоємності; Успадкування вразливостей	Включає одночасно приховування та шифрування даних

Доцільність використання комбінованих методів приховування інформації обумовлена потребою в підвищеному рівні безпеки даних у ІКС ВП та кібербезпеці. У військових системах вони застосовуються для захисту стратегічно важливих інформаційних повідомлень, а в корпоративних мережах – для запобігання витоку критично важливої інформації. Таким чином, комбіновані методи є перспективним напрямом у сфері інформаційної безпеки, що поєднує переваги криптографії та стеганографії, проте вимагає ретельного підходу до вибору алгоритмів та їхньої реалізації.

Теоретичною основою для наведених оцінок слугували наукові праці, що аналізують як окремі підходи – стеганографію [3, 5] та криптографію [2, 4], – так і ефективність їх поєднання у комбінованих методах [12, 13]. З урахуванням цих факторів, таблиця 3 допоможе оцінити ефективність різних підходів за основними критеріями, де 1 – погано, 5 – дуже добре.

Таблиця 3

Оцінка ефективності методів з приховування інформації

Умова	Стеганографія	Криптографія	Комбінований метод
Висока швидкість передавання	4	3	4
Стійкість до виявлення	5	4	5
Ресурсоємність	3	4	4

Результати порівняльного аналізу окремих та комбінованих підходів приховування інформації дозволяють сформулювати ключові висновки щодо їх ефективності у ІКС військового призначення.

Висновки. У статті проведено порівняльний аналіз сучасних методів приховування інформації в інформаційно-комунікаційних системах військового призначення. Комбіновані методи, які поєднують криптографічні та стеганографічні підходи приховування інформації, дозволяють створити багаторівневий захист, який суттєво ускладнює виявлення та

розшифрування критично важливої інформації. Така інтеграція забезпечує не лише конфіденційність та цілісність даних, але й прихованість самого факту обміну інформацією. Проведена оцінка ефективності підтвердила їхню доцільність для використання в умовах сучасного інформаційного протиборства. Однак, впровадження таких методів супроводжується певними обмеженнями, зокрема збільшенням обчислювального навантаження, затримками передачі даних та необхідністю балансувати між рівнем захисту та ефективністю системи.

Перспективним напрямом подальших досліджень є розроблення методики оцінювання достовірності інформації в ІКС ВП на основі визначення показників із врахуванням сучасних методів приховування інформації в інформаційно-комунікаційних системах військового призначення, що дозволить забезпечити більш комплексну оцінку ефективності захисних механізмів та підвищити стійкість комунікацій у бойових умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Maurer T., Janz J. Cyber and Information Warfare in the Ukrainian Conflict / T. Maurer, J. Janz. Zurich: Center for Security Studies, ETH Zurich, 2018. 36 p. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf (дата звернення: 23.09.2025).

2. Яковенко С. В. Криптографія та стеганографія в інформаційних системах. Л.: Сполом, 2021. 315 с.

3. Жежнич П. Я. Методи та засоби стеганографії: основи теорії та практики. Л.: Вид-во ЛНУ, 2015. 312 с.

4. Романчук О. П. Захист інформації: криптографічні та стеганографічні методи. К.: Наукова думка, 2018. 284 с.

5. Кривошей Д. В. Технології приховування інформації: сучасний стан та перспективи. К.: Політехніка, 2019. 298 с.

6. Дудник В. С. Математичні основи захисту інформації. К.: КНУ ім. Т. Шевченка, 2019. 280 с.

7. Wang B., Zhang M., Liu F., Niu X. SparSamp: efficient provably secure steganography based on sparse sampling / B. Wang, M. Zhang, F. Liu, X. Niu // arXiv.org: e-Print archive. 2024. URL: https://arxiv.org/abs/2401.03669 (дата звернення: 23.09.2025).

8. Kumar S., Kumar R., Singh A. K. A novel reversible data hiding scheme with high payload based on pixel value ordering and prediction error expansion / S. Kumar, R. Kumar, A. K. Singh // Multimedia Tools and Applications. 2023. Т. 82. С. 2825–2849.

9. Al-Juaid A. A., Gutub A. A. A novel generative mathematical model for container-less steganographic system based on image generation / A. A. Al-Juaid, A. A. Gutub // IEEE Access. 2023. Т. 11. С. 83615–83630.

10. Бєляєв А. В. Захист інформації: комбіновані методи криптографії та стеганографії. Х.: Фоліо, 2021. 290 с.

11. Петренко О. В. Технології безпеки інформації у військових системах зв’язку. К.: МО України, 2016. 250 с.

12. Mohammed S. H., Othman W. M. Solvability and nilpotency of Lie algebras in cryptography and steganography / S. H. Mohammed, W. M. Othman // Journal of Computer Science and Technology Studies. 2024. Т. 6, № 1. С. 44–53.

13. Hasan Z. A., Jassim W. K. Steganographic cryptosystem based on the use of chaos theory and cellular automata / Z. A. Hasan, W. K. Jassim // Engineering and Technology Journal. 2024. Т. 42, № 3. С. 382–392.

14. Kumar S., Kumar R., Singh A. K. A novel reversible data hiding scheme with high payload based on pixel value ordering and prediction error expansion / S. Kumar, R. Kumar, A. K. Singh // Multimedia Tools and Applications. 2023. Т. 82. С. 2825–2849.

15. Гончарук В. І. Основи кіберзахисту інформаційних систем. О.: ОНПУ, 2017. 270 с.

16. Барановський О. М. Інформаційна безпека та захист інформації: теорія і практика. Х.: ХНУРЕ, 2020. 356 с.

DOI: 10.58254/viti.8.2025.11.133

УДК 004.8:004.021.64:519.85

Меркотан Д. Ю. ORCID: 0000-0003-1425-9948 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Троцько О. О. ORCID: 0000-0001-7535-5023 (ВІТІ ім. Героїв Крут)

МЕТОД ГРАФОВОГО ЗЛИТТЯ МУЛЬТИМОДАЛЬНИХ ДАНИХ З ВИКОРИСТАННЯМ БАГАТОЗАДАЧНОГО НАВЧАННЯ

У реальних умовах дані зазвичай містять декілька модальностей та можуть мати неексклюзивні мітки. Ключовим етапом мультимодального навчання є процес злиття мультимодальної інформації, оскільки він забезпечує об’єднання ознак з різних джерел у спільний векторний простір. Це дає змогу класифікатору використовувати сформований інтегрований вектор для отримання кінцевого прогнозу. Водночас традиційні методи мультимодального злиття рідко беруть до уваги міжмодальні взаємодії, які відіграють важливу роль у виявленні залежностей між модальностями та побудові єдиного простору їх інтеграційного представлення.

У цій роботі запропоновано метод графового злиття мультимодальних даних з використанням багатозадачного навчання. Він спрямований на формування спільного простору інтеграційного представлення для всіх міжмодальних взаємодій та на адаптивне налаштування функцій втрат окремих завдань з метою досягнення оптимальних показників ефективності обробки мультимодальних даних. Розроблений метод використовує вдосконалену графову мережу мультимодального злиття, яка враховує міжмодальні взаємодії між усіма комбінаціями модальностей та динамічно розподіляє вагові коефіцієнти для кожної пари модальностей залежно від конкретного зразка даних. Крім того, впроваджено новий підхід багатозадачного навчання для розв’язання проблем багатомітковості шляхом автоматичного регулювання процесу навчання, як на рівні завдань, так і на рівні окремих зразків.

Експериментальні результати засвідчують, що запропонований метод перевищує ефективність базових моделей та окремих сучасних методів. Також продемонстровано гнучкість і модульність запропонованих компонентів мультимодального злиття та динамічного багатозадачного навчання, що дозволяє інтегрувати їх у різні типи нейронних мереж.

Ключові слова: *машинне навчання, злиття даних, мультимодальне злиття, обробка даних, багатозадачне навчання, штучний інтелект, нейронні мережі, інформаційні системи.*

D. Merkotan, O. Trotsko. Method of graph fusion of multimodal data using multitask learning

In real-world conditions, data typically contain multiple modalities and may have non-exclusive labels. A key stage of multimodal learning is the process of multimodal fusion, as it enables the integration of features from different sources into a unified vector space. This allows the classifier to utilize the constructed integrated vector to produce the final prediction. At the same time, traditional multimodal fusion methods rarely take into account cross-modal interactions, which play an essential role in uncovering dependencies between modalities and in constructing a shared space of their integrated representation.

In this paper, we propose a conceptual framework for multimodal fusion with the use of multi-task learning. It is aimed at modeling a joint integrated representation space for all cross-modal interactions and adaptively tuning the loss functions of individual tasks in order to achieve optimal performance. The developed model employs a novel hierarchical multimodal fusion network that captures cross-modal interactions across all modality combinations and dynamically allocates weight coefficients for each pair depending on the specific data sample.

In addition, a new multi-task learning approach is introduced to address multi-label classification challenges by automatically adjusting the training process both at the task level and at the sample level. Experimental results demonstrate that the proposed conceptual framework outperforms baseline models as well as several state-of-the-art methods. Furthermore, the flexibility and modularity of the proposed components of multimodal fusion and dynamic multi-task learning are showcased, making them applicable to various types of neural network architectures.

Keywords: *machine learning, data fusion, multimodal fusion, data processing, multi-task learning, artificial intelligence, neural networks, information systems.*

Актуальність та постановка завдання в загальному вигляді. Мультимодальне навчання привертає значну увагу наукової спільноти завдяки своїй здатності ефективно використовувати великі обсяги реальних даних, що зазвичай містять декілька джерел інформації [1–6]. На відміну від підходів з використанням лише однієї модальності, мультимодальне навчання орієнтоване на розкриття багатого інформаційного потенціалу, що міститься у різних вхідних модальностях.

Одним із ключових етапів мультимодального навчання є злиття даних із різних модальностей, у процесі якого вхідні ознаки кожної модальності об’єднуються для формування єдиного векторного представлення. Відтак спосіб, у який здійснюється злиття ознак, суттєво впливає на здатність моделі ефективно засвоювати інформацію, надану кількома джерелами вхідних даних.

На відміну від традиційного уявлення, просте збільшення кількості вхідних модальностей не завжди приводить до кращих результатів [5]. Основною причиною зниження ефективності є ігнорування міжмодальних взаємодій.

Ефективне злиття представлень різнорідних модальностей перетворилося на актуальну проблему мультимодального навчання та, відповідно, привернуло значну увагу наукової спільноти. Гетерогенна природа мультимодальних даних створює суттєвий бар’єр на шляху до використання повної сукупності інформації з усіх модальностей, що є ключовим для глибокого розуміння та ефективного застосування насичених мультимедійних даних [7].

Перші спроби мультимодального злиття ґрунтувалися на окремому опрацюванні кожної модальності. Кожна модальність опрацьовувалася у власній мережі, а проміжні ознаки поєднувалися на різних етапах обробки – зокрема у формах раннього злиття та пізнього злиття [8]. Однак через гетерогенність мультимодальних даних та відсутність узгодженості між мережами, отримане інтегроване векторне представлення виявляється недостатнім для відображення складного розподілу між модальностями.

Багатозадачне навчання є технікою, що набула значної популярності у сфері машинного та глибокого навчання, багатоміткового навчання й багатовимірної регресії [9]. Багатозадачне навчання використовує переваги ширшого охоплення різних предметних областей шляхом одночасного вирішення кількох завдань. Такий підхід довів свою високу ефективність у багатьох сценаріях, оскільки дає змогу сформувати більш узагальнену та стійку модель. Це досягається завдяки спільному використанню знань між завданнями та зменшенню ризику перенавчання.

Відкритим питанням у багатозадачному навчанні залишається проблема балансування процесу навчання між завданнями. Поширеною практикою є призначення однакових ваг для всіх завдань або ж евристичне вагове налаштування функцій втрат кожного завдання. Перше рішення часто призводить до погіршення результатів, коли одне завдання починає домінувати у процесі навчання через надмірне значення функції втрат, що може бути зумовлене як самою функцією, так і складністю завдання. Друге рішення повністю залежить від людського судження, що обмежує його гнучкість у застосуванні до різних проблемних доменів і зазвичай потребує ресурсозатратного процесу підбору ваг.

З огляду на викладене, актуальним є **наукове завдання** щодо розроблення методів, які поєднують мультимодальне злиття з динамічним багатозадачним навчанням. Такий підхід має забезпечити ефективну інтеграцію ознак із різних модальностей та адаптивне балансування вагових коефіцієнтів завдань упродовж навчання, що дозволить уникнути домінування окремих завдань і підвищити загальну якість обробки мультимодальних даних.

Аналіз останніх досліджень і публікацій. Традиційне мультимодальне злиття зазвичай реалізується на трьох рівнях: раннє злиття, пізнє злиття та гібридне злиття.

Раннє злиття зазвичай здійснюється шляхом конкатенації необроблених або попередньо оброблених ознак кожної модальності безпосередньо після етапу вилучення ознак [10–12]. Такий підхід є простим у реалізації та потребує менш складної мережевої структури. Водночас раннє злиття стикається з труднощами у випадках, коли одна з модальностей представлена безперервним потоком даних, тоді як інша — дискретними даними. Крім того, зі зростанням кількості модальностей суттєво ускладнюється навчання міжмодальних взаємодій між гетерогенними ознаками.

Пізнє злиття передбачає використання декількох моделей для формування модально-специфічних предикативних оцінок. Надалі ці оцінки аналізуються й комбінуються для

отримання остаточного рішення [13–16]. Пізнє злиття має низку переваг порівняно з раннім. По-перше, моделі, орієнтовані на окремі модальності, дають змогу навчатися різним семантичним представленням для кожної модальності. По-друге, застосування пізнього злиття дозволяє використовувати переваги доменно-специфічних моделей і алгоритмів, наприклад, застосування моделей на основі згорткових нейронних мереж (CNN) для візуальних даних або моделей на основі рекурентних нейронних мереж (RNN) для послідовних даних. Проте пізнє злиття не враховує міжмодальні взаємодії на рівні ознак, що призводить до втрати критично важливої міжмодальної інформації.

Гібридне злиття поєднує переваги раннього та пізнього підходів, перетворюючи необроблені вхідні дані на представлення вищого рівня, що спрощує процес злиття різних модальностей і сприяє навчанню міжмодальних представлень [17; 18].

Останнім часом метод тензорного злиття привернув увагу значної кількості науковців. Тензорне злиття вирішує проблему гетерогенного розподілу даних у мультимодальному навчанні шляхом злиття кожної модальності на рівні тензора. У результаті модель здобуває можливість навчатися з урахуванням деталізації міжмодальних взаємодій. Тензорне злиття продемонструвало перспективні результати у сфері глибокого мультимодального навчання для завдань візуального питання-відповіді [19] та аналізу сентиментів [20].

Беньйоунес та інші запропонували концептуальну структуру для розв’язання задачі візуальної відповіді на запитання [19]. Вони екстрагували ознаки як із візуальних зображень, так і з текстових запитань за допомогою GRU (Gated Recurrent Unit) та ResNet [21]. Далі ознаки об’єднувалися із застосуванням методу тензорного злиття. У процесі злиття використовувався підхід тензорної декомпозиції Такера для параметризації кореляції тензорів між візуальними та текстовими представленнями. В іншій роботі Жао та інші [22] застосували мультиагентний тензорний шар і згорткове злиття для фіксації міжмодальних взаємодій.

Моделі злиття на основі графів перетворюють модальності та взаємодії між ними у графи злиття. Ознаки кожної модальності розглядаються як вершини, а взаємозв’язки між ними реалізуються у вигляді ребер. Задех та інші використали динамічний граф злиття для моделювання *n*-модальної динаміки [23]. Порівняно з тензорним злиттям графове злиття досягає вищої ефективності навчання, оскільки вимагає значно меншої кількості параметрів. Крім того, графове злиття застосовує динамічні параметри для керування активацією певних ребер, тим самим динамічно змінюючи структуру мережі. Поєднання мультимодального метричного навчання та графового злиття використовується для оцінки подібності ознак між модальностями [24]. Чен та інші [25] запропонували гетерогенну графову мережу злиття, яка орієнтується на інтеграцію мультимодальних даних із відсутніми модальностями. Вона застосовує графову мережу для проєктування відсутніх даних разом з іншими модальностями у спільний простір інтеграційного представлення.

Багатозадачне навчання забезпечує низку переваг завдяки одночасному вирішенню кількох завдань. Окрім очевидної переваги скорочення часу навчання за рахунок виконання лише одного циклу, воно також допомагає моделі формувати більш узагальнене представлення всієї предметної області, що значно знижує ризик перенавчання [9]. Багатозадачне навчання демонструє великий потенціал у сфері мультимодального навчання. Сенер та інші [26] використали багатокритеріальну оптимізацію для пошуку Парето-оптимального розв’язку шляхом мінімізації зваженої комбінації функцій втрат завдань. Ху та Сінгх [27] використали механізм “кодер-декодер”, який кодує кожну вхідну модальність та декодує їх у спільний простір інтеграційного представлення.

Мета статті – розробка методу графового злиття мультимодальних даних з використанням багатозадачного навчання, який враховуватиме міжмодальні взаємодії, адаптивно налаштовуватиме функції втрат окремих завдань та автоматично регулюватиме процес навчання моделі, як на рівні завдань, так і на рівні окремих зразків вибірки.

Виклад основного матеріалу дослідження. Враховуючи аналіз, який був проведений в [6] та сформовані завдання, запропоновано метод графового злиття мультимодальних даних з використанням багатозадачного навчання, який складається з двох основних компонентів. Перший компонент – вдосконалена графова мережа злиття (ВГМЗ), яка вирішує завдання представлення ознак кожної модальності та їх об'єднання. Другий компонент – модуль динамічного багатозадачного навчання (ДБН), який на основі спільних ознак, сформованих першим компонентом, регулює процес вирішення кожного окремого завдання.

Графова мережа злиття. Спираючись на [28], сформовано графову мережу злиття, використовуючи *n*-модальні взаємодії. Графова мережа злиття об'єднує всі модальності на унімодальному, бімодальному та тримодальному рівнях і моделює взаємодії та відношення між кожною парою комбінацій. Загальний вигляд графової мережі злиття наведено на рисунку 1.

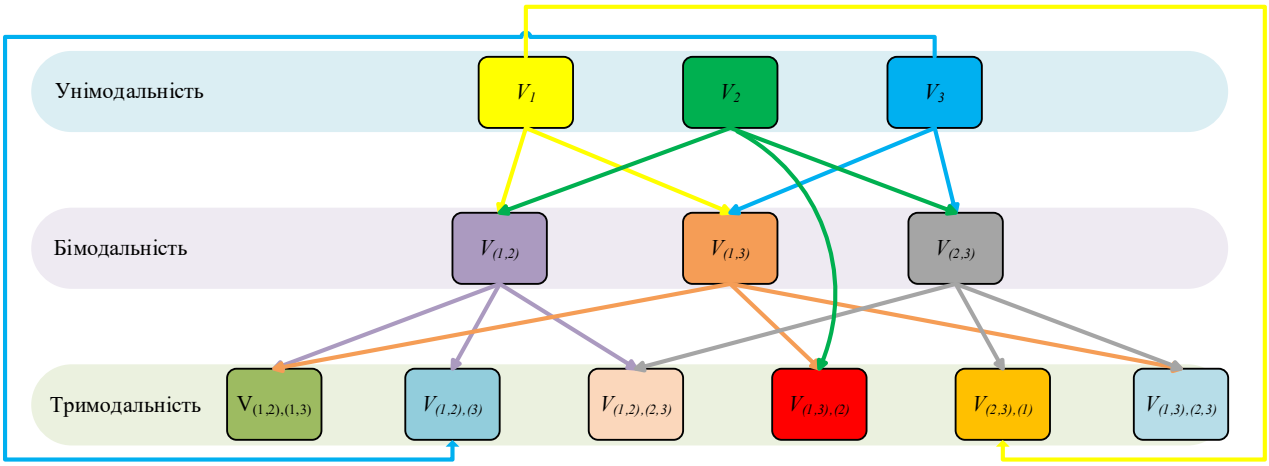


Рис. 1. Графова мережа злиття з трьома вхідними модальностями

Перший рівень графової мережі містить усі унімодальні вектори та їхні взаємодії. Унімодальний вхідний вектор ознак задано як Vi, де $i=[1,N]$, N – загальна кількість модальностей. Хоча графова мережа злиття може бути застосована до будь-якої кількості модальностей, надалі у статті прийнято обмеження для трьох модальностей, тобто $N=3$. Після попередньої обробки даних, застосовується паддінг для приведення векторів ознак різних модальностей до однієї розмірності. Далі вектори ознак з кожної модальності конкатенуються. Сформований вектор ознак подається до блока динамічної уваги – $\boldsymbol{B}$, який визначає значущість кожної модальності й призначає її як вагу для з'єднувальних ребер, він представлений нейронною мережею, що складається з двох згорткових шарів Conv 5×5 та Conv 1×1 і функцією активації LeakyReLU. Цей процес можна описати так:

$$w_1 \oplus w_2 \oplus \ldots \oplus w_N = \boldsymbol{B}(V_1 \oplus V_2 \oplus \ldots \oplus V_N), \quad (1)$$

де $\oplus$ – операція конкатенації; $V_1, V_2, \ldots, V_N$ – унімодальні вектори N-модальностей; w_1, w_2, w_N – відповідні ваги. $\boldsymbol{B}$ визначає динамічний коефіцієнт важливості, що має бути призначений кожному вектору у вибірково-залежний спосіб. Ці коефіцієнти важливості використовуються як основа для формування ваг ребер на вищих рівнях.

Фінальний унімодальний вектор рівня може бути отриманий як зважене середнє векторів усіх унімодальних вершин:

$$G_{unm} = \frac{1}{N}\sum_{i=1}^{N} w_i V_i. \quad (2)$$

На бімодальному рівні кожна пара унімодальних векторів об'єднується для формування вершин цього рівня. Для поєднання унімодальних векторів і побудови всіх бімодальних вершин використовується нейронна мережа – *NN*, що складається з одного одномірного згорткового шару та одного повнозв'язного шару з активацією LeakyReLU. Ця процедура описується так:

$$V_{(x,y)} = NN(V_x \oplus V_y) \quad \text{x=1, 2, ..., N; y=1, 2, ..., N; x≠y,} \tag{3}$$

де $V_{(x,y)}$ – бімодальний вектор.

Щодо ребер, які з'єднують вершини між унімодальним та бімодальним рівнями, припускається, що чим ближчі дві ознаки у векторному просторі, тим більш однорідною є інформація, яку вони містять. Отже, комбінація таких ознак не надає стільки додаткової інформації, як поєднання більш відмінних ознак. Виходячи з цього припущення, обчислюється подібність між кожною парою вершин на бімодальному рівні:

$$S_{x,y} = COS(\tilde{V}_x, \tilde{V}_y), \tag{4}$$

де $S_{x,y}$ позначає показник подібності між вершинами x та y, COS – функція косинусної подібності, а $\tilde{V}_x$ та $\tilde{V}_x$ – нормовані за допомогою нормованої експоненційної функції вектори V_x та V_y. Метою нормалізації є обмеження значень обох векторів у діапазоні від 0 до 1. Відповідно до нашого припущення, чим подібніші два вектори, тим меншу вагу вони повинні мати при об'єднанні. Іншими словами, вага ребра між двома вершинами має зростати оберненопропорційно до показника подібності.

Таким чином, вага ребра, що з'єднує вершину *x* на унімодальному рівні з вершиною *xy* на бімодальному рівні, обчислюється як $\frac{w_x}{S_{x,y}+\delta}$. Аналогічно, вага ребра, що з'єднує вершину *y* та *xy*, визначається як $\frac{w_y}{S_{x,y}+\delta}$.

Показник δ є регульованим коефіцієнтом, що контролює швидкість зростання й приймає значення в інтервалі від 0 до 1. На основі емпіричних досліджень у цій роботі використано значення δ = 0.5. Відповідно, вага вершини на бімодальному рівні формалізується як:

$$q_{x,y} = \frac{w_x + w_y}{S_{x,y} + \delta}, \quad w_{x,y} = \frac{e^{q_{x,y}}}{\sum_{j=1}^{N}\sum_{k=1,j\neq k}^{N} e^{q_{j,k}}}, \tag{5}$$

де $q_{x,y}$, є вагою вершини для $V_{(x,y)}$ на бімодальному рівні, а $w_{x,y}$ позначає нормовану за softmax форму $q_{x,y}$. Тоді остаточний об'єднаний вектор бімодального рівня можна подати так:

$$G_{bim} = \sum_{x=1}^{N}\sum_{y=1,x\neq y}^{N} w_{x,y} * V_{(x,y)}, \tag{6}$$

де G_{bim} – об'єднаний бімодальний вектор.

На тримодальному рівні всі обчислення подібні до процедури, наведеної для бімодальної частини. Формули (4)–(6) використовуються для обчислення показників подібності, ваг

вершин і об'єднаного тримодального вектора на цьому рівні. Тримодальний рівень містить два типи вершин:

комбінації бімодальних вершин;

поєднання кожної бімодальної вершини з унімодальною вершиною, яка не входила до складу цієї бімодальної вершини.

Таким чином, для набору даних із трьома вхідними модальностями загальна кількість вершин на тримодальному рівні становитиме 6.

На завершальному етапі об'єднані вектори з унімодального, бімодального та тримодального рівнів конкатенуються для формування остаточного об'єднаного вектора:

$$G_{summ} = G_{unm} \oplus G_{bim} \oplus G_{trm}. \tag{7}$$

Динамічне багатозадачне навчання. У багатозадачному навчанні підсумкова функція втрат обчислюється як лінійна комбінація втрат усіх завдань, що використовується для оптимізації параметрів моделі. Типові підходи багатозадачного навчання або призначають усім завданням однакові ваги, або ж визначають вагу для кожного завдання на основі емпіричних досліджень. В роботі запропоновано модуль динамічного багатозадачного навчання, здатний обчислювати та корегувати ваги функцій втрат як на рівні вибірки, так і на рівні завдань. Крім того, модуль здійснює повторне балансування початкових значень функцій втрат на кожному циклі навчання, аби уникнути потрапляння вагових коефіцієнтів у локальні мінімуми чи максимуми.

Модуль динамічного багатозадачного навчання на рівні вибірки має на меті надавати вищий пріоритет навчанню тих вхідних прикладів, які були класифіковані неправильно. Використовуючи кросс-ентропію, як функцію втрат, цей процес можна описати так:

$$H(p_d) = -\log(p_d), \tag{8}$$

$$p_d = \begin{cases} p, & \text{якщо } y = 1 \\ 1 - p, & \text{інакше} \end{cases}, \tag{9}$$

де $y \in \{0,1\}$ – істинна мітка, $a\ 0 \le p \le 1$ – ймовірність того, що зразок має мітку 1. Функція вагового коефіцієнта втрат на рівні вибірки L_s визначається як:

$$L_s(x) = -(1 - p_d)^{\beta} \log(p_d), \tag{10}$$

де x — це вхідні дані;

β — параметр фокусування на рівні вибірки, який контролює величину зменшення ваги для простих (істинно-негативних) зразків.

На основі емпіричних досліджень у цій роботі використано значення $\beta = 2$. Коли p_d є малим і зразок класифіковано неправильно, значення $(1 - p_d)^{\beta}$ наближається до 1, що має дуже обмежений вплив на функцію втрат. З іншого боку, зі збільшенням p_d величина $(1 - p_d)^{\beta}$ поступово прямує до 0, що зменшує втрати, породжені правильно класифікованими зразками. Це змушує модель приділяти більше ресурсів навчанню складних (хибно-негативних) зразків.

Для порівняння, модуль динамічного багатозадачного навчання на рівні завдань автоматично коригує ваги втрат, згенерованих кожною мережею, що відповідає за певне завдання. Функція втрат кожного завдання контролюється та використовується як метрика для регулювання зваженого градієнта в кожному шарі. В роботі застосовується спеціалізована функція втрат для мінімізації різниці між: градієнтами ваг серед усіх завдань та зваженим за

швидкістю навчання середнім градієнтом. L1-норма динамічної функції балансування втрат на рівні завдань, на ітерації навчання *t* визначається так:

$$L_D(t) = \sum_f \frac{M}{m_f} \left| G_W^{(f)}(t) - \bar{G}_W(t) \times \left[r_f(t) \right]^{\alpha} \right|_1, \quad (11)$$

де M представляє загальну кількість вибірок,

m_f – кількість позитивних зразків у завданні *f*;

$\frac{M}{m_f}$ – обернене співвідношення розподілу вибірки для завдання *f*;

W – ваговий параметр останнього шару мережі, специфічної для завдання;

$G_W^{(f)}(t)$ – *L2*-норма градієнта зваженої функції втрат завдання *f* на ітерації *t*;

$\bar{G}_W(t)$ – середній градієнт усіх завдань на ітерації *t*;

$r_f(t)$ – обернена швидкість навчання завдання *f*;

α – коефіцієнт, що контролює величину оберненої швидкості навчання.

У деяких випадках оновлення ваг функції втрат через обчислення динамічної функції балансування втрат може бути недостатнім, якщо складність завдань є надто нерівномірною. Це може уповільнити процес оновлення функцій втрат і призвести до потрапляння ваг деяких завдань у локальні мінімуми чи максимуми. Щоб розв'язати цю проблему, виконується повторне балансування ваг функцій втрат після завершення повного циклу навчання. Це забезпечує більш агресивний процес оновлення втрат, що допомагає моделі швидше досягти оптимальних ваг функцій втрат і уникнути їх потрапляння в локальні мінімуми чи максимуми.

На практиці середні значення функцій втрат для кожного завдання обчислюються протягом усього циклу навчання. Потім ваговий коефіцієнт генерується шляхом ділення найбільшого значення серед усіх середніх втрат на середню втрату кожного завдання. Нарешті, цей ваговий коефіцієнт застосовується до всіх завдань для повторного балансування втрат на початку циклу навчання. Відстежується втрата на валідаційній вибірці, і процес навчання зупиняється, якщо ця втрата перестає зменшуватися.

Оцінка ефективності запропонованого методу

CrisisMMD [29] – це мультимодальний мультимедійний набір даних із Twitter, який містить понад 16000 твітів і 18000 зображень, пов'язаних із сімома великими природними катастрофами. Кожен зразок анотовано за трьома групами концептів: інформаційний рівень даних, гуманітарна категорія та рівень руйнувань. Інформаційний рівень даних відображає обсяг корисної інформації, гуманітарна категорія охоплює тип гуманітарної кризи та заходи з ліквідації наслідків, що відбувалися на місці події, а рівень руйнувань – характеризує масштаб пошкоджень інфраструктури та комунальних об'єктів. Для цього набору даних подаються результати за метриками F1, HL та MAP. Для метрик F1 та MAP більші значення означають кращу якість моделі, тоді як для HL – нижчі значення є кращими.

Виділення візуальних ознак. Для обробки візуальних даних використовується методика InceptionV3 [30], попередньо навчена на наборі ImageNet [31], як екстрактор ознак.

Виділення текстових ознак. Для текстових даних використовується методика ELMo [32] для формування векторних уявлень слів. Порівняно з традиційними методами текстової векторизації, такими як Word2vec [33] та GloVe [34], ELMo здатний враховувати морфологічну інформацію та ефективніше працює з позасловниковими словами.

Розподіл даних для експерименту: 60 % даних використовується для навчання, 20 % – для валідації та 20 % – для тестування. Набір для валідації застосовується для налаштування всіх гіперпараметрів, а коефіцієнт α у динамічній функції втрат встановлюється рівним 1 на

основі емпіричних досліджень. Для оптимізації процесу навчання використовується алгоритм Adam [35], а початкова швидкість навчання встановлена на рівні 0,01.

Модуль динамічного багатозадачного навчання застосовується до трьох груп концептів у наборі даних CrisisMMD, де кожен концепт моделюється як окреме завдання. Це перетворює початкову задачу багатоміткової класифікації на задачу багатозадачного навчання.

Результати та обговорення. Для демонстрації ефективності запропонованої структури було обрано кілька базових методів, включно з найсучаснішими підходами.

Базові методи мультимодального злиття включають:

метод конкатенаційного злиття (КЗ), який виконує просту конкатенацію ознак кожної модальності безпосередньо після етапу початкового виділення ознак;

тензорний метод злиття (ТМЗ) [21];

графова мережа злиття (ГМЗ) [27].

Базові методи для багатозадачного навчання включають:

лінійна сума функцій втрат із рівними вагами (ЛСРВ);

багатооб'єктна оптимізація (БОО) [25];

багатомасштабні мережі взаємодії завдань (БМВЗ) [36].

Для цілей порівняння у кожному базовому методі нижчі рівні моделі замінено на вищезгадані попередньо навчені моделі.

Мультимодальне злиття. У таблицях 1, 2 та 3 наведено результати ефективності запропонованого методу, а також базових методів для концептів "інформаційний рівень даних", "гуманітарна категорія" та "рівень руйнувань" у наборі даних CrisisMMD.

Таблиця 1

Оцінювання ефективності за інформаційним концептом даних у наборі CrisisMMD

Методи	F1	HL	MAP
КЗ + ЛСРВ	0,633	0,227	0,597
ТМЗ + ЛСРВ	0,784	0,151	0,738
ГМЗ + ЛСРВ	0,823	0,114	0,772
ВГМЗ + ЛСРВ	0,849	0,107	0,794
КЗ + БОО	0,675	0,202	0,648
КЗ + БМВЗ	0,683	0,214	0,635
КЗ + ДБН	0,746	0,164	0,719
ВГМЗ + ДБН	**0.872**	**0,041**	**0,835**

Таблиця 2

Оцінювання ефективності за концептом гуманітарної категорії у наборі CrisisMMD

Методи	F1	HL	MAP
КЗ + ЛСРВ	0,537	0,293	0,506
ТМЗ + ЛСРВ	0,691	0,207	0,659
ГМЗ + ЛСРВ	0,687	0,209	0,652
ВГМЗ + ЛСРВ	0,722	0,181	0,695
КЗ + БОО	0,613	0,246	0,581
КЗ + БМВЗ	0,624	0,237	0,598
КЗ + ДБН	0,696	0,194	0,670
ВГМЗ + ДБН	**0,772**	**0,153**	**0,759**

Таблиця 3

Оцінювання ефективності за концептом рівня руйнувань у наборі CrisisMMD

Методи	F1	HL	MAP
КЗ + ЛСРВ	0,644	0,229	0,607
ТМЗ + ЛСРВ	0,791	0,148	0,745
ГМЗ + ЛСРВ	0,829	0,117	0,793
ВГМЗ + ЛСРВ	0,862	0,080	0,839

Методи	F1	HL	MAP
КЗ + БОО	0,693	0,181	0,664
КЗ + БМВЗ	0,688	0,186	0,650
КЗ + ДБН	0,756	0,149	0,715
ВГМЗ + ДБН	**0,923**	**0,029**	**0,897**

Як видно комбінація КЗ + ЛСРВ показує найнижчі результати за всіма метриками. Це не дивно, оскільки проста конкатенація ознак на ранньому етапі часто не здатна відобразити гетерогенний розподіл різних модальностей. Крім того, лінійна сума функцій втрат із рівними вагами в межах багатозадачного навчання має дуже обмежену ефективність або навіть негативний вплив, коли кілька завдань домінують у процесі навчання.

Тензорний метод злиття та графовий метод злиття – обидва демонструють покращення ефективності порівняно з підходом КЗ + ЛСРВ. При цьому ГМЗ має помітну перевагу над ТМЗ, особливо у випадках з більшою кількістю вхідних модальностей. Це частково пояснюється тим, що традиційні методи тензорного злиття на кшталт ТМЗ моделюють спільне представлення лише після виконання операції злиття, тоді як ГМЗ долає цей недолік, навчаючись міжмодальним взаємодіям уже на ранніх етапах.

Запропонований нами вдосконалений графовий метод злиття перевершує всі базові методи й перевищує результат другого найкращого підходу на **4,2 % за метрикою F1** та на **8,5 % за MAP**. Ми вважаємо, що частково це зумовлено застосуванням динамічного показника **B**, який навчається визначати відносну важливість кожної модальності та інтегрує її вже на початковому етапі графової мережі злиття.

Багатозадачне навчання. У таблицях 1–3 також наведено результати роботи методів багатозадачного навчання на наборі даних CrisisMMD. Методи БОО та БМВЗ демонструють кращу ефективність порівняно з підходом багатозадачного навчання із лінійною сумою функцій втрат з рівними вагами. Проте загальне покращення не є суттєвим. Ймовірним поясненням цього є ситуація дисбалансності класів, коли обидва методи зазнають значного зниження ефективності.

Запропонований нами метод вирішує проблему дисбалансу класів завдяки введенню у функцію втрат параметра оберненого співвідношення вибірки для завдань. Це дозволяє моделі посилювати штрафування класів-більшостей, виділяючи більше ресурсів на навчання класів-меншостей. Крім того, ми стверджуємо, що повторне балансування ваг функцій втрат на початку циклу навчання допомагає моделі й надалі зменшувати загальну навчальну втрату, тоді як у двох інших методів цей механізм відсутній.

Для набору даних CrisisMMD запропонований метод перевищує другий найкращий метод на **7,2 % за F1** та на **7,3 % за MAP**.

Загалом, запропонований нами метод з графовою мережею злиття та динамічним багатозадачним навчанням демонструє найкращі результати серед усіх базових методів при роботі з мультимодальним набором даних **CrisisMMD**. Крім того, модульність компонентів методу забезпечує високу гнучкість та простоту їхнього застосування до інших типів даних і структур моделей.

Висновки. У цій роботі запропоновано новий метод графового злиття мультимодальних даних з використанням багатозадачного навчання. Запропонований метод здійснює ієрархічне поєднання кожної модальності з утворенням графової структури, де вершини відповідають об'єднаним модальностям, а ребра містять міжмодальні взаємодії. Відносна важливість між модальностями на одному рівні визначається у вибірково-орієнтованій манері та використовується для формування спільного інтеграційного представлення, яке надалі передається на наступний рівень.

Крім того, ми пропонуємо новий підхід динамічного багатозадачного навчання, що трансформує задачу багатоміткової класифікації у сукупність окремих двійкових задач

класифікації. Завдяки моніторингу складності навчання для кожного завдання компонент динамічного багатозадачного навчання автоматично коригує вагові коефіцієнти функції втрат завдань так, щоб досягався оптимальний баланс. Цей компонент також призначає початковий набір вагових коефіцієнтів для функцій втрат на початку циклу навчання та постійно оновлює їх упродовж процесу аби уникнути потрапляння у локальні мінімуми чи максимуми.

Експериментальні результати на мультимодальному наборі даних продемонстрували суттєву перевагу нашого методу над базовими методами. Більше того, запропонований метод завдяки своїй модульній архітектурі може бути легко застосований до інших типів даних і архітектур мереж.

Таким чином отриманий метод є підґрунтям для подальшої розробки методики обробки мультимодальних даних в інформаційних системах військового призначення, яка дасть можливість підвищити ефективність обробки великих масивів даних та якість прийняття управлінських рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dashenkov D., Smelyakov K. Extending the ImageNET dataset for multimodal text and image learning // INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES. 2025. No. 1 (31)/. P. 20–31. URL: https://doi.org/10.30837/2522-9818.2025.1.020.

2. Олег Басистюк, Наталія Мельникова, Ірина Думин, Андрій Думин. Ансамблевий підхід у мультимодальній обробці даних на основі Google API // Вісник Хмельницького національного університету. Серія: Технічні науки. 2024. № 4 (339). С. 235–238.

3. Yuan Tao, Wanzeng Liu, Jun Chen, Jingxiang Gao, Ran Li, Xinpeng Wang, Ye Zhang, Jiaxin Ren, Shunxi Yin, Xiuli Zhu, Tingting Zhao, Xi Zhai, Yunlu Peng. A graph-based multimodal data fusion framework for identifying urban functional zone // International Journal of Applied Earth Observation and Geoinformation. 2025. Vol. 136. URL: https://doi.org/10.1016/j.jag.2024.104353.

4. Dong J., Hao M., Ding F., Chen S., Wu J., Zhuo J., Jiang D. A Novel Multimodal Data Fusion Framework: Enhancing Prediction and Understanding of Inter-State Cyberattacks // Big Data and Cognitive Computing. 2025. No. 9 (3)/. P. 63. URL: https://doi.org/10.3390/bdcc9030063.

5. T. Baltruˇ saitis, C. Ahuja, L.-P. Morency. Multimodal machine learning: A survey and taxonomy // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2018. Vol. 41, no. 2. Pp. 423–443.

6. Меркотан Д. Ю., Троцько О. О. Методики обробки мультимодальних даних в інформаційних системах з використанням моделей штучного інтелекту // Збірник наукових праць Харківського національного університету Повітряних Сил. 2025. № 2 (84). С. 117–125. URL: https://doi.org/10.30748/zhups.2025.84.14.

7. P. Hu, Y.-A. Huang, K. C. Chan, Z.-H. You. Learning multi modal networks from heterogeneous data for prediction of lncrna–mirna interactions // IEEE/ACM Transactions on Computational Biology and Bioinformatics. 2019. Vol. 17, no. 5. Pp. 1516–1524.

8. C. G. Snoek, M. Worring, A. W. Smeulders. Early versus late fusion in semantic video analysis // in Proceedings of the 13th Annual ACM International Conference on Multimedia. 2005. Pp. 399–402.

9. Y. Zhang, Q. Yang. A survey on multi-task learning // IEEE Transactions on Knowledge and Data Engineering, 2021.

10. Liu Z., Yin Z., Mi Z., Guo B., Zheng Z. A Comparative Analysis of Three Data Fusion Methods and Construction of the Fusion Method Selection Paradigm // Mathematics. 2025. No. 13 (8). P. 1218. URL: https://doi.org/10.3390/math13081218.

11. Songtao L., Hao T. Multimodal Alignment and Fusion: A Survey, arXiv:2411.17040v1 [cs.CV]. 26 Nov 2024.

12. K. Gadzicki, R. Khamsehashari, C. Zetzsche. Early vs Late Fusion in Multimodal Convolutional Neural Networks // 2020 IEEE 23rd International Conference on Information Fusion (FUSION), Rustenburg, South Africa, 2020. Pp. 1–6. DOI: 10.23919/FUSION45008.2020.9190246.

13. Y. Zhang, O. Morel, M. Blanchon, R. Seulin, M. Rastgoo, D. Sidib´e. Exploration of deep learning-based multimodal fusion for semantic road scene segmentation in VISIGRAPP (5: VISAPP). 2019. Pp. 336–343.

14. Qihang Yang, Yang Zhao, Hong Cheng. MMLF: Multi-modal Multi-class Late Fusion for Object Detection with Uncertainty Estimation // arXiv:2410.08739v1. URL: https://doi.org/10.48550/arXiv.2410.08739.

15. Clemens Witt, Thiemo Leonhardt, Nadine Bergner, Mareen Grillenberger. Multimodal Late Fusion Model for Problem-Solving Strategy Classification in a Machine Learning Game // arXiv:2507.22426v1 [cs.LG]. 30 Jul 2025.

16. Y. Cheng, R. Cai, Z. Li, X. Zhao, K. Huang. Locality-sensitive deconvolution networks with gated fusion for rgb-d indoor semantic segmentation // in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2017., Pp. 3029–3037.

17. J. Jiang, L. Zheng, F. Luo, Z. Zhang. Rednet: Residual encoder decoder network for indoor RGB-D semantic segmentation // CoRR. 2018. Vol. abs/1806.01054.

18. A. Valada, R. Mohan, W. Burgard. Self-supervised model adap tation for multimodal semantic segmentation // International Journal of Computer Vision. 2019. Pp. 1–47.

19. H. Ben-Younes, R. Cadene, M. Cord, N. Thome. Mutan: Multimodal tucker fusion for visual question answering // in Proceedings of the IEEE International Conference on Computer Vision. 2017. Pp. 2612–2620.

20. A. Zadeh, M. Chen, S. Poria, E. Cambria, L. Morency. Tensor fusion network for multimodal sentiment analysis // in Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP). Association for Computational Linguistics. 2017. Pp. 1103–1114.

21. Desai A., Mahto R. Multi-Class Classification of Breast Cancer Subtypes Using ResNet Architectures on Histopathological Images // Journal of Imaging. 2025. No. 11 (8). P. 284. URL: https://doi.org/10.3390/jimaging11080284.

22. T. Zhao, Y. Xu, M. Monfort, W. Choi, C. Baker, Y. Zhao, Y. Wang, Y. N. Wu. Multi-agent tensor fusion for contextual trajectory prediction // in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019. Pp. 12126–12134.

23. A. B. Zadeh, P. P. Liang, S. Poria, E. Cambria, L.-P. Morency. Multimodal language analysis in the wild: Cmu-mosei dataset and interpretable dynamic fusion graph // in Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). 2018. Pp. 2236–2246.

24. M. Angelou, V. Solachidis, N. Vretos, P. Daras. Graph-based multimodal fusion with metric learning for multimodal classification // Pattern Recognition. 2019. Vol. 95. Pp. 296–307.

25. J. Chen, A. Zhang. Hgmf: Heterogeneous graph-based fusion for multimodal data with incompleteness // in Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2020. Pp. 1295–1305.

26. O. Sener, V. Koltun. Multi-task learning as multi-objective optimization // in Annual Conference on Neural Information Processing Systems. 2018. Pp. 525–536.

27. R. Hu, A. Singh. Unit: Multimodal multitask learning with a unified transformer // arXiv preprint arXiv:2102.10772. 2021.

28. S. Mai, H. Hu, S. Xing. Modality to modality translation: An adversarial representation learning and graph fusion network for multimodal fusion // in Proceedings of the AAAI Conference on Artificial Intelligence. 2020. Vol. 34, no. 01. Pp. 164–172.

29. F. Alam, F. Ofli, M. Imran. Crisismmd: Multimodal twitter datasets from natural disasters // in Proceedings of the International AAAI Conference on Web and Social Media. 2018. Vol. 12, no. 1.

30. C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, Z. Wojna. Rethinking the inception architecture for computer vision // in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2016. Pp. 2818–2826.

31. J. Deng, W. Dong, R. Socher, L. Li, K. Li, F. Li. Imagenet: A large-scale hierarchical image database // in IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR). IEEE Computer Society. 2009. Pp. 248–255.

32. M. E. Peters, M. Neumann, M. Iyyer, M. Gardner, C. Clark, K. Lee, L. Zettlemoyer. Deep contextualized word representations // in Proceedings of the Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, (NAACL-HLT). Association for Computational Linguistics. 2018. Pp. 2227–2237.

33. T. Mikolov, K. Chen, G. Corrado, J. Dean. Efficient estimation of word representations in vector space // in 1st International Conference on Learning Representations (ICLR), Y. Bengio and Y. LeCun, Eds., 2013.

34. J. Pennington, R. Socher, C. D. Manning. Glove: Global vectors for word representation // in Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP). ACL, 2014. Pp. 1532–1543.

36. D. P. Kingma, J. Ba. Adam: A method for stochastic optimization // in 3rd International Conference on Learning Representations (ICLR), 2015.

37. S. Vandenhende, S. Georgoulis, L. Van Gool. Mti-net: Multi-Scale task interaction networks for multi-task learning // in European Conference on Computer Vision. Springer. 2020. Pp. 527–543.

DOI: 10.58254/viti.8.2025.12.145

УДК 629.35:62-50:004.94

д-р філософії Романенко М. М. ORCID: 0000-0002-0646-2797 (ВІТІ ім. Героїв Крут)
д-р філософії Погребняк С. В. ORCID: 0000-0002-7902-9847 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ПІДВІСКИ РОБОТИЗОВАНОГО КОМПЛЕКСУ

Тенденції еволюції технологій в сфері роботизованих систем та штучного інтелекту окреслили перспективи та напрямки багатьох аспектів глобального розвитку людства в осяжному майбутньому. Не виключенням стало застосування роботизованих комплексів і у військовій справі. Реалії російсько-української війни показали широкий спектр можливостей застосування роботизованих комплексів. У відповідь на значну перевагу сил російської окупаційної армії в особовому складі, артилерійських системах, бронетехніці та авіації сили оборони України ефективно застосовують роботизовані комплекси різних форм, моделей та специфікацій.

Одним із варіантів застосування роботизованих комплексів, які останнім часом все активніше використовуються на фронті, є наземні роботизовані комплекси в якості багатофункціональних (бойових) платформ на колісній або гусеничній базі. Такі платформи здатні виконувати різноманітні завдання та задачі.

Виходячи з такого широкого спектру завдань які здатні виконувати наземні роботизовані комплекси, можна стверджувати, що в осяжному майбутньому вони зможуть значною мірою замінити людину на полі бою, що дасть змогу зберегти життя та здоров'я військовослужбовця. Проте ефективність їх використання залежить від ряду факторів: зв'язок і навігація, прохідність транспортної платформи, характеристики бойового (спеціалізованого) модуля. Проблематиці, вдосконаленню, оптимізації та моделюванню функціонування саме підвіски транспортної бази і присвячена ця стаття.

Розглянуті варіанти різноманітних діянь на транспортну базу. Визначені основні характеристики, що впливають на підресорну частину транспортної бази. Проведено моделювання зовнішнього впливу профілю дорожнього полотна на підресорну частину транспортної бази. Отримані числові показники збурних діянь та відклик основних елементів підвіски транспортної бази. Запропоновано способи використання результатів роботи в якості керуючого впливу системи автоматичної стабілізації для покращення керованості та прохідності НРК.

Ключові слова: *транспортна база, платформа, роботизований комплекс, підвіска, профіль поверхні, демпфер, система стабілізації, математична модель.*

M. Romanenko, S. Pohrebniak. Suspension model of the robotic complex

Trends in the evolution of technologies in the field of robotic systems and artificial intelligence have outlined the prospects and directions of many aspects of the global development of humanity in the foreseeable future. The use of robotic complexes in military affairs was no exception. The realities of the Russian-Ukrainian war showed a wide range of possibilities for the use of robotic complexes. In response to the significant superiority of the Russian occupation army in personnel, artillery systems, armored vehicles and aviation, the Ukrainian defense forces effectively use robotic complexes of various forms, models and specifications.

One of the options for using robotic complexes, which have recently been increasingly used on the front, is ground robotic complexes as multifunctional (combat) platforms on a wheeled or tracked base. Such platforms are capable of performing a variety of tasks and missions.

Based on such a wide range of tasks that ground robotic complexes are capable of performing, it can be argued that in the foreseeable future they will be able to largely replace humans on the battlefield, which will allow preserving the life and health of a serviceman. However, the effectiveness of their use depends on a number of factors: communication and navigation, the cross-country ability of the transport platform, the characteristics of the combat (specialized) module. This article is devoted to the problems, improvement, optimization and modeling of the functioning of the suspension of the transport base.

Variants of bison actions on the transport base are considered. The main characteristics that affect the under-spring part of the transport base are determined. The modeling of the external influence of the roadbed profile on the under-spring part of the transport base is carried out. Numerical indicators of turbulent actions and the response of the main elements of the transport base suspension are obtained. Methods of using the results of the work as a control effect of the automatic stabilization system to improve the controllability and patency of the NRC are proposed.

Keywords: *transport base, platform, robotic complex, suspension, surface profile, damper, stabilization system, mathematical model.*

Постановка завдання у загальному вигляді

Наземні роботизовані комплекси (НРК) являють собою рухому платформу на колісному або гусеничному шасі. До складу такої системи входять: пристрій відеоспостереження, блок

керування та система зв’язку і навігації. Залежно від завдань, що вирішуються, на платформу може бути встановлено додаткове обладнання:

роботизований маніпулятор (для мінування/розмінування);

модуль для транспортування (для завдань логістики);

ноші або захищений короб (для транспортування поранених);

системи та пристрої спостереження (для завдань розвідки);

вогневі засоби ураження (для виконання завдань ураження противника).

В будь-якому випадку, основою для РНК є уніфікована транспортна платформа.

Враховуючи стрімкий розвиток роботизованих технологій та мультизадачність РНК, постає питання вибору транспортної бази, яка б задовольняла визначеним задачам.

Аналіз останніх публікацій

З метою порівняння тактико-технічних характеристик здійснено аналіз публікацій останніх років, що стосуються існуючих роботизованих наземних комплексів. Він не дає однозначної відповіді на питання яка транспортна база є кращою чи оптимальнішою [1–3].

Технологічно розвинені країни такі як США, Великобританія, Франція, Ізраїль, Китай, Японія та ряд інших займаються розробкою випробуваннями та практичним застосуванням роботів на державному рівні [4]. Здійснюються дослідження в напрямку покращення прохідності та керованості НРК. Це реалізується двома головними способами: покращенням існуючих платформ та розробкою нових (інколи нетипових або інноваційних) транспортних платформ.

Оцінка ефективності застосування різних типів транспортної бази дуже різниться. Залежно від висунутих вимог та практичних рішень, кожен вид має ряд своїх переваг та недоліків [5].

Вивчені літературні джерела [6–8] приводять приклади конструктивних рішень побудови транспортної бази наземних роботизованих комплексів. До прикладу, представлені різновиди схем підресорних частин та електродвигунів. Розглянуті переваги використання голчатих підшипників, практичні варіанти використання амортизаторів, торсіонів та поперечних важелів. Запропоновані оригінальні конструктивні рішення з’єднань електроприводів, редукторів та шарнірів. В багатьох випадках пропонується застосування, планетарних, хвильових та циклоїдальних редукторів та високооборотних малогабаритних сервоприводів. Наведені схемотехнічні рішення не відрізняються від традиційних деталей автомобілів та іншої техніки. Разом з тим присутні інноваційні рішення щодо використання оригінальних запчастин та нетипового використання відомих технологічних рішень, застосування наноматеріалів та новітніх сполук металів чи полімерів в якості основ для виробництва. Зазвичай такі дані (інноваційні рішення чи матеріали виготовлення конструкцій) є частковими та потребують додаткового вивчення.

В роботах [9; 10] наведено класифікацію та узагальнені вимоги до РНК, проведена коротка оцінка ефективності застосування наземних роботизованих комплексів вітчизняного виробництва у збройних конфліктах, їхньої ролі на полі бою та проаналізовано розвиток наземних роботизованих комплексів.

Аналіз основних характеристик, відомих НРК, різник класів виявив недоліки конструкцій та невідповідність цих характеристик вимогам, що висуваються до них у сучасних умовах. Це підтверджує актуальність досліджень щодо моделювань впливу навколишніх умов на шасі наземних роботизованих комплексів, раціонального вибору типу транспортної платформи та розробки перспективних зразків наземних роботизованих комплексів.

Мета статті полягає в розробці математичної моделі взаємодії підвіски транспортної бази та зовнішнього чинника – профілю поверхні дорожнього полотна. Отримана модель надасть змогу розраховувати чисельні значення впливу та оцінити ефективність підвіски транспортної бази РНК.

Виклад основного матеріалу. Оцінка функціональної ефективності типів транспортної бази ґрунтується на порівнянні переваг та недоліків двох найрозповсюдженіших типів: колісного та гусеничного шасі.

Перевагами гусеничного виду є вища прохідність (в порівнянні з колісним шасі) та можливість встановлення диференціальних механізмів синхронної зміни величини кліренсу і геометрії гусеничних обводів, що включає в себе, як правило, два бортових синхронізатора, які встановлені вздовж бортів корпусу гусеничного шасі всередині гусеничних обводів.

Недоліком є низька надійність та складність обслуговування.

Перевагами колісної платформи є більша надійність (в порівнянні з гусеничним шасі) та висока ремонтопридатність. Недолік недостатня прохідність.

Однак обидва типи підвіски зазнають впливу при русі по поверхнях різного виду. Характерними умовами є різноманітні типи доріг, пересічена місцевість, пересування у приміщеннях та подолання перешкод. Значна відмінність поверхонь по яких відбувається пересування ускладнює дослідження їх впливу на транспорту базу. Таким чином актуальним є застосування методів математичного моделювання для дослідження впливу дорожніх умов на характеристики транспортної платформи.

З метою розрахунку впливу різних умов на ефективність НРК використовують експериментальні та розрахункові методи [11]. Найбільш ефективним та раціональним методом дослідження впливу таких умов на особливості функціонування наземних роботизованих комплексів є математичне моделювання. Воно дозволяє проводити розрахунки з урахуванням жорстких умов навколишнього середовища, дорожніх умов та факторів зовнішнього впливу на підвіску таких як вплив вогневого засобу встановленого на РНК. Здатність наземних роботизованих комплексів рухатись різними типами поверхні характеризується їх прохідністю [12].

Основні параметри профільної прохідності визначаються з компонувальної схеми транспортної платформи та безпосередніми вимірюваннями наступних характеристик:

дорожній просвіт (кліренс) – (h);

передній та задній звиси – (l_1, l_2);

кути переднього та заднього звисів – (γ_1, γ_2);

повздовжній та поперечний радіуси прохідності – (R_1, R_2);

найбільший кут підйому – (α).

Отже врахування саме цих характеристик необхідне для розрахунку та моделювання впливу на підвіску транспортної бази. Також конструктивні особливості будови транспортної бази визначають характеристики контакту опорних частин шасі з нерівностями дороги, а отже і теоретичну модель впливу дорожнього полотна на транспортний засіб. На рисунку 1 представлена узагальнена класифікація нерівносетй поверхні за основними характеристиками.

За характером нерівностей поверхні умовно розподіляються на дві групи: квазістаціонарні умови, за своїм характером наближені до прямолінійного профілю з незначними плавними в часі змінами висоти профілю поверхні; умови пересічної місцевості із стрімко змінними ступінчатими або різко нахиленими змінами параметрів (пересування НРК через завали, воронки, окопи чи траншеї, апарелі та ескарпи, виступи та круті схили таке інше). Пересування такими дорожніми умовами обумовлюється особливістю: наявністю періодичного або постійного контакту ходової частини транспортної бази із поверхнею дорожнього полотна.

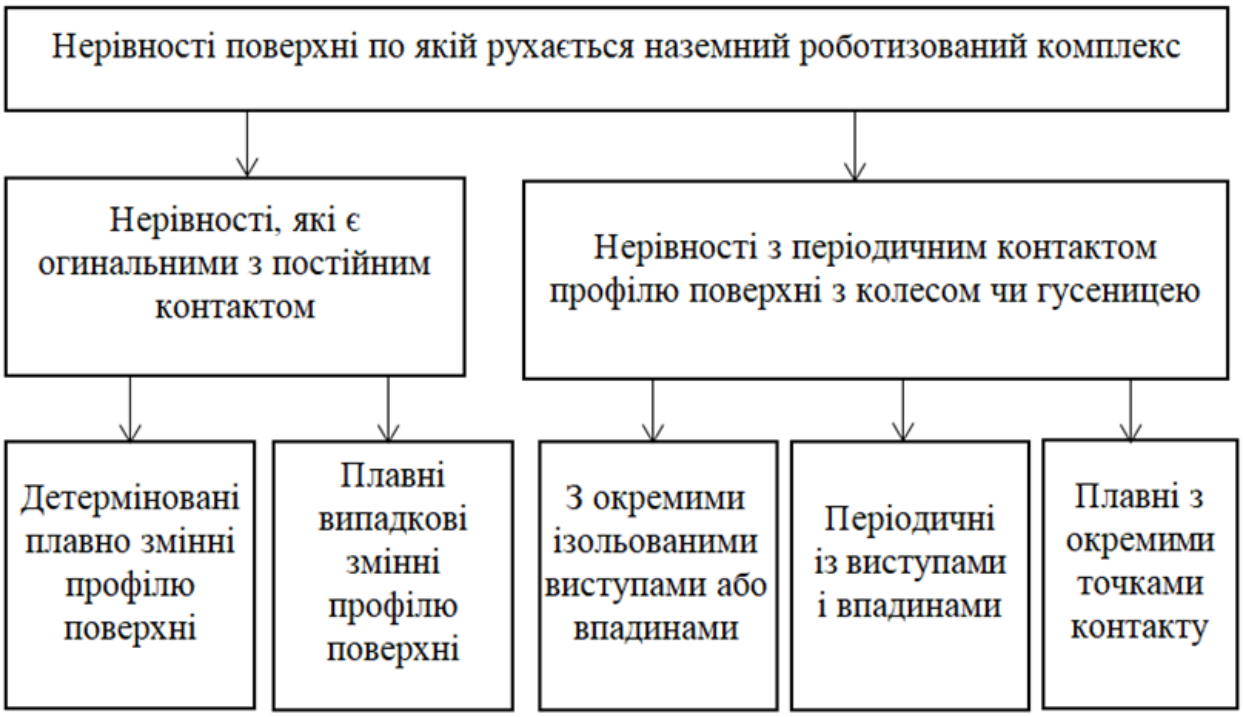


Рис. 1. Класифікація характеристики профіля поверхні за фактом наявності неперервного чи точкового контакту з колесом чи гусеницею

Точковий контакт відображає відгук взаємодії полотна поверхні по якій рухається НРК та квазіциліндричній поверхні колеса, або гусениці. Функція зміни профілю дороги від часу $Z_{(x)}(t)$ за довжиною ординати, має характерний опис зміни місця перебування квазіциліндричної поверхні підресорної частини транспортної бази у вертикальній площині та її значення екстремумам відповідає кліренсу h. Тоді h=h(Z). Ця залежність незначно змінюється за рахунок пружної деформації квазіциліндричної поверхні та торсіонно-амортизаційного вузла транспортної бази у відповідності до опорної реакції b_k. Враховуючи вищевикладене, доходимо висновку, що профіль полотна дороги однозначно і всебічно відображає характер взаємодії транспортної бази і місцевості, якою він пересувається.

Більшість існуючих та перспективних НРК відносяться до середнього класу. Вони мають незначні масогабаритні розміри (по відношенню до можливих перешкод). Такі НРК, як правило, використовуються на відкритій місцевості, що зменшує ймовірність наявності різких ступінчатих перешкод які б мали співвідношення висоти “сходинки” до кліренсу 1:1.

На рисунку 2 зображено розрахунок плавних змінних в часі (по осі ординат) профілів поверхні з квазіперіодичним точковим контактом, відносно шасі, вбачається основним напрямком для розрахунку математичної моделі.

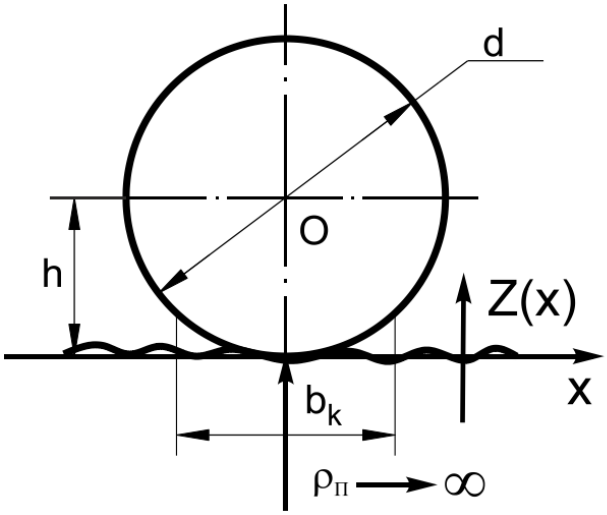


Рис. 2. Схема відгуку положення колеса залежно від характеру контакту з дорожнім покриттям

Плавні зміни профілю окремої колії можуть бути описані як у вигляді детермінованих функцій, так і у формі випадкових процесів. Тому при моделюванні впливу дорожніх умов першої групи використовуються як детерміновані, так і стохастичні моделі профілю колії. У разі детермінованого підходу геометрія колії подається у вигляді часткового ряду Фур’є [13]:

$$Z(x) = \frac{a_0}{2} + \sum_{k=1}^{\infty} a_k \cos(k\omega_0 x) + b_k \sin(k\omega_0 x),$$

де Z – наявна висота поверхні дороги в зазначеній точці з координатою x;

a_0, a_k, b_k – коефіцієнти ряду Фур’є;

ω_0 – параметр, періоду зміни висоти полотна поверхні.

Коефіцієнти, які визначають співвідношення із профілем дороги $Z(x)$:

$$a_k = \frac{2}{T}\int_0^T z(\tau)\cos(k\omega_0\tau)d\tau, \qquad b_k = \frac{2}{T}\int_0^T z(\tau)\sin(k\omega_0\tau)\,d\tau.$$

Математичний опис профілю поверхні по якої відбувається рух здійснено полігармонічною функцією:

$$z(x) = \sum_{k=0}^{\infty} A_k \sin(k\omega_0 x + \psi_{0k}), \qquad (1)$$

де A_k – амплітуда складових гармонік профіля поверхні;

ψ_{0k} – початкова фаза складових гармонік профіля поверхні.

Визначення цих коефіцієнтів здійснюється через коефіцієнти ряду Фур’є [13]:

$$A_k = \sqrt{a_k^2 + b_k^2}, \quad \psi_{0k} = \operatorname{arctg}\frac{b_k}{a_k}.$$

Застосування математичної залежності (1) дозволяє представити форму профілю поверхні у вигляді певного набору періодичних функцій. Одночасно з цим дає можливість

врахувати параметри, які визначають її основні характеристики (особливості) та описати параметри схожих поверхонь для побудови моделі відклику підресорної частини транспортних засобів, що будуть рухатись по ній.

Однак, при використанні рядів Фур'є для розрахунку детермінованих профілів поверхні, можуть траплятися випадки розрахунку нескінченних рядів (викликано некоректною постановкою задачі). Для вирішення таких задач за розрахунком детермінованих та (або) квазіперіодичних профілів поверхні пропонується введення коректуючого форм-фактора.

Слід також зауважити, що при фронтальному контакті колеса транспортної бази НРК з перешкодою, яка перевищує радіус колеса, виникає збурне діяння на всю підресорну частину. Величина миттєвого значення цього збурного діяння залежатиме від швидкості руху та вектора:

$$Z(x) = h[1(x) - z(x - x_1)], \tag{2}$$

де h – висота перешкоди;

x_1 – протяжність (довжина) перешкоди.

Таким чином, вирішення поставленого в роботі завдання зводиться до комплексного врахування множин варіантів збурних діянь (1) та (2) на підвіску НРК.

Для розрахунку опорного зміщення профілю дороги застосуємо вираз [14]:

$$yr(t) = A * \sin(2\pi\lambda\upsilon t + \varphi) * \exp(-\alpha\, r\, \lambda), \tag{3}$$

де *A* – амплітуда коливань;

υ – швидкість;

t – час;

r – відстань;

α – коефіцієнт загасання.

Синусоїдальна функція представляє собою збурне діяння, від профілю дороги, а експоненціальна складова додає затухання або згасання під час пересування вздовж нього.

Для опису системи на яку впливають сили інерції $m \cdot \ddot{y}(t)$, сили демпфування $(\dot{y}(t) - \dot{y} \cdot r(t)$ та сили пружності $k \cdot \big(y(t) - y \cdot r(t)\big)$ застосуємо вираз (4).

Сили демпфування та пружини діють так, щоб привести переміщення системи *y(t)* до еталонного переміщення $\dot{y} \cdot r(t)$:

$$m \cdot y''(t) + c \cdot (y'(t) - y' \cdot r(t) + k \cdot \big(y(t) - y \cdot r(t)\big) = 0, \tag{4}$$

де m – маса;

$y''(t)$ – друга похідна *y(t)* відносно часу (прискорення);

c – коефіцієнт демпфування;

$y'(t)$ – перша похідна y(t) відносно часу (швидкості);

$y \cdot 'r(t)$ – перша похідна $y \cdot r(t)$ відносно часу (швидкості опорного переміщення);

k – коефіцієнт жорсткості;

$y(t)$ – переміщення системи.

З метою вирішення цих завдань запропоновано використання програмного забезпечення "Mathematica". Перевірку та підтвердження адекватності отриманих результатів здійснено засобами вебплатформи "Github".

Фрагмент програмного коду математичного моделювання наведено нижче:

```
\begin{cases}
y_r(t) = A \cdot \sin(2\pi \lambda v t + \phi) \cdot \exp(-\alpha r \lambda) \\
m \cdot \ddot{y}(t) + c \cdot \left( \dot{y}(t) - \dot{y}_r(t) \right) + k \cdot \left( y(t) - y_r(t) \right)=0
\end{cases}
```

Графічне відображення перекосу транспортної бази НРК, під час руху по двох коліях з різним профілем на та результуючими силами, що діють на НРК зображено на рисунку 3.

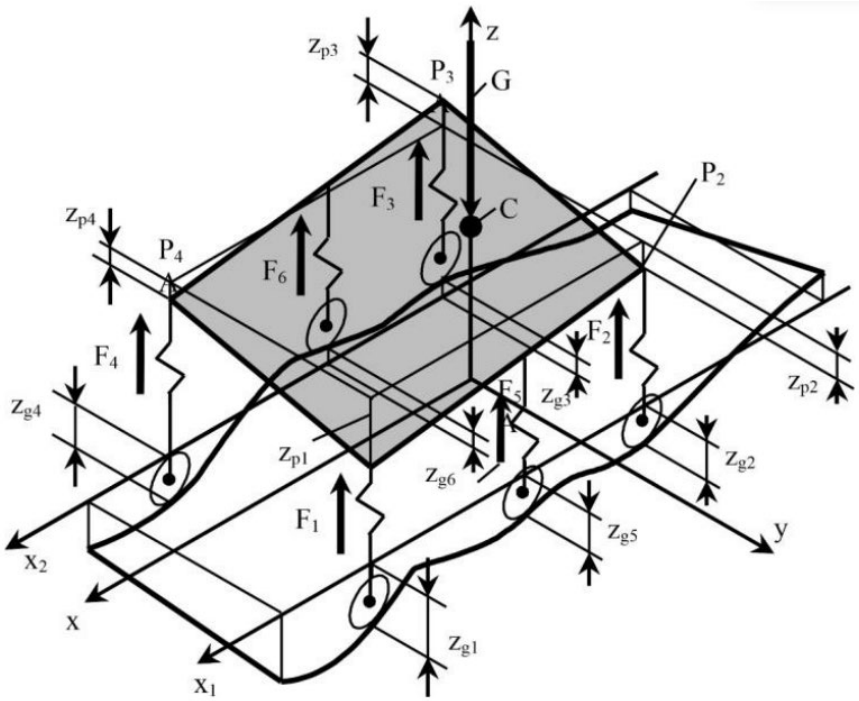


Рис. 3 Перекіс транспортної бази НРК при русі по пересічній місцевості

На рисунку 3 позначено:
Z_{g1}….. Z_{g6} – результуючі сили які впливають на підресорну частину платформи НРК;
Z_{p1}….. Z_{p6} – результуючі відхилення (крен, тангаж) платформи;
X_1, X_2, – прямолінійний напрям руху платформи;
C – результуюча сила демпфірування;
F_1 …. F_6 – результуючі сили, які діють безпосередньо на платформу НРК.

Висновки і перспективи подальших досліджень

В роботі наведено математична модель розрахунку впливу профілю поверхні дорожнього покриття на підресорну частину НРК. Розрахунок дає можливість не лише оцінити (визначити чисельні значення) зовнішнього впливу, але й використовувати ці результати як керуючий вплив системи автоматичної стабілізації.

Подальшим розвитком роботи можливо вважати покращення керованості та прохідності НРК. Все це дає змогу підвищити бойову ефективність НРК. Водночас, наведені результати можуть братись до уваги при проєктуванні, розробці та виготовленні нових роботизованих платформ, або нетипових транспортних засобів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Anis Koubaa. Robot Opereting System. Berlin: Springer, 2019. P. 16.

2. Коваль В., Семененко О., Баранов С., Островський С., Акініна Т., Сеченев О. Роль і місце роботизованих систем у сучасних війнах і збройних конфліктах: теоретичний аспект // Journal of Scientific Papers «Social Development and Security». 2023. Vol. 13. № 5.

3. Кириченко І. В. Наземні роботизовані комплекси: основи та майбутнє // Молодий вчений. 2021. № 12 (100).

4. Ісакова Т. О. Проблеми формування стратегічних пріоритетів державної політики щодо розвитку робототехніки: перспективи для України / Т. О. Ісакова // Офіційний сайт Нац. Ін-ту стратегічних досліджень від 13.09.2019. URL: https://niss.gov.ua/doslidzhennya/informaciynistrategii/problemi-formuvannya-strategichnikh-prioritetiv-derzhavnoi.

5. Кучеров Д. П. Перспективи розвитку роботизованих систем військового призначення / Д. П. Кучеров, З. М. Копилова, Ю. В. М'якухін // Системи озброєння і військова техніка. 2007. Вип. 1 (9). С. 44–46.

6. Чепков І. Б., Григор'єв О. П., Беліков В. Т., Ковалішин С. С. Класифікація бойових наземних робототехнічних комплексів – дієвий шлях до з'ясування цієї категорії озброєння // Наука і оборона. 2017. № 3/4.

7. Сердюк О. Залізні воїни майбутнього. Тренди ринку бойових роботів / Олексій Сердюк // URL: https://zbroya.info/uk/blog/11902_zalizni-voyini-maibutnogo-trendirinku-boiovikh-robotiv//.

8. Семененко О., Баранов С., Акініна Т., Добровольський Ю., Ярмольчик М., Мусієнко В. Концептуальні погляди щодо розвитку та застосування роботизованих систем в ЗС України (концепція, завдання, класифікація, система управління, виклики щодо застосування, перспективи) // Journal of Scientific Papers «Social Development and Security». 2023. Vol. 13. № 3.

9. Прохорський С. І., Андрущенко В. М., Бондаренко О. Є., Сергієнко А. В., Бригадир С. П., Гетьман А. В. Вплив наземних роботизованих комплексів вітчизняного виробництва на перебіг подій у збройних конфліктах та їх розвиток // Вісник Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Комунікаційні та інформаційні системи. Випуск 1 (5). Київ: ВІТІ, 2024. 104 с.

10. Слюсар В. І. Мінімальні вимоги до спроможностей як складова концепції розвитку наземних роботизованих комплексів / В. І. Слюсар // Науково-практична конференція «Актуальні проблеми застосування Збройних Сил України, управління ними, їх оперативного та матеріально технічного забезпечення». 17–18 вересня 2019 р. ЦНДІ ЗСУ. URL: https://slyusar.kiev.ua/CNDI_2019_1.pdf.

11. Strutinsky V. B. Determination of development grounds and characteristics of mobile multi-coordinate robotic machines for materials machining in field conditions / V. B. Strutinsky, A. A. Hurzhii, O. V. Kolot, V. E. Polunichev // Науковий вісник Національного гірничого університету. Науково-технічний журнал. 2016. № 5 (155). С.43–51.

12. Аржаєв Г. О. Визначення складової сили тяги рушія, що обумовлена зовнішнім тертям виступів рисунка протектора пневматичної шини / Г. О. Аржаєв, Л. Є. Пелевін, М. М. Балака // Вісник Кременчуцького державного політехнічного університету ім. М. Остроградського. 2008. Вип. 5 (52). Ч. 2. С. 75–79.

13. Мэнли Р. Анализ и обработка записей колебаний / Р. Мэнли. М.: Машиностроение, 1972. 368 с.

14. Чихладзе Е. Д. Динамічні розрахунки конструкцій: підручник / Е. Д. Чихладзе, С. Ю. Берестянська, І. М. Лисяков. Харків: УкрДУЗТ, 2015. 161 с.

DOI: 10.58254/viti.8.2025.13.153

УДК 621.396.662

д-р техн. наук Самохвалов Ю. Я. ORCID: 0000-0001-5123-1288 (ВІТІ ім. Героїв Крут)
канд. техн. наук Бовда Е. М. ORCID: 0000-0002-8267-2120 (ВІТІ ім. Героїв Крут)
Клименко В. М. ORCID: 0000-0001-7834-7213 (ВІТІ ім. Героїв Крут)
Устинов Д. А. ORCID: 0009-0004-3993-1096 (ВІТІ ім. Героїв Крут)

УПРАВЛІННЯ БАЛАНСУВАННЯМ НАВАНТАЖЕННЯ В ГІБРИДНИХ SDN-МЕРЕЖАХ НА ОСНОВІ АЛГОРИТМУ ІТЕРАЦІЙНОГО РОЗСЛАБЛЕННЯ З МАСШТАБУВАННЯМ І ОКРУГЛЕННЯМ

У статті розглянуто задачу оптимального перерозподілу трафіку в гібридних SDN-мережах, де поєднуються традиційні технології маршрутизації (OSPF) та програмно-керовані мережі (SDN). Показано, що класичні методи балансування навантаження (DNS-Round Robin, ECMP, ADC тощо) не забезпечують необхідної гнучкості у складних телекомунікаційних середовищах. Проаналізовано сучасні підходи, зокрема використання нейронних мереж, навчання з підкріпленням, багатошляхове та енергоефективне балансування. Встановлено, що для гібридних мереж актуальним є врахування як QoS, так і обмежень апаратних ресурсів комутаторів (TCAM).

Формалізовано задачу багатопродуктового обмеженого поділу потоку (MCFS) у вигляді задачі оптимізації з урахуванням пропускної здатності каналів, кількості шляхів та обмежень пам'яті комутаторів. Доведено, що точне розв'язання задачі є NP-складним, тому запропоновано наближений метаевристичний метод – ітераційне розслаблення з масштабуванням та округленням (Iterative Relaxation with Scaling and Rounding, IRSR). Алгоритм поєднує розв'язання лінійного розслаблення, масштабування пропускної здатності та поетапне округлення з повторною оптимізацією.

Отримані результати підтверджують ефективність IRSR у зменшенні максимального навантаження на лінії зв'язку та підвищенні ефективності використання мережевих ресурсів. Запропонований підхід дозволяє автоматизувати процеси управління трафіком, запобігати перевантаженням та формувати адаптивну політику маршрутизації. Подальші дослідження спрямовані на інтеграцію інтелектуальних методів прогнозування для підвищення рівня автоматизації та продуктивності гібридних SDN-мереж.

Ключові слова: *гібридна SDN-мережа, оптимальний перерозподіл трафіку, балансування навантаження, багатопродуктовий потік, метаевристичні методи, IRSR-алгоритм, QoS, обмеження TCAM.*

Y. Samokhvalov, E. Bovda, V. Klimenko, D. Ustinov. Load balancing management in hybrid SDN networks based on iterative relaxation algorithm with scalation and rounding

The paper addresses the problem of optimal traffic redistribution in hybrid SDN networks that combine traditional routing technologies (OSPF) with Software-Defined Networking (SDN). It is shown that classical load balancing methods (DNS-Round Robin, ECMP, ADC, etc.) lack the required flexibility in complex telecommunication environments. A survey of recent approaches highlights the use of neural networks, reinforcement learning, multipath and energy-efficient balancing. For hybrid networks, special attention is given to both Quality of Service (QoS) requirements and hardware constraints of switches (TCAM).

The problem is formalized as a Multicommodity Constrained Flow Splitting (MCFS) optimization task considering link capacities, path limitations, and memory constraints of network devices. Since the exact solution is NP-hard, an approximate metaheuristic method – Iterative Relaxation with Scaling and Rounding (IRSR) – is proposed. The algorithm combines solving a relaxed linear program, scaling of link capacities, and iterative rounding with resource reallocation.

The obtained results demonstrate that IRSR effectively reduces maximum link utilization and improves bandwidth resource efficiency. The proposed approach enables automated traffic management, prevents network overloads, and supports adaptive routing policies. Future research will focus on integrating intelligent forecasting and decision-making techniques to enhance automation and performance in hybrid SDN environments.

Keywords: *hybrid SDN network, optimal traffic redistribution, load balancing, multicommodity flow, metaheuristic methods, IRSR algorithm, QoS, TCAM constraints.*

Вступ. Мережева інфраструктура центрів обробки даних (ЦОД) працює в умовах підвищеного навантаження та неоднорідності трафіку. Існує кілька методів керування навантаженням [1–6]: *DNS*-Round Robin, Link Aggregation, *ECM*P, *ADC*, *SDN* мережі. Серед цих методів використання *SDN* мереж дозволяє більш ефективно управляти трафіком (*traffic engineering*) в розподілених телекомунікаційних середовищах. В *SDN*-мережі управління

трафіком здійснює контролер, який регулює пропускну здатність мережі та реалізує вибрану політику балансування навантаження на основі заданих правил, а також спеціалізованих додатків. Балансування навантаження в *SDN*-мережах застосовується в дата-центрах, мережах операторів, *IoT* (Інтернет речей), бездротових мережах.

До основних політик балансування навантаження в *SDN* відносяться:

алгоритми балансування навантаження [7–13];

застосування нейронних мереж для прогнозування навантаження, виявлення аномалій і прийняття рішень щодо перебалансування трафіку в режимі реального часу [14–16];

архітектурні підходи (централізоване балансування, розподілене балансування, ієрархічне балансування) [17–20].

В межах політик балансування навантаження в *SDN* мережах на сьогодні виділяються декілька напрямів наукових досліджень по перерозподілу навантаження: використання штучних нейронних мереж (далі – ШНМ) або навчання з підкріпленням для динамічного балансування навантаження; балансування навантаження з урахуванням *QoS* (Quality of Service); балансування невеликої кількості дуже великих потоків («слонів»), які займають більшу частину пропускної здатності і величезної кількості дрібних потоків («ми шей»); балансування багатошляхового навантаження; енергоефективне балансування навантаження; балансування навантаження в мультиконтролерних середовищах *SDN*-мереж. Нижче проведено аналіз відомих робіт по балансуванню навантаження.

Аналіз останніх досліджень і публікацій. Робота [21] присвячена механізму роботи *OpenFlow*, який дозволяє реалізувати балансування навантаження. В роботі [22] дається інформація про різні методи детекції та управління слонівними потоками, які є основою для їх балансування. В роботі [23] розглянуто приклад розподілу навантаження на контролери *SDN*. В роботі [24] показано використання глибокого навчання з підкріпленням для завдань трафік-інженерінга, що включає балансування навантаження. В роботі [25] розглянуто приклад реалізації багатошляхового балансування. В роботі [26] розглянуто приклад, який поєднує енергоефективність з машинним навчанням. В роботі [27] пропонується використовувати поглиблене навчання для побудови адаптивної системи балансування навантаження в *SDN*. Розглядається, як глибокі нейронні мережі можуть аналізувати складні стани мережі та динамічно приймати рішення щодо маршрутизації трафіку для оптимізації продуктивності. Такі підходи дозволяють системі самостійно навчатися та адаптуватися до мінливих моделей трафіку без явного програмування правил. В роботі [28] пропонується механізм балансування навантаження для самих контролерів *SDN*, який враховує їх «довіру» та «репутацію», що є критично важливим у розподілених середовищах з декількома контролерами. Це дозволяє не тільки розподілити навантаження, але і забезпечити надійність і захист від потенційно скомпрометованих хостів. В роботі [29] розглянуто методи, які спрямовані на досягнення низької затримки та високої пропускної здатності, і що вони є основними цілями балансування навантаження. Обговорюються різні підходи та алгоритми, які *SDN* надає для оптимізації продуктивності мережі, включаючи конкретні методи для зменшення затримки, що особливо актуально для додатків, чутливих до часу. В роботі [30] досліджується гібридний підхід до балансування навантаження в мережах *SDN* з кількома контролерами. Де «гібридний» означає комбінацію традиційних технологій маршрутизації та технології *SDN*. У великих, складних мережах, де повна централізація може бути неефективною, гібридні моделі відіграють ключову роль у забезпеченні більшого балансування навантаження та підвищеної масштабованості.

На основі проведеного аналізу маємо зробити висновок, що переважна більшість вище наведених авторів проводили свої дослідження за різної конфігурації мереж, для окремих видів мереж. Разом з тим, в неповній мірі враховуються завдання перерозподілу навантаження в мережі у випадку одночасного використання традиційних технологій маршрутизації в поєднанні з технологіями *SDN* та оптимізації пропускної здатності ліній зв'язку.

В статті розглянуто підхід до управління навантаженням в гібридних *SDN*-мережах, який дозволяє знаходити можливі конфігурації поділу потоку трафіку. Це дає змогу формувати політики управління трафіком для попередження перевантажень та оптимізації використання ресурсів пропускної здатності мережі.

Метою статті є створення алгоритму управління в гібридних *SDN*-мережах для мінімізації максимального використання ліній зв’язку в мережі (балансування навантаження) та оптимізації ресурсів пропускної здатності мережі.

Постановка задачі оптимального перерозподілу трафіку в гібридних *SDN*-мережах.

Під гібридною *SDN*-мережею розуміють мережу, у якій поєднуються традиційні технології маршрутизації з технологіями *SDN* (*SDN*-комутатори, *OSPF*-маршрутизатори, комутатори) (рис. 1). Такі мережі є найбільш поширеними на практиці, оскільки, по-перше, базуються на перевірених технологіях передавання даних, а по-друге, застосування *SDN*-контролерів і комутаторів (до 30 % обладнання) суттєво підвищує гнучкість та ефективність мережі [21; 22; 30].

У мережі, що складається з *SDN*-елементів (контролерів і комутаторів *SDN*) та *OSPF*-маршрутизаторів, здійснюється керування трафіком із метою мінімізації максимального навантаження на канали мережі та оптимізації пропускної здатності мережі. *OSPF*-маршрутизатори періодично оновлюють свої таблиці, обчислюючи оптимальні маршрути, тоді як *SDN*-комутатори переналаштовуються за вказівками *SDN*-контролера. Для моніторингу мережі *SDN*-контролер періодично опитує *OSPF*-маршрутизатори та *SDN*-комутатори, отримуючи дані щодо навантаження потоків.

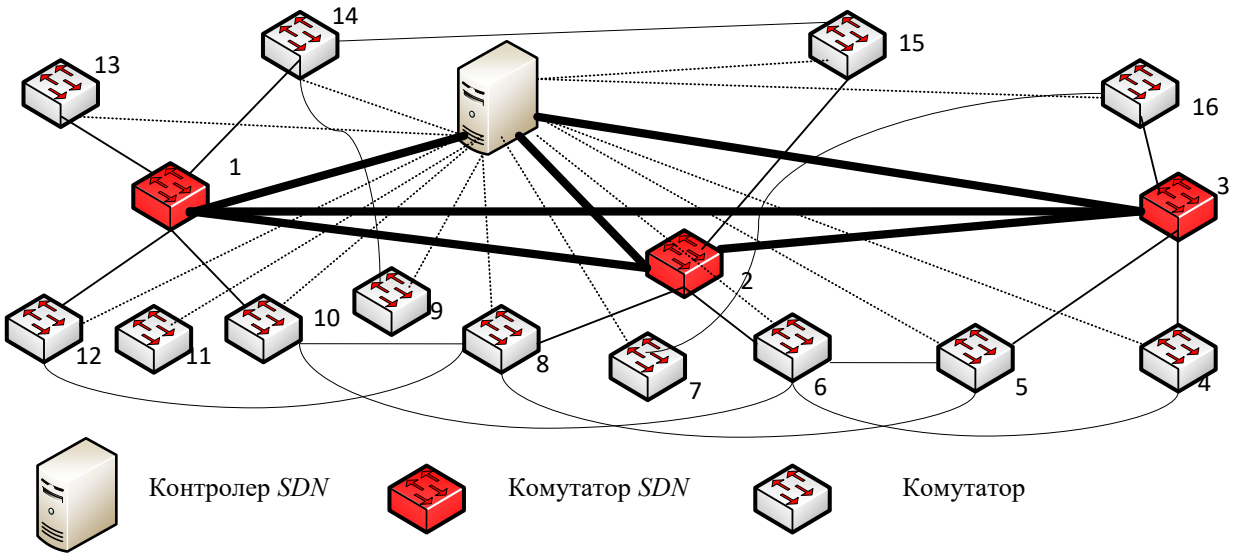


Рис. 1. Варіант використання традиційної технології маршрутизації в поєднанні з технологіями *SDN*

SDN-контролер містить самонавчальну базу знань, у якій зберігаються дані та можливі варіанти розподілу трафіку. На основі аналізу цієї інформації контролер, керований оператором, за допомогою системи підтримки прийняття рішень, формує впливи на *SDN*-комутатори, змінюючи їхню логіку роботи. Це дозволяє автоматизувати процеси маршрутизації, комутації, поділу трафіку, а також формувати політику управління потоками для запобігання перевантаженням та ефективної оптимізації пропускної здатності [22; 28; 29].

Формалізація задачі. Нехай гібридна мережа описується орієнтованим графом $G=(V, E)$, де V – множина вузлів мережі $V=\{\upsilon_1,\dots \upsilon_n\}$, E – множина спрямованих ліній зв’язків

$E=\{\boldsymbol{e_1, \dots, e_m}\} \in \boldsymbol{V \times V}$. Кожна лінія $\boldsymbol{e}$ характеризується b_e – пропускною здатністю, c_e – вартістю передачі одиниці трафіку та ρ_e – коефіцієнтом завантаження. C – множина *SDN*-комутаторів; D – множина комутаторів (маршрутизаторів); $w(e)$ – вага лінії зв'язку *OSPF*; набір $\underline{D} = \{\underline{D}_1, \underline{D}_2, \dots, \underline{D}_K\}$ потоків $к$ повинен бути маршрутизований через мережу. Кожен потік $к$ представляється як кортеж $\underline{D}_k = (h_k, t_k, T_k, P^k_p)$, де h_k і t_k є вузол-джерело та вузол-призначення; T_k – обсяг трафіку, що передається між вузлами; P^k_p – множина допустимих шляхів. $f_{k,p} \geqslant 0$ – реальна кількість трафіку (пропускної здатності) потоку k, яка призначена на шлях $p \in P_k$. T_{ht} – швидкість трафіку від вузла $\boldsymbol{s \in N}$ до деякого іншого вузла $d \in N$; W_{ud} – загальний обсяг трафіку для вузла призначення $d \in N$, що або бере свій початок або проходить через *SDN*-комутатор $e \in C$; P_{ht} – множина допустимих шляхів між h і t; I_{ut} – трафік, який вводиться за допомогою *SDN*-комутатора.

Введемо наступні обмеження. *SDN*-комутатор u може вимірювати W_{ut} для всіх адресатів t, використовуючи розширену таблицю маршрутизації; значення T_{ht} для всіх пар вузлів (h, t) *SDN* контролера не відомо. Для більш ефективного використання мережевих ресурсів, кожен потік може бути передана через кілька шляхів. Однак, для того, щоб обмежити джиттер в загальному потоці, поділ трафіку по декількох шляхах (так званий поділ потоку) може бути виконано тільки на вході пристрою, використовуючи не більше P^k_p шляхів. Для кожного потоку в мережі повинні бути виконані умови (це збереження потоків):

Обмеження. Прийнятий обсяг для потоку k не перевищує обсягу трафіку, що передається між вузлами T_k:

$$\sum_{p \in P_k} f_{k,p} \leqslant T_k, \forall k \in K. \quad (1)$$

Обмеження ємності ребер

$$\sum_{k \in K} \sum_{p \in P_k} f_{k,p} \cdot \delta_{uv}^{k,p} \leqslant b_{uv}, \ \forall (u,V) \in E. \quad (2)$$

Обмеження на виділену смугу для кожного шляху потоку:

$$f_{k,p} \geq 0, \ f_{k,p} \leqslant T_k \cdot z_{k,p}, \ \forall k, \forall p \in P_k, \quad (3)$$

де $z_{k,p} \in \{0,1\}$ – бінарна змінна, що вказує, чи використовується шлях p для потоку k. Зв'язка $f_{k,p} \leqslant T_k \cdot z_{k,p}$ дозволяє лінійно пов'язати використання шляху з присутністю потоку на ньому.

Потрібно, щоб в гібридній мережі G перерозподіл трафіку здійснювався таким чином, щоб враховувалося балансування навантаження і при цьому оптимально використовувалися ресурси пропускної здатності мережі. Це можливо здійснити шляхом перерозподілу трафіку по кільком шляхах.

Механізм поділу потоків. Поділ трафіку на кілька шляхів у гібридній *SDN*-мережі здійснюється на рівні *SDN*-комутатора з використанням хеш-функції. Вона формує числове значення на основі заданих полів пакета (*IP*-адреса джерела та призначення, номери портів, протокол тощо). Комутатор отримує пакет, обчислює хеш і за його результатом вибирає один із кількох можливих шляхів.

Набір умов пересилання, визначений формулами (1)–(3), задає конфігурацію поділу потоку. Пересилання пакетів реалізується через дві таблиці: таблицю пересилання та групову таблицю. Перша відображає пакет у групу розщеплення, друга – розподіляє потоки між наступними переходами за допомогою хеш-функції. Нерівний поділ реалізується повторенням записів у груповій таблиці. Ці записи називають відрами (*buckets*). Вони задають частки

трафіку для кожного маршруту (рис. 2). Завдання *SDN*-контролера полягає в обчисленні конфігурацій відер для комутаторів та передачі відповідних управляючих команд.

Рис. 2. Процес поділу потоку D_1 на три субшляхи з використанням хеш-функції

На рисунку 2 наведено приклад, де потік D_1 розділено з використанням хеш-функції на 3 субшляхи з коефіцієнтами (1/6, 1/3, 1/2). Поділ виконується лише на вході. На проміжних вузлах кожного суб-шляху (наприклад, вузол 4) ніякого розщеплення потоку не допускається, і тільки одне відро потрібно для зберігання умов пересилання. Таблиця пересилання і групова таблиця комутатора u містять відповідно τ_u^F та τ_u^G відра, за умови, що їх сума не перевищує розмір тернарної асоціативної пам'яті *TCAM* комутатора *SDN* мережі. Ємність тернарної асоціативної пам'яті комутатора *SDN* мережі (*TCAM*), де зберігаються правила пересилання, обмежена (до кількох тисяч записів [30]). Це накладає обмеження на поділ і може спричиняти відхилення від оптимального розподілу

Хеш-поділ потоку може відрізнятися від оптимального фракційного поділу вирішенням завдання багатопродуктового потоку (кілька типів трафіку або трафік від конкретного вузла-джерела до конкретного вузла-призначення). Таким чином, постає задача багатопродуктового обмеженого поділу потоку (*Multicommodity Constrained Flow Splitting, MCFS*), яка полягає в максимізації прийнятого трафіку та мінімізації вартості маршрутизації за умови обмежень пропускної здатності, кількості шляхів і обсягу пам'яті *TCAM*.

Нижче наведені всі параметри завдання багатопродуктового обмеженого поділу потоку (*MCFS*) [31]:

h_k – вузол-джерело для потоку k;

t_k – вузол призначення для потоку k;

T_k – трафік, що генерується потоком k;

P^k_p – максимальне число шляхів для потоку k;

c_{uv} – вартість лінії зв'язку (u,v);

b_{uv} – пропускна здатність лінії зв'язку (u,v);

τ_u – TCAM розмір пам'яті вузла u.

MCFS може бути сформульовані наступним чином:

$$max\zeta \ \sum_{k=1}^{K} \sum_{p=1}^{P_p^k} \sum_{(h_k;v)\in E} y_{h_k v}^{kp} - \sum_{k=1}^{K} \sum_{p=1}^{P_p^k} \sum_{(u,v)\in E} c_{uv} y_{uv}^{kp}, \tag{4}$$

$$\sum_{(h_k;v)\in E} x_{h_k v}^{kp} = 1, \ \sum_{(u;h_k)\in E} x_{u h_k}^{kp} = 0, \tag{5}$$

$$\sum_{(t_k;v)\in E} x_{t_k v}^{kp} = 0, \ \sum_{(u;t_k)\in E} x_{u t_k}^{kp} = 1, \tag{6}$$

$$\sum_{(u;v)\in E} x_{uv}^{kp} - \sum_{(v;u)\in E} x_{vu}^{kp} = 0, \ \forall u \in V\{h_k, t_k\}, \tag{7}$$

$$\sum_{k=1}^{K}\sum_{p=1}^{P_p^k} y_{uv}^{kp} \le b_{uv}, \tag{8}$$

$$y_{uv}^{kp} = T_k x_{uv}^{kp} \sum_{Q=1}^{\theta} \frac{q_Q^{kp}}{Q}, \tag{9}$$

$$\sum_{p=1}^{P_p^k} q_Q^{kp} = Q z_Q^k, \quad \sum_{Q=1}^{\theta} z_Q^k = 1, \tag{10}$$

$$\sum_{\substack{k\in K:\\ h_k=u}} \sum_{Q=1}^{\theta} Q z_Q^k + \sum_{\substack{k\in K:\\ h_k\neq u}} \sum_{p=1}^{P_p^k} \sum_{(u,v)\in E} h_{uv}^{kp} \le \tau_u, \tag{11}$$

$$h_{uv}^{kp} \le x_{uv}^{kp}, \quad h_{uv}^{kp} \le q_Q^{kp}, h_{uv}^{kp} \ge \frac{y_{uv}^{kp}}{T_k}, \tag{12}$$

$$x_{uv}^{kp}, h_{uv}^{kp} \in \{0,1\}, y_{uv}^{kp} \in R \tag{13}$$

$$q_Q^{kp} \in \{0, \dots, Q\}, z_Q^k \in \{0,1\}, \tag{14}$$

де ζ – досить велика постійна і $\theta = max\{\tau_u\}$ – це максимальне число правил, які можуть бути збережені в *TCAM*. Якщо цей параметр не заданий, діапазон змінних виглядає наступним чином:

$$k \in K,\ u \in V,\ \ p \in \left\{1, \dots, P_p^k\right\}, (u,v) \in E.$$

Цільова функція (4) в вищенаведеному формулюванні максимізує пропускну здатність, прийняту в мережі, в той час як другий додаток мінімізує витрати маршрутизації серед усіх допустимих рішень з максимально допустимою пропускною спроможністю. Для цього досить встановити, $set\ \zeta = |K||V| \max\limits_{k\in K} P_p^k \cdot \max\limits_{(u,v)\epsilon E} c_{uv}$ так, що збільшення кількості прийнятої смуги пропускання завжди буде пріоритетним в порівнянні зі зменшенням вартості маршрутизації.

Обмеження (5)–(7) по збереженню потоку, дозволяють спрямовувати трафік кожного потоку від свого вузла-джерела h_k до його вузла призначення t_k за P_p^k шляхом. Вони також запобігають циклам, що утворюються у джерела або цілі призначення.

Обмеження (8) гарантують, що обсяг трафіку, що передається по кожному спрямованому зв'язку в (u, v) не перевищує смуги пропускання b_{uv}. Обмеження (9) обчислюють частковий потік y_{uv}^{kp} (тобто пропускну здатність, що призначена шляху *p*) як добуток змінного шляху x_{uv}^{kp}, який вказує шлях *p* потоку *k* та використовує ребро (u, v), та частину потоку *k*, що виділений шляху *p*, а саме $T_k \sum_{Q=1}^{\theta} \frac{q_Q^{kp}}{Q}$. Ці нерівності є нелінійними, так як вони пов'язані з продуктом змінними x_{uv}^{kp} и q_Q^{kp}.

Набір обмежень (10) обмежує конфігурацію відра, визначаючи, скільки відер використовується для кожного шляху p, заданого для потоку *k*. Зокрема, друге обмеження в (10) обирає лише одну загальну кількість відер *Q*, щоб бути використаними для потоку *к* серед θ можливостей в більшості, і перше обмеження гарантує, що це число *Q* розподіляється і користується потоком *к* тому, що тільки одна величина *Q* є активною, змінні q_Q^{kp} можуть бути ненульовим тільки для одного значення *Q* в (10). Таким чином, вираз $\sum_{Q=1}^{\theta} \frac{q_Q^{kp}}{Q}$ в (9) дає частку потоку *k*, яка виділяється в шлях *p*.

Обмеження (11) гарантують, що правила пересилання визначені як для розщеплення потоку, що виникають на вузлі *u*, так шляху, які проходять через вузол *u*, та не перевищують ємність *TCAM u*. Для підрахунку, скільки відер повинні бути зарезервовано для пересилання правил, ми не можемо підсумувати всі вимоги змінних x_{uv}^{kp}, які вказують на активацію витікаючих зв'язків для шляху p. Дійсно, оптимальним рішенням можна вибрати шлях з нульовим потоком на ньому ($x_{uv}^{kp}=1$ та $y_{uv}^{kp}=0$). З цієї причини, ми використовуємо двійкові змінні h_{uv}^{kp} в другій сумі (11), і ми також визначили обмеження (12), (13) щоб встановити змінну $h_{uv}^{kp}=1$, тільки якщо деякий трафік потоку *к* направляється до місця призначення по шляху *p* по лінії зв'язку (u, v). Нарешті, обмеження (14) визначають області рішення наших змінних.

Ми бачимо, що вищевказані формулювання дійсні для мережі зі спрямованими зв'язками. Однак, ми можемо легко відновити формулювання з неорієнтованим зв'язком шляхом інтерпретації (u, v) як в протилежному напрямку (v, u), так і замінити y_{uv}^{kp} на $y_{uv}^{kp}+y_{vu}^{kp}$ в обмеженнях (8).

Щоб вирішити проблему *MCFS,* запропоновано метаеврістіческій підхід, який називається ітераційне розслаблення з масштабуванням і округленням Iterative Relaxation with Scaling and Rounding (*IRSR*). *IRSR* – відноситься до наближеного (евристичного) методу, який:

спочатку розслабляє початкову (часто цілочислову) задачу до задачі лінійного програмування (*LP*);

потім масштабує значення потоків (зменшує масштаб, щоб простіше округлювати);

далі округлює знайдене дробове рішення до цілочислового (або до значень, прийнятних для практичного використання в *SDN*);

і, на решті, ітеративно повторює процес, покращуючи рішення та виконуючи повторне виділення ресурсів, поки не буде досягнуто прийнятного рішення або поки не вичерпано обчислювальний ресурс;

дозволяє розв'язувати великі задачі швидше, ніж точні методи (такі як *ILP*);

отримувати наближене рішення з гарантіями щодо відхилення;

підтримувати адаптивність у реальному часі, що особливо важливо в *SDN* мережах, де маршрути можуть динамічно змінюватись [32].

Алгоритм ітераційного розслаблення з масштабуванням і округленням (*IRSR*). Оскільки вирішення цілочисельного лінійного програмування *MILP* нездійсненно з обчислювальної точки зору, розглянемо лінійне розслаблення, видаляючи обмеження шляху і відра. Вирішуючи отриманий *LP*, який ми називаємо розслабленим *LP* (*RLP*), дамо набір засобів для підмножини вимог [32]. Недоліком цього підходу є те, що вимога $\underline{D}_K$ в кінцевому підсумку, працює більш ніж по P_p^k шляхів, і оскільки обсяг потоку на кожному шляху є дробовим, то воно також не узгоджується з обмеженнями відра, яке розташоване в оригінальній *MILP*. Таким чином, ці порушення повинні бути виправлені для отримання відповідного рішення.

Припустимо, що вимога $\underline{D}_K$ була допущена в рішенні *RLP* і припустимо, що $\hat{P_p^k} > P_p^k$ шляхів були виділені на це. Розглянемо $\hat{P_p^k} > P_p^k$ шляхів з найменшою кількістю смуги пропускання $\underline{D}_K$, що виділяються на них. Ми видаляємо їх і рівномірно перерозподіляємо їх пропускні спроможності на інші P_p^k шляхи. Після цього перерозподілу шляху, ми виходимо з округленого відра в спробі знайти відповідне рішення в рамках розмірності відра, що дається на кожну вимогу відра обмежень.

При виконанні вищевикладеного може виявитися, що краї ємностей порушуються. Ми маємо справу з цим двома способами: по-перше, перш ніж вирішувати *RLP*, ми множимо краї ємності мережі на (1 – α), де α ∈ [0,1) – параметр. Можливості, що обмежуються таким чином, можуть змусити *RLP* вибрати більш дорожчі шляхи, але це дає нам можливість виконувати наступні фази перерозподілу і округлення (які, звичайно ж, виконуються з

фактичними ємностями країв). Насправді, оскільки ми не знаємо α апріорно, яке гарне значення α, ми пробуємо їх набір і вибираємо той, який дає кращий результат з точки зору виділеної смуги пропускання після фази округлення відра. Це можна зробити паралельно, оскільки платформи *SDN* мають велику обчислювальну потужність.

Другий спосіб, з яким ми маємо справу з порушеннями пропускної здатності – це ітерація: вимоги, які відкидаються для порушення обмежень пропускної здатності, стають внеском в інше округлення алгоритму. Ми продовжуємо ітерацію до тих пір, поки не буде досягнуто якогось поліпшення в кількості виділень або розподілі всіх вимог.

Слід зазначити, що ми вирішуємо *RLP* з використанням генерації стовбцю (Column Generation – *CG*), що є підходом, який часто ефективний при роботі з *LP* з великим числом змінних. Однак *CG* можна не використовувати, і замість цього може бути використаний будь-який відомий алгоритм для вирішення *LP*, наприклад:

1. Масштабування. Завдання масштабів країв пропускної здатності (1 - α).

2. Розслаблений *LP* (*RLP*). Видалення номера шляху і обмеження відра, ослаблення цілих змінних і рішення.

3. Проміжні відра. Для кожного (повністю або частково) виділеного запиту $\underline{D}_K$ видаляється один запис у вигляді відра з кожного вузла по кожній шляху в розподілі (маршрутизація шляху через *TCAM* важить одному запису).

4. Відро округлення. Використати округлення в результуючий мережі і вимагати установки для отримання розміру *B* відра для кожного запиту.

5. Перерозподіл шляхів. Для кожного (повністю або частково) виділеного $\underline{D}_K$, якщо $\hat{P}_p^k > P_p^k$ йому були виділені шляхи, то рівномірно перерозподілити $\hat{P}_p^k > P_p^k$ надлишкові шляхи на найбільш сильно розподіленому P_p^k.

6. Округлення відер. Для кожного виділеного $\underline{D}_K$ для b= 1,..., B_k перерозподіляється потік між виділеними (не більше P_p^k) підшляхами $\underline{D}_K$ в одиницях d_k/b, щоб максимально точно відтворити попередній розподіл.

7. Фільтрація. Проведення перевірки, які вимоги тепер порушують обмеження пропускної здатності. Виконати це послідовно, завжди перевіряючи залишки мережі на вже виділені вимоги.

8. Оновлення залишкових відер. Оновлювати використання відер як на вихідних вузлах, так і на проміжних вузлах для вимог, які були виділені під час цієї ітерації.

9. Ітерація. Всі вимоги, відхилені на попередній фазі, стають внеском в повторення цього виділеного алгоритму.

Слід зазначити, що округлення відра є нетривіальним завданням. Підхід полягає в наступному: для кожного виділеного $\underline{D}_K$ виділяється відра по одному, і при цьому створюється профіль потоку для кожного шляху для $\underline{D}_K$ на основі цих відер. Якщо ми збираємося додати рівно *b* відер в цілому, то кожне відро додає d_k/b до мінімуму шляху, якому він призначений. Відро поміщається випадковим чином на розподіл ймовірності, що отримане з профілю потоку, яке викликане розподілом поточного відра і яке задається рішенням *RLP*. Більша відмінність цих профілів по конкретному шляху робить його більш імовірним, що відро буде прив'язане до цього шляху.

Переваги алгоритму *IRSR*. Обчислювальна ефективність – значно менші витрати часу порівняно з *ILP*-методами. Адаптивність – можливість повторного запуску при зміні стану мережі. Якість рішень – гарантує допустимий розподіл, близький до оптимального.

Висновки

Сформульовано та досліджено задачу оптимального розподілу потоків у гібридних *SDN*-мережах з урахуванням обмежень пропускної здатності та ресурсів *TCAM*. Доведено, що точне розв'язання є *NP*-складним, тому запропоновано використання наближеного алгоритму *IRSR*.

Отримані результати підтверджують ефективність підходу для балансування трафіку та запобігання перевантаженням. Подальші дослідження будуть спрямовані на інтеграцію методів прогнозування та інтелектуального керування для підвищення рівня автоматизації та ефективності трафік-інженерії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Konrad Połys, Krzysztof Grochla, Michał Gorawski. LTE Load Balancing with Tx Power Adjustment and the Real Life Mobility Model // Computer Networks (CN 2018). Pp. 183–192.

2. Ahmed Hazim Alhilali, Ahmadreza Montazerolghaem. Artificial intelligence based load balancing in SDN: A comprehensive survey Networking and Internet Architecture (cs.NI). URL: https://doi.org/10.48550/arXiv.2308.02149.

3. Alejandro Aguilar-Garcia, Raquel Barco, Sergio Fortes, Pablo Muñoz. Load balancing mechanisms for indoor temporarily overloaded heterogeneous femtocell networks. *EURASIP Journal on Wireless Communications and Networking.* 2015. Article number: 29.

4. Електронне посилання від 06.10.2025. URL: https://avinetworks.com/what-is-load-balancing/.

5. Електронне посилання від 10.10.2025. URL: https://www.resonatenetworks.com/2020/05/25/what-are-the-different-types-of-load-balancers/.

6. Електронне посилання від 16.10.2025. URL: https://www.dnsstuff.com/what-is-server-load-balancing.

7. A Survey on Static and Dynamic Load Balancing Algorithms in Cloud Computing (Mukati & Upadhyay, 2019).

8. A Comprehensive Study of Static, Dynamic and Hybrid Load Balancing (Hamadah, ~2014).

9. Load balancing in cloud computing: Methodological survey on different types of algorithm (~2016).

10. Dynamic Load Balancing in Cloud Computing: A Review and a Novel Approach (Laha et al., 2024).

11. Load balancing techniques in cloud computing environment (Shafiq et al., 2022).

12. Comparative analysis of metaheuristic load balancing algorithms for efficient load balancing in cloud computing (Zhou et al., 2023).

13. Classification of Load Balancing Optimization Algorithms (Moharamkhani, 2024).

14. Elastic neural network method for load prediction in cloud computing grid (Qaddoum et al., IJECE).

15. Host Load Prediction with Bi-directional Long Short-Term Memory in Cloud Computing (Shen & Hong, 2020).

16. A hybrid CNN-LSTM model for predicting server load in cloud computing (2024).

17. Hierarchical Load Balancing Strategy in Cloud Environment (RTIS 2017 / Springer, 2018).

18. Multi-Level Load Balancing Methods for Hierarchical Web Server Clusters (Yeon & Jeong, 2015).

19. Centralized and Decentralized Non-Cooperative Load-Balancing Games among Federated Cloudlets (Mondal et al., 2020).

20. A Load-Balance System Design of Microgrid Cluster Based on Hierarchical Petri Nets (Sicchar et al., 2018).

21. Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Jonathan Turner. OpenFlow: Enabling Innovation in Campus Networks // ACM SIGCOMM Computer Communication Review (CCR). 2008. DOI: 10.1144/ccr.38.2.69.

22. S. A. Al-rubaye, Z. H. Zaidan, R. H. Zaidan, M. S. Mahmood, O. M. J. Al-Musa, T. M. Al-Jobouri. Elephant Flow Detection and Migration for Software-Defined Networks: A Comprehensive Review // Wireless Personal Communications. 2022. DOI: 10.1007/s11277-022-10023-x.

23. S. Al-rubaye, J. L. De La Fuente-Moya, J. A. Hernandez, P. S. S. De Silva SDN Controller Load Balancing Based on Reinforcement Learning. 2021 IEEE International Conference on Communications Workshops (ICC Workshops). DOI: 10.1109/ICCWorkshops50700.2021.9473859.

24. Y. Mao, Y. Ji, Y. Li, S. Mao, T. Zhang, B. Ning, N. Zhang. Deep Reinforcement Learning for Network Traffic Engineering: A Survey // IEEE Communications Surveys & Tutorials. 2021. DOI: 10.1109/COMST.2021.3060505.

25. K. A. H. Hassan, M. S. Rahman, M. A. A. Al-Haj, A. F. M. S. Islam. Multi-path Load Balancing in SDN Using Link Status and Traffic Type. 2020. 2nd International Conference on Advanced Information and Communication Technology (ICAICT). DOI: 10.1109/ICAICT50694.2020.9273574.

26. A. E. M. E. Elghoniemy, E. I. Hassan, M. M. Fouad Energy-Efficient Load Balancing in Software-Defined Data Centers: A Deep Reinforcement Learning Approach // IEEE Access. 2023. DOI: 10.1109/ ACCESS.2023.3243161.

27. J. R. Aguilar-Velazco, F. H. Rivera-Reyes, F. J. Ramos-Velasco, M. A. Portilla-Flores. Deep Learning-Based Load Balancing for Software-Defined Networking // Sensors. 2024. DOI: 10.3390/s24082531.

28. H. A. K. Al-Hasib, M. N. A. Khan, K. M. A. Salam, M. Z. Abedin. A Load Balancing and Fault Tolerance Mechanism for SDN Controllers Using Trust and Reputation System // IEEE Access. 2022. DOI: 10.1109/ACCESS.2022.3142079.

29. F. M. H. Aldughaim, M. K. Abdullah, S. D. Al-Sharabi. Traffic Engineering for Low Latency and High Throughput in Software-Defined Networks: A Survey // Journal of Network and Computer Applications. 2021. DOI: 10.1016/j.jnca.2021.103009.

30. H. N. Ahmed, M. I. Sarim, S. N. Che-Pazi, N. A. A. Nordin. Hybrid Load Balancing for Software Defined Networks with Multiple Controllers // 2020 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS). DOI: 10.1109/IoTaIS50847.2020.9329402.

31. Бовда Е. М. Метод управління перерозподілом навантаження в SDN мережах // Зб. наук. праць / Військовий інститут телекомунікації та інформатизації. Київ, 2017. С. 6–16.

32.François Lamothe, Emmanuel Rachelson, Alain Haït, Cedric Baudoin, Jean-Baptiste Dupe. Randomized rounding algorithms for large scale unsplittable flow problems. URL: https://doi.org/ 10.1007/s10732-021-09478-w.

DOI: 10.58254/viti.8.2025.14.163

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)
д-р філософії Фомін М. М. ORCID: 0000-0002-6864-4238 (ВІТІ ім. Героїв Крут)
д-р техн. наук, професор Туровський О. Л. ORCID: 0000-0002-4961-0876 (ДУІКТ)
Лисенко Д. О. ORCID: 0009-0009-5120-7929 (ДУІКТ)

АНАЛІЗ ВПЛИВУ ФАЗОВИХ ШУМІВ НА ПАРАМЕТРИ РОБОТИ СИСТЕМ СИНХРОНІЗАЦІЇ МЕРЕЖ КОГНІТИВНОГО РАДІО В УМОВАХ НЕСТАБІЛЬНОСТІ НАПРУГИ ЖИВЛЕННЯ ОПОРНИХ ГЕНЕРАТОРІВ

У роботі проведено аналіз впливу фазових шумів на параметри роботи систем синхронізації мереж когнітивного радіо на фоні нестабільності напруги живлення опорних генераторів.

У першій частині дослідження проведено оцінку впливу похибок пристрою фазової синхронізації та пристрою тактової синхронізації на достовірність повідомлення, що приймається. Отримані залежності ймовірності помилки когерентного прийому протилежних двійкових сигналів за наявності похибок фазової та тактової синхронізації чисельними методами.

У другій частині розроблена імітаційна модель оцінки впливу фазових шумів на параметри роботи систем синхронізації мереж когнітивного радіо на фоні нестабільності напруги живлення опорних генераторів. За основу була взята лінійна модель фазової петлі (PLL) з ПІ-фільтром (пропорційно-інтегральний фільтр). Новизна дослідження полягає у розробці імітаційної моделі фазової петлі з ПІ-фільтром, яка дозволяє оцінювати вплив фазових шумів та нестабільності напруги живлення опорних генераторів на параметри синхронізації. Отримано залежності спектральної щільності фазової помилки та передаточної функції від шуму живлення до фазової помилки, що дозволяє кількісно оцінити механізм проникнення нестабільності живлення в частотні характеристики PLL. Проведено чисельне порівняння впливу параметрів ПІ-фільтра (T_i, Kf) на якість роботи PLL та стійкість системи до шумів живлення, що поглиблює методику оптимізації параметрів синхронізаторів. Практична цінність дослідження: розроблена модель дозволяє прогнозувати стійкість систем синхронізації когнітивних радіомереж у реальних умовах, коли опорні генератори зазнають впливу нестабільності живлення. Отримані результати можуть бути використані під час проєктування PLL-структур для когнітивних приймачів, де критично важливе збереження когерентності прийому при дії внутрішніх шумів та завад. Визначені критерії (спектральна щільність, RMS фазова помилка), які можуть застосовуватись як метрики надійності та якості для порівняння різних архітектур систем синхронізації.

У третій частині розроблена методика оцінки впливу точності стабілізаторів напруги на фазову стабільність системи синхронізації. Наукова новизна розробленої методики: запропоновано новий підхід до кількісної оцінки впливу нестабільності стабілізаторів живлення на фазову стабільність систем синхронізації; розроблено MATLAB-модель, яка дозволяє проводити віртуальні експерименти та визначати допустимі межі нестабільності живлення з урахуванням конкретних параметрів PLL та VCO.

Ключові слова: *фазові шуми, нестабільність живлення, методика оцінки впливу точності стабілізаторів напруги.*

V. Saiko, G. Radzivilov, V. Komarov, M. Fomin, O. Turovskyi, D. Lysenko. Analysis of the influence of phase noise on the operation parameters of cognitive radio network synchronization systems in conditions of instability of the power supply voltage of reference generators

The paper analyzes the influence of phase noise on the operation parameters of cognitive radio network synchronization systems against the background of instability of the power supply voltage of reference generators. In the first part of the study, the influence of the errors of the phase synchronization device and the clock synchronization device on the reliability of the received message was assessed. The dependences of the probability of error of coherent reception of opposite binary signals in the presence of phase and clock synchronization errors were obtained by numerical methods. In the second part, a simulation model was developed to assess the influence of phase noise on the parameters of the synchronization systems of cognitive radio networks against the background of instability of the supply voltage of the reference generators. The basis was taken as a linear model of the phase loop (PLL) with a PI filter (proportional-integral filter). The novelty of the study lies in the development of a simulation model of the phase loop with a PI filter, which allows to assess the influence of phase noise and instability of the supply voltage of the reference generators on the synchronization parameters. The dependences of the spectral density of the phase error and the transfer function from the supply noise to the phase error were obtained, which allows to quantitatively assess the mechanism of penetration of the supply instability into the frequency characteristics of the PLL. A numerical comparison of the influence of PI filter

parameters (T_i, Kf) on the quality of PLL operation and the system's resistance to power supply noise was carried out, which deepens the methodology for optimizing synchronizer parameters. Practical value: the developed model allows predicting the stability of synchronization systems of cognitive radio networks in real conditions, when reference oscillators are affected by power supply instability. The results obtained can be used in the design of PLL structures for cognitive receivers, where it is critically important to maintain reception coherence under the influence of internal noise and interference. The determined criteria (spectral density, RMS phase error) can be used as reliability and quality metrics for comparing different architectures of synchronization systems. In the third part, a methodology for assessing the influence of voltage stabilizer accuracy on the phase stability of the synchronization system is developed. Scientific novelty of the developed methodology: a new approach to quantitatively assessing the influence of power supply stabilizer instability on the phase stability of synchronization systems is proposed; A MATLAB model has been developed that allows for virtual experiments and the determination of acceptable limits for power supply instability, taking into account specific PLL and VCO parameters.

Keywords: *phase noise, power supply instability, method for assessing the impact of voltage stabilizer accuracy.*

Постановка завдання у загальному вигляді

Розвиток когнітивних радіомереж обумовлює підвищені вимоги до надійності та завадостійкості систем синхронізації, які забезпечують коректне відновлення фазових і часових параметрів сигналів. В умовах динамічного використання спектра, високого рівня завад і мінливих характеристик каналів зв’язку похибки синхронізації безпосередньо впливають на достовірність прийому повідомлень та ефективність функціонування мережі.

Особливу увагу привертають фазові шуми та нестабільність напруги живлення опорних генераторів, що призводять до зміни робочої частоти генераторів та погіршення характеристик фазових автопідлаштованих систем (PLL). Це може зумовлювати виникнення додаткової фазової помилки, зростання ймовірності бітових помилок при когерентному прийомі та зниження стійкості системи синхронізації.

Традиційні підходи до аналізу фазових автопідлаштованих систем розглядають їх у ідеалізованих умовах, часто нехтуючи впливом нестабільності живлення та внутрішніх шумів. У сучасних когнітивних мережах така спрощена модель є недостатньою. Необхідним є створення більш детальної моделі, що враховує чутливість фазового детектора, параметри керованого генератора Voltage-Controlled Oscillator (VCO), характеристики ПІ-фільтра та додаткові фактори, зокрема вплив шумів живлення.

Таким чином, актуальною є задача розробки імітаційної моделі фазової петлі з ПІ-фільтром та оцінки впливу фазових шумів і нестабільності напруги живлення на параметри синхронізації когнітивних радіомереж. Це дозволить отримати кількісні характеристики фазових помилок, визначити критичні параметри системи та сформувати практичні рекомендації для проєктування надійних синхронізаторів у когнітивних приймачах. Важливою також є розробка методики оцінки впливу точності стабілізаторів напруги на фазову стабільність системи синхронізації.

Аналіз публікацій за темою досліджень

Вступ до проблематики

Польові та лабораторні дослідження когнітивних радіомереж підтверджують, що надійність когерентного прийому значною мірою визначається якістю фазової та часової синхронізації. Ключовими джерелами деградації є фазовий шум опорних генераторів, джитер, а також проникнення шумів живлення у контур PLL та тракти відновлення тактової частоти. Тому сучасні роботи фокусуються на моделюванні шумів, методах їх фільтрації та оптимізації параметрів контуру [1–5].

Моделі фазового шуму та основи PLL

Класичні праці з фазових автопідлаштованих систем [1–18] обґрунтовують використання лінійної моделі малих сигналів PLL, де ПІ/ПІД-фільтри формують бажану смугу пропускання та запас стійкості. Для оцінки власних шумів генератора застосовують моделі на кшталт формули Лісона [2] та стохастичні описи шуму фази/частоти. Подальші роботи

деталізують джерела шуму у фазовому детекторі, керованому генераторі (VCO) та у ланцюгах керування напругою, підкреслюючи роль параметрів чутливості K_d та K_f [5].

Вплив похибок фазової і тактової синхронізації на BER

У літературі показано, що систематична та випадкова фазові похибки призводять до ефективного зменшення відношення сигнал/шум на вході детектора, що безпосередньо підвищує ймовірність бітової помилки при когерентному прийомі BPSK/QPSK [3; 4]. Для тактової синхронізації джитер семплювання викликає міжсимвольні завади та зміщення рішення, що погіршує характеристики приймача навіть при незмінних канальних умовах. Поширеною є практика оцінювати BER через інтегральну (RMS) фазову помилку в заданій смузі частот та її зв’язок з еквівалентним SNR-перекосом [5].

Проникнення шумів живлення у контур синхронізації

Окрема група робіт присвячена впливу нестабільності живлення на частоту VCO та контурне керування [5; 8]. Автори вводять коефіцієнт чутливості частоти до напруги живлення (PSKVCO) і розглядають шлях перетворення шуму живлення у фазову помилку через передаточні функції PLL. Зазначається важливість високого коефіцієнта придушення пульсацій живлення (PSRR) регуляторів, ізоляції живлення VCO/мікшера, використання LDO/фільтрів НЧ та правильного трасування землі [8].

Оптимізація ПІ-фільтра та вибір смуги контуру

Дослідження показують компроміс між швидкодією та завадостійкістю: ширший контур краще придушує низькочастотні відхилення, але пропускає більше високочастотних шумів фази; занадто вузький — погіршує захоплення та стійкість до доплерівських/частотних зсувів [1; 3]. Запропоновані методики налаштування (через коефіцієнти підсилення та запас фазової стійкості) дозволяють мінімізувати інтегральну фазову помилку з урахуванням спектра джерел шуму та вимог до часу захоплення [4; 5].

Метрики та підходи до моделювання

Сучасні публікації рекомендують використовувати узгоджені метрики: спектральну щільність фазової помилки, інтегральну (RMS) фазову помилку у робочій смузі, передаточні функції від зовнішніх збурень (живлення, температура) до фази, а також емпіричні залежності BER для типових модуляцій [2; 4; 5]. Імітаційні моделі у середовищах MATLAB/Simulink та Python дозволяють поєднати лінеаризовані моделі PLL із шумовими збудженнями, відтворити як стаціонарний режим, так і перехідні процеси (захоплення/утримання синхронізму).

Системи синхронізації в когнітивному радіо

У контексті когнітивного радіо підкреслюється, що динамічний доступ до спектра і перестроювання несучої/тактової частоти підсилюють вимоги до швидкого захоплення та низького рівня фазової помилки [6; 7; 9]. Досліджуються адаптивні стратегії налаштування параметрів PLL залежно від сценарію використання спектра, каналів із завмираннями та наявності зовнішніх завад, а також взаємодія контурів фазової і тактової синхронізації у приймачах з багатостандартною підтримкою [7; 9; 10].

Відомі підходи до зниження впливу шумів

Серед інженерних рішень виділяють: рознесення живлення «чутливих» блоків, застосування високоякісних опорних генераторів із низьким фазовим шумом, оптимізацію коефіцієнтів підсилення, а також методи післядетекторної обробки (фазова згладжувальна фільтрація, відстеження частоти) [5; 8]. Для тактової синхронізації використовують петлі відновлення такту з покращеною фільтрацією джитера та алгоритмічне пригнічення ISI [3; 4].

Висновки за результатами огляду і дослідницькі прогалини

Незважаючи на значний прогрес у моделюванні та інженерних рішеннях, менше уваги приділено стику двох факторів: одночасному впливу фазових шумів і нестабільності живлення опорних генераторів у когнітивних приймачах з ПІ-фільтрами [9; 10]. Обмежено представлені узгоджені порівняння варіантів налаштування за інтегральною фазовою помилкою, спектральними метриками та безпосереднім впливом на BER у динамічних сценаріях

когнітивного радіо [7; 9]. Заповненню саме цієї прогалини присвячена ця робота, де поєднано чисельну оцінку похибок фазової/тактової синхронізації з імітаційним моделюванням впливу шумів живлення у лінійній PLL з ПІ-фільтром.

Постановка завдання

Метою роботи є дослідження впливу фазових шумів на параметри роботи систем синхронізації мереж когнітивного радіо на фоні нестабільності напруги живлення опорних генераторів.

Виклад основного матеріалу

І. Оцінка впливу похибок пристроїв фазової та тактової синхронізації на достовірність повідомлення, що приймається

Системи синхронізації важливі для забезпечення правильної роботи багатьох електронних пристроїв, особливо в телекомунікаціях та обробці сигналів. У таких системах часто використовується опорне коливання, яке служить еталоном для інших сигналів. Метод синхронізації по миттєвій фазі (СПМ) дозволяє досягти високої точності синхронізації, враховуючи миттєву зміну фази опорного коливання. Це особливо важливо в умовах, коли фаза коливання може змінюватися з часом, наприклад, через завади або зміни умов передачі сигналу.

У цій частині розглянемо аспекти впливу на сигнал короткочасної нестабільності частот опорних генераторів систем синхронізації — фазового шуму. Треба зауважить, що шум живлення підключається до внутрішнього процесу генерації частоти VCO і являє собою зовнішнє збурення, яке додається паралельно до керуючого сигналу в частотному домені. Контур може частково або повністю пригнічувати цей вплив у смузі регулювання. VCO — Voltage-Controlled Oscillator, українською — *генератор, керований напругою*. Його основна властивість: частота вихідного сигналу змінюється пропорційно прикладеній керуючій напрузі. У контексті PLL (фазової автопідлаштованої системи) VCO — це елемент, який «підганяє» свою частоту під еталонний сигнал так, щоб зменшити фазову помилку. Ключовим параметром VCO є фазовий шум — власний шум генератора, який впливає на стабільність сигналу.

Наявність флуктуацій фази призводить до того, що СПМ опорного коливання виявляється відмінною від дельта-функції. Можна показати, що спектр прийнятого сигналу є згорткою спектрів переданого сигналу та опорного коливання. Таким чином, крім випадкового повороту сигнального сузір’я відбувається розмиття форми прийнятого сигналу в частотній області, втрата ортогональності між піднесучими, і, як наслідок, посилення міжканальної інтерференції (МКІ). Зі зменшенням відстані між піднесучими вплив фазових шумів значно посилюється і може призвести до непрацездатності системи. Нині існують системи, в яких відстань між піднесучими вимірюється сотнями герц — одиницями кілогерц. Це вимагає застосування високостабільних опорних генераторів як на передавальній, так і на приймальній стороні, а також спеціальних алгоритмів обробки сигналу для оцінки та компенсації як флуктуації фази, так і МКІ. Вплив фазового шуму на OFDM-системи оцінено в [17; 18]. Але дослідженню питань, які пов’язані з впливом нестабільності напруги у системах синхронізації на якісні характеристики сигналів приймальних пристроїв, розробники не достатньо приділяють увагу. Тому далі ми зупинимося більш детально на цьому питанні.

Робота окремих ступенів системи синхронізації по-різному позначається на якості роботи мереж радіозв’язку загалом. Похибки в роботі пристрою циклової синхронізації (ПЦС) та пристрою кадрової синхронізації (ПКС) призводять до неправильного прийому всього повідомлення або частини його, а в роботі пристрою фазової синхронізації (ПФС) та пристрою тактової синхронізації (ПТС) — до зниження його достовірності. Оцінимо вплив похибок ПФС та ПТС на достовірність повідомлення, що приймається. ПФС входить до складу когерентного демодулятора та забезпечує збіг по фазі напруги місцевого генератора та несучої

частоти. Похибки $\Delta\varphi$ ПФС призводять до зменшення відношення сигнал/ шум на виході пристрою обробки:

$$q^2(\Delta\varphi) = \left(\frac{2E}{N_0}\right) cos^2(\Delta\varphi), \quad (1)$$

де q^2 — ефективне відношення сигнал/шум (SNR) на виході приймача;
E — енергія символу (для BPSK — енергія біта);
N_0 — спектральна густина шуму (одностороння);
$\Delta\varphi$ — похибка фазової синхронізації (рад).

Тому, оцінюючи достовірність повідомлення з урахуванням помилок ПФС, можна ввести умовну ймовірність помилки $P_{о\,ш}(\Delta\varphi)$. Якщо швидкість флуктуації помилок ПФС мала (інтервал кореляції випадкового процесу $\Delta\varphi(t)$ багато більше тривалості посилок), то середню ймовірність помилок $\overline{P_{о\,ш}}(\Delta\varphi)$ можна знайти за формулою:

$$\overline{P_{о\,ш}}(\Delta\varphi) = \int_{-\pi}^{\pi} P_{о\,ш}(\Delta\varphi)\, w(\Delta\varphi) d(\Delta\varphi), \quad (2)$$

де $P_{ош}(\Delta\varphi)$ — умовна ймовірність помилки при фіксованій Δφ;
$w(\Delta\varphi)$ — густина ймовірності похибки $\Delta\varphi$ (далі — гаусівська, $N(0, \sigma_\varphi^2)$.

Складність залежності ймовірності помилок $P_{о\,ш}$ від похибки $\Delta\varphi$ не дозволяє отримувати точну формулу для $P_{о\,ш}(\Delta\varphi)$. Тому користуються або наближеними співвідношеннями, знайденими за тих чи інших спрощеннях, або чисельними методами. Вплив помилок ПФС на стійкість до завад можна оцінити за наближеною формулою, справедливою для систем із фазовою модуляцією будь-якої кратності m:

$$\overline{P_{о\,ш}}(\Delta\varphi) \approx 1 - \Phi\left[\frac{\pi}{m}\frac{h}{\sqrt{1+2\sigma_\varphi^2 h^2}}\right], \quad (3)$$

де $\Phi(x)$ — функція Лапласа-Гауса (CDF стандартного нормального), $1 - \Phi(x) = Q(x)$;
m — кратність фазової модуляції (для BPSK $m = 2$);
$h = \sqrt{2E/N_o}$ — похибка фазової синхронізації;
σ_φ — СКВ похибки фази (рад).

Значення σ_φ у формулі (3) задано у радіанах.

Графік залежності ймовірності помилки когерентного прийому протилежних двійкових сигналів за наявності похибок фазової синхронізації наведено на рисунку 1.

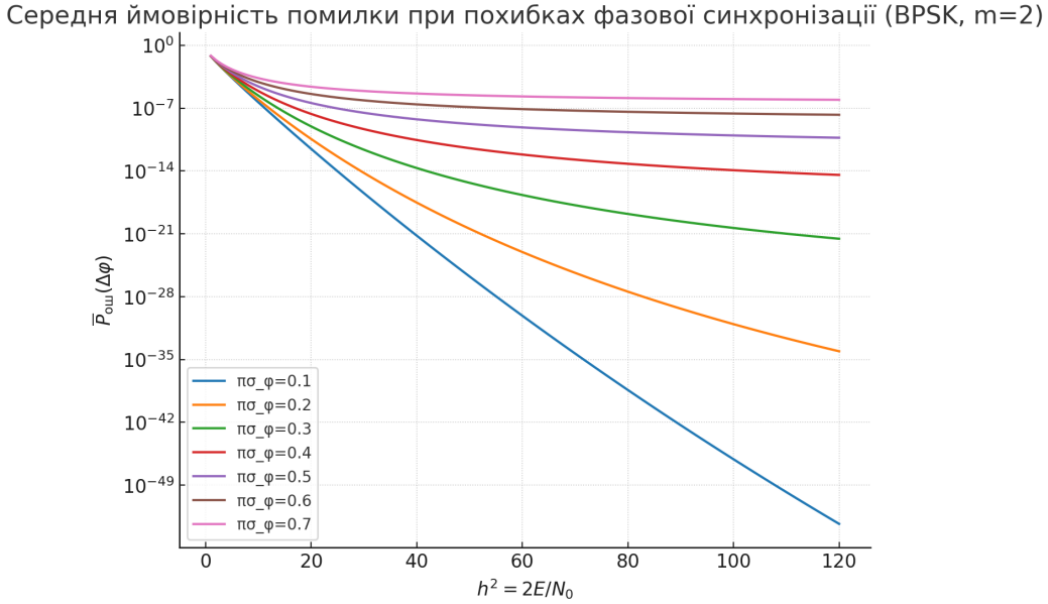


Рис. 1. Залежності ймовірності помилки когерентного прийому протилежних двійкових сигналів за наявності похибок фазової синхронізації

Похибки тактової синхронізації призводять до того, що момент відліку напруги на виході корелятора або узгодженого фільтра не відповідає моменту закінчення посилки. Тоді при зміні символів на вході вирішальної схеми будуть накопичуватися сигнали від посилок різного знака і відношення сигнал/шум q^2 зменшиться:

$$q^2(\varepsilon) = q^2(1 - 2|\varepsilon|), \tag{4}$$

де ε — нормована похибка моменту відбору (частка тривалості символу; $|\varepsilon| \leq 0.5$ — «вікно» синхронного відбору).

Ввівши умовну ймовірність помилки $P_{о\,ш}(\varepsilon)$ і знаючи закон зміни $w(\varepsilon)$, можна обчислити середню ймовірність помилки $\overline{P_{о\,ш}}(\varepsilon)$ аналогічно (2). Як і в попередньому випадку, кількісні результати можна отримати чисельними методами. Помилки тактової синхронізації, на відміну від фазової, будуть впливати тільки на прийом символів, що чергуються.

Для випадкової послідовності двійкових символів імовірність зміни знаку дорівнює 0,5, а середня ймовірність помилки дорівнює:

$$\overline{P_{о\,ш}}(\varepsilon) = 0{,}5\,[P_{о\,ш}(\varepsilon) + P_{о\,ш}], \tag{5}$$

де $P_{ош}(\varepsilon)$ — умовна BER для символів, що чергуються, за наявності ε;

$P_{ош}$ — BER при ідеальній тактовій синхронізації (для BPSK $P_{ош} = Q(h)$);

множник 0,5 — імовірність чергування бітів у випадковій двійковій послідовності.

Графік залежності ймовірності помилки когерентного прийому протилежних двійкових сигналів за наявності похибок тактової синхронізації наведено на рисунку 2.

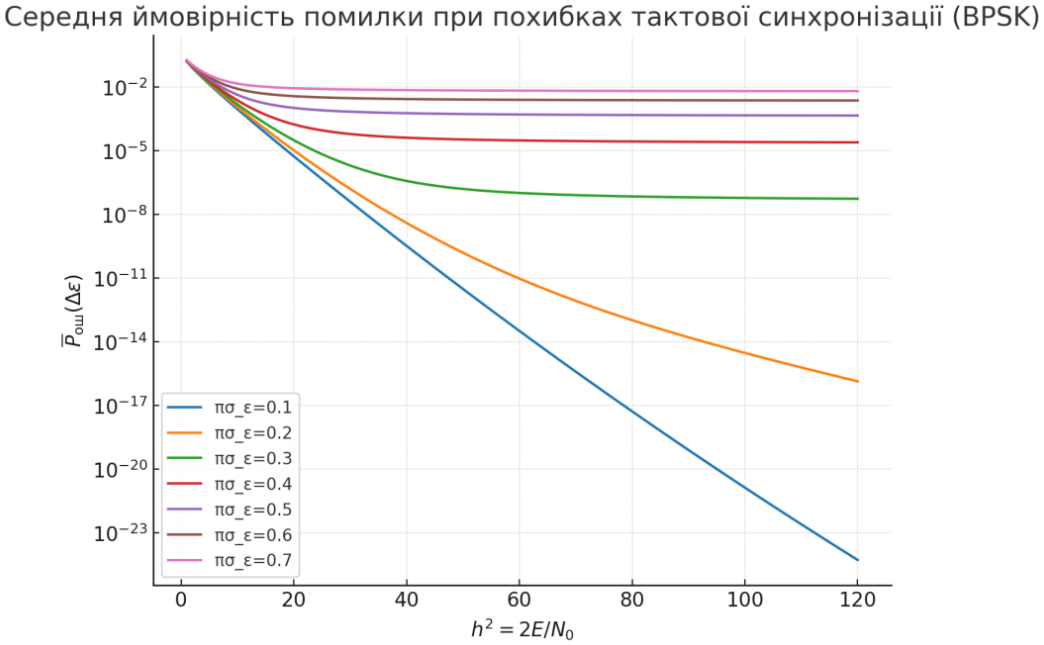


Рис. 2. Залежності ймовірності помилки когерентного прийому протилежних двійкових сигналів за наявності похибок тактової синхронізації

Із отриманих графіків (див. рис. 1 та рис. 2) виходить, що зростання джитера (більші $\pi\sigma_\varphi$ або $\pi\sigma_\varepsilon$) створює помилкову "підлогу": при великому SNR крива перестає спадати експоненційно й виходить на плато тим вище, чим більша дисперсія похибки. Це видно на обох рисунках. Помилкова "підлога" у висновках означає, що навіть при збільшенні SNR нестабільність напруги живлення вносить обмеження → рівень помилок не падає нижче певного значення. Вона виникає через системні похибки, такі як нестабільність генераторів (VCO, гетеродинна), фазові шуми PLL, джитер тактових імпульсів. У випадку синхронізації: навіть при високій потужності сигналу нестабільність напруги живлення викликає фазові коливання, і крива BER (bit error rate) «застигає» на певному рівні.

Плато — це ефект, коли система синхронізації, внаслідок фазових шумів від живлення, «застигає» на ділянці зі сталою ймовірністю помилки, і подальше збільшення потужності сигналу чи фільтрації не покращує результат.

Цікаво порівняти ступінь впливу на завадостійкість помилок фазової та тактової синхронізації при заданому відношенні сигналу в каналі. Для цього припустимо, що тактова частота формується з опорної, рівної частоті несучої, шляхом поділу на k_d (k_d — коефіцієнт ділення частоти). Тоді флуктуації фази тактової частоти будуть меншими за флуктуації фази опорної частоти в k_d. разів. При цього випливає, що в режимі стеження, коли неоднозначність відліку фази тактової частоти усунена, на завадостійкість будуть впливати помилки пристрою фазової синхронізації. Це твердження справедливе і тоді, коли опорна та тактова частоти формуються від різних генераторів.

II. Імітаційна модель оцінки впливу фазових шумів на параметри роботи систем синхронізації мереж когнітивного радіо на фоні нестабільності напруги живлення опорних генераторів

Для проведення подальших досліджень була розроблена імітаційна модель, параметри якої наведено нижче.

Опис моделі

За основу була взята лінійна модель фазової петлі (PLL) з ПІ-фільтром (пропорційно-інтегральний фільтр).

ПІ-фільтр у PLL — це коригуюча ланка, яка забезпечує швидку реакцію на зміну фази (P) і ліквідує сталу похибку (I), формуючи оптимальний баланс між швидкодією та точністю.

Фільтр у фазовій автопідлаштованій системі знаходиться між фазовим детектором і VCO. Його задача:

сформувати таку напругу керування для VCO, щоб система була стійкою і точно відслідковувала вхідний сигнал;

зменшити вплив шумів і збурень.

ПІ-фільтр — це комбінація двох дій:

P – пропорційна дія, коли вихід прямо пропорційний вхідному сигналу;

I – інтегральна дія, яка накопичує помилку у часі, щоб усунути сталу похибку.

Пропорційна частина P швидко реагує на зміни фази, що робить систему швидшою.

Інтегральна частина I накопичує навіть маленькі відхилення фази у часі, щоб усунути постійну фазову похибку (PLL стає «точним»). Разом із тим, інтегральна дія робить систему чутливішою до шумів, тому вибір T_i важливий для компромісу між точністю та стійкістю.

Передавальна функція визначається наступним виразом:

$$F(s) = K_f\left(1 + \frac{1}{sT_i}\right) \quad з \ K_f=1, T_i = 0.01\ c,$$

де K_f — коефіцієнт підсилення ПІ-фільтра у каналі керування. Він масштабує вихід напруги з фільтра перед подачею на VCO. Фізично K_f визначає швидкість реакції PLL на фазові похибки: чим більше K_f, тим швидше PLL реагує, але тим сильніше чутлива до шумів;

T_i — інтегральний час у ПІ-фільтрі у частотній області, який визначає «силу» інтегрування;

T_i — визначає швидкість інтегратора:

малий $T_i \rightarrow$ швидке усунення сталої помилки, але більша чутливість до шумів;

великий $T_i \rightarrow$ повільніше усунення помилки, але краща стійкість.

Його характеристики АЧХ та ФЧХ наведені на рисунках 3 та 4.

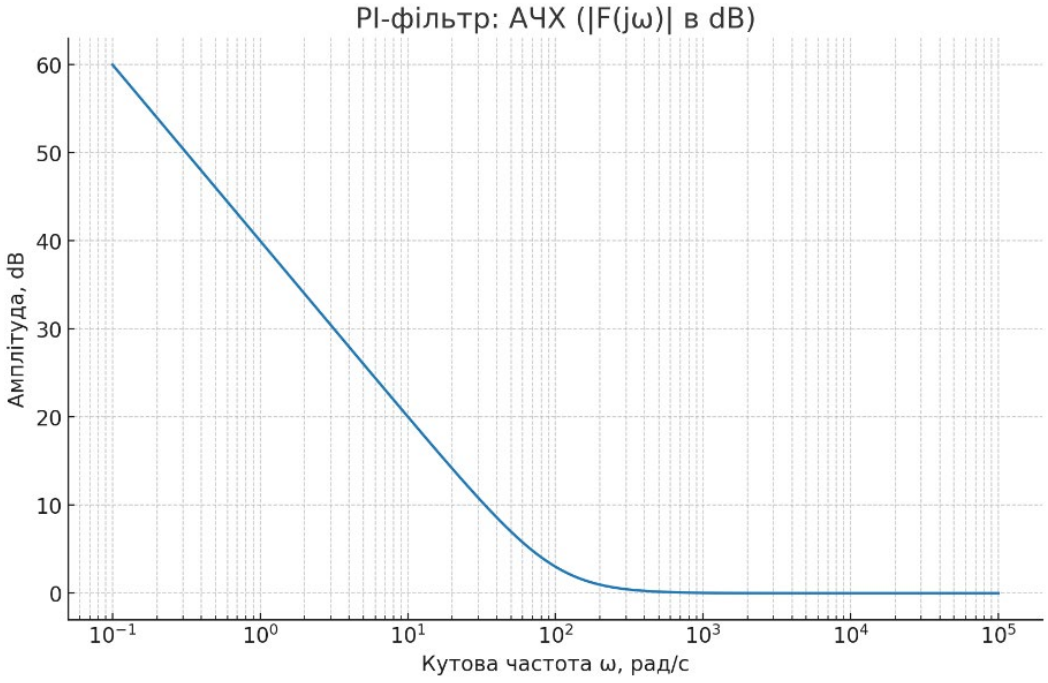


Рис. 3. АЧХ (|$F(j\omega)$ | у dB) ПІ-фільтра

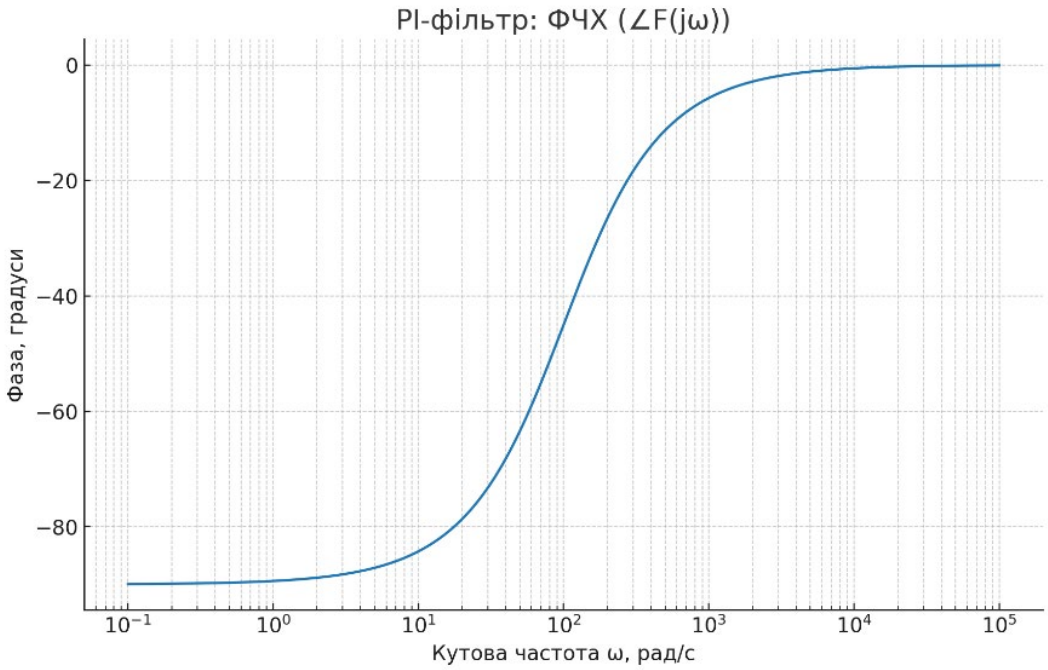


Рис. 4. ФЧХ (∠*F*(*jω*)) ПІ-фільтра

Фазова помилка від шуму живлення. Це передавальна функція від збурення (нестабільності напруги живлення) до фазової помилки PLL. Вона показує, наскільки шум живлення впливає на фазову помилку на виході PLL, та визначається:

$$F_e(j\omega) = \frac{K_{vs}}{j\omega\,(1+L\,(j\omega))},\ L(j\omega) = \frac{K_d K_{vco} F(j\omega)}{j\omega},$$

де $K_d = \frac{1\text{рад}}{\text{В}}$ — чутливість фазового детектора;

$K_{vso} = 2\pi * \frac{10^6 \frac{\text{рад}}{\text{с}}}{\text{В}}$ — чутливість VCO;

$K_{vs} = 2\pi * \frac{10^5 \frac{\text{рад}}{\text{с}}}{\text{В}}$ — *вплив нестабільності напруги живлення на частоту VCO.*

Спектральна щільність фазової помилки:

$$S_\phi(\omega) = |F_e(j\omega)|^2 S_v.$$

Шум живлення прийнято як білий зі спектральною щільністю $S_v = 1 * 10^{-6\,V^2}/Hz$.

Амплітудна щільність (фазовий шум):

$$S\varphi\ (f) = \sqrt{S_\phi(\omega)}\,.$$

Результати моделювання

На рисунку 5 показано спектр фазової помилки від шуму живлення.

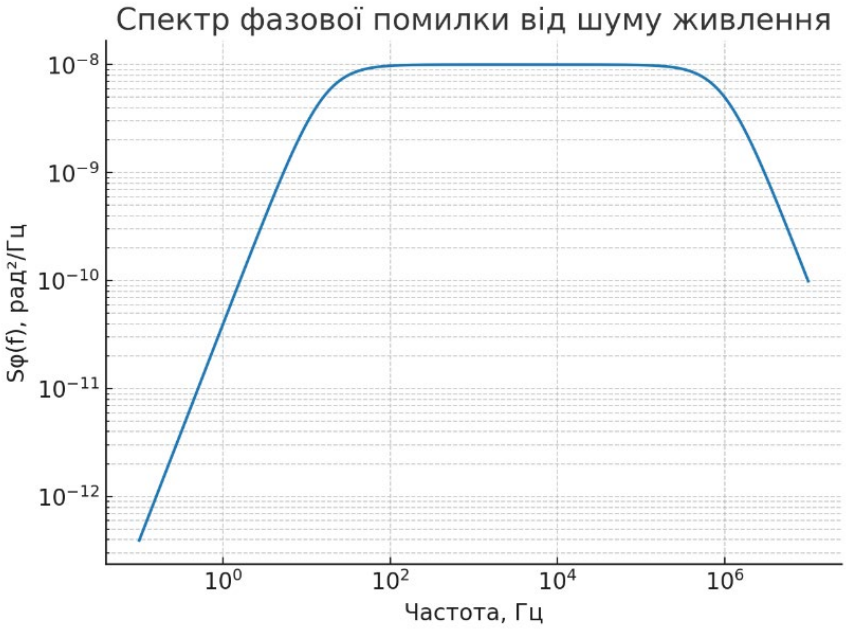


Рис. 5. Спектр фазової помилки від шуму живлення

Як випливає із графіків, на низьких частотах спектральна щільність фазової помилки майже стала. Це пояснюється тим, що при дуже низьких частотах збурення в основному проходить на вихід PLL без значного придушення, бо фільтр та контур ще не створюють суттєвої корекції.

На середніх частотах — в області частот, близьких до смуги пропускання петлі (~десятки-сотні кГц для наших параметрів), починається спад $S\varphi(f)$. Це обумовлено роботою петлі PLL, яка пригнічує низькочастотні збурення завдяки зворотному зв’язку.

На високих частотах — при частотах значно вищих за смугу пропускання PLL (вище ~1 МГц) спектральна щільність знову вирівнюється і навіть зростає, бо петля вже не може компенсувати швидкі зміни. Тут фаза VCO безпосередньо повторює миттєві зміни частоти від шуму живлення.

У цілому, смуга придушення шуму живлення обмежена пропускною здатністю PLL. Чим ширша смуга — тим ефективніше зниження низькочастотної складової фазової помилки.

На рисунку 6 показано передаточну функцію від шуму живлення до фазової помилки.

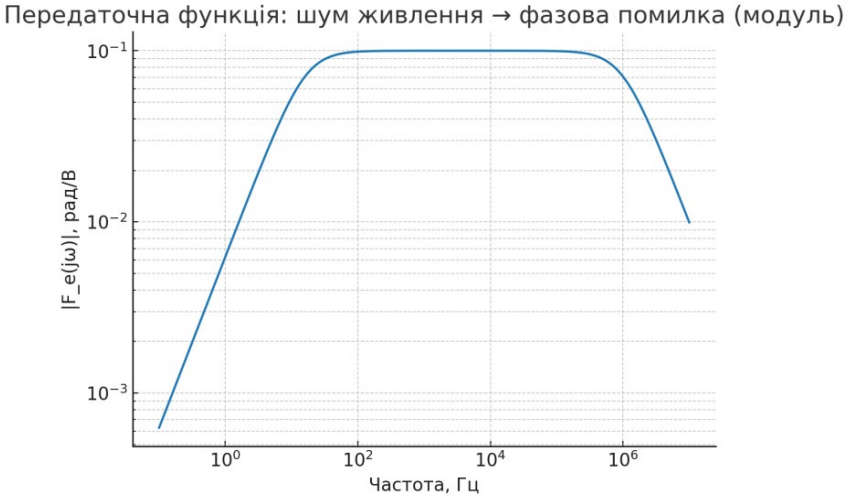


Рис. 6. Передаточна функція від шуму живлення до фазової помилки

Передаточна функція показує, що основний захист від шуму живлення відбувається лише в межах смуги пропускання петлі PLL. За її межами збурення проходять практично без ослаблення.

На дуже низьких частотах значення $|Fe|$ велике, бо зворотний зв’язок не встигає коригувати фазу VCO — майже весь вплив нестабільності живлення передається на фазу вихідного сигналу.

У смузі регулювання PLL видно спад характеристики приблизно з нахилом −20 дБ/дек (для нашої ПІ-петлі). Тут шум живлення ефективно пригнічується.

На високих частотах (вище частоти зрізу) передаточна функція знову наближається до передатної VCO без регулювання, бо зворотний зв’язок не працює.

Далі наведемо інтегральну (RMS) фазову помилку на заданій смузі частот, яка дає кількісну оцінку якості придушення.

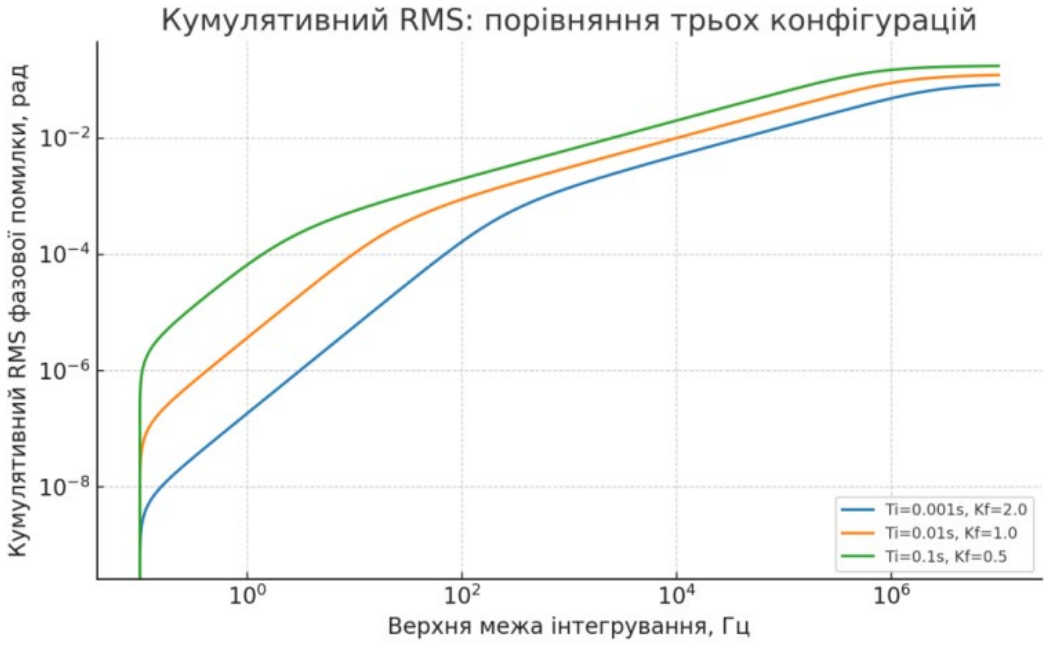


Рис. 7. Кумулятивний RMS: порівняння трьох конфігурацій

На рисунку 7 додано графік кумулятивного RMS від верхньої межі інтегрування, який показує, на яких частотах накопичується основна помилка:

загальний RMS фазової помилки: 0.1213 рад ≈ 6.95°;

загальна дисперсія: 1.4711×10^{-2} рад².

Дані рисунка 7 показують, що в діапазоні ≤ десятки Гц крива зростає дуже повільно і вклад низьких частот мінімальний. Це наслідок зворотного зв’язку PLL та інтегрувальної природи. На середніх частотах (кГц…сотні кГц) крива зростає — у цій області майже пласке. На високих частотах (≈ МГц і вище) крива продовжує зростати та добирає велику частку загального RMS, бо за межами смуги регулювання петля вже не пригнічує збурення, і фаза VCO повторює зміну частоти від шуму живлення. На графіку кумулятивного RMS видно (див. рис. 7): конфігурація з високим K_f та малим T_i дає найменший накопичений RMS у всьому діапазоні (синя крива нижня). Конфігурація з великим T_i і малим K_f (зелена крива) — найгірша.

На рисунку 8 показані результати моделювання $|Fe|$ порівняння для різних T_i, K_f.

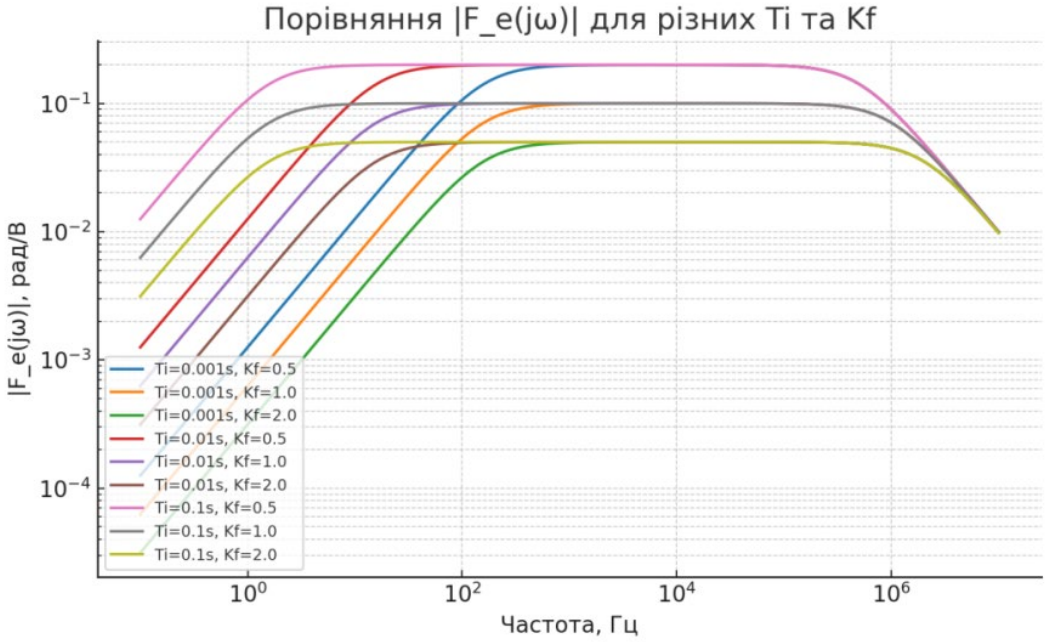


Рис. 8. Результати моделювання $|Fe|$ порівняння для різних T_i, K_f

Збільшення K_f (підсилення фільтра) зменшує $|Fe|$ у смузі регулювання (видимий зсув кривої вниз/вліво) і, відповідно, знижує вклад шуму живлення у фазу — це призводить до зменшення RMS.

Зменшення T_i (швидший інтегральний термін) також підвищує швидкодію петлі на низьких частотах, зменшуючи вплив низькочастотного шуму. Однак занадто мале T_i може вплинути на стійкість (ця модель — лінійна, тому частотна оцінка, стабільність потребує додаткового аналізу запасу по фазі).

III. Методика оцінки впливу точності стабілізаторів напруги на фазову стабільність системи синхронізації

Проведений вище аналіз дозволив сконцентрувати увагу на задачах, пов'язаних із нестабільністю напруги живлення, яка впливає на фазову стабільність системи синхронізації, а, отже, на якість демодуляції, стійкість до завад і загальну надійність приймальних пристроїв.

Для цього спочатку були класифіковані основні фактори, які пов'язані з впливом нестабільності напруги живлення на якість роботи систем синхронізації телекомунікаційних мереж.

Класифікація основних факторів, які пов'язані з впливом нестабільності напруги живлення

1. Зростання фазового шуму та джитера

Нестабільність живлення викликає коливання частоти VCO, що проявляється у вигляді фазового шуму та джитера. Це безпосередньо погіршує часову точність відліків сигналу та знижує коректність синхронізації.

2. Погіршення відношення сигнал/шум (SNR)

Додаткові флуктуації у фазі перетворюються в еквівалентний шум. Це знижує ефективне SNR на вході демодулятора і призводить до зростання похибок відновлення сигналу.

3. Зростання ймовірності бітових помилок (BER)

Для систем із цифровою модуляцією (QPSK, QAM) навіть невеликі фазові відхилення через нестабільність живлення призводять до збільшення BER, особливо при високих порядках модуляції.

4. Втрата ортогональності в OFDM-системах

У багатонесучих системах (LTE, Wi-Fi, 5G NR) фазова нестабільність спричиняє інтерференцію між піднесучими (ICI), що погіршує пропускну здатність і збільшує необхідність у складних алгоритмах компенсації.

5. Зниження точності оцінки частоти та фази

У системах із когерентним прийомом нестабільність живлення ускладнює оцінку несучої частоти та фази, що призводить до зсувів у фазових діаграмах сигналу (IQ-площина).

6. Вплив на синхронізацію в часі

Джитер, спричинений шумом живлення, може призвести до помилок при визначенні моменту початку символів, що особливо критично для систем із щільним мультиплексуванням.

7. Підвищене енергоспоживання компенсуючих алгоритмів

Для компенсації нестабільності напруги необхідно використовувати додаткові фільтри, коректори частоти або цифрові PLL-алгоритми, що збільшує складність і енергоспоживання приймального пристрою.

На цей час розроблено багато методів та інженерних рішень по проблематиці щодо зниження впливу шумів. Незважаючи на значний прогрес у моделюванні та інженерних рішеннях, мало уваги приділено розробці методів підвищення точності роботи стабілізаторів напруги для систем синхронізації в радіотехнічних пристроях і засобах телекомунікації. Тому важливою є розробка методики оцінки впливу точності стабілізаторів напруги на фазову стабільність системи синхронізації.

Методика та алгоритм оцінки впливу точності стабілізаторів напруги на фазову стабільність системи синхронізації

Як відомо, нестабільність живлення напруги впливає на фазову стабільність системи синхронізації, а, отже, на якість демодуляції, стійкість до завад і загальну надійність приймальних пристроїв. Нижче наведена методика, яка дозволяє кількісно оцінити вплив стабілізаторів напруги на роботу системи синхронізації.

Етап 1. Вихідні дані та постановка задачі

Вхідний параметр — нестабільність напруги живлення:

$$\Delta U = (U - U_{ном}) / U_{ном},$$

де U — миттєве значення напруги живлення;

$U_{ном}$ — номінальне значення.

Відомо, що нестабільність живлення впливає на:

роботу гетеродинів і генераторів (VCO);

фазову помилку в PLL;

спектр фазових шумів.

Етап 2. Модель перетворення нестабільності живлення у фазову нестабільність

Для генератора з керуванням напругою (VCO):

$$\Delta f = K_v * \Delta U,$$

де K_v — коефіцієнт чутливості VCO [Гц/В].

Фазова похибка за час t:

$$\varphi(t) = 2\pi \int_0^t \Delta f(\tau)\, d\tau.$$

Фазова дисперсія:

$$\sigma^2_\varphi \approx (2\pi K_v \cdot \Delta U \cdot T)^2,$$

де T — характерний час інтеграції в PLL.

Етап 3. Критерії оцінки впливу

1. Ймовірність помилки фазової синхронізації:

$$P_{slip} \approx \exp(-\Delta\omega_{hold} / \sigma_\varphi),$$

де $\Delta\omega_{hold}$ — смуга утримування PLL.

2. Вплив на якість демодуляції (BER) для когерентного прийому:

$$\text{BER} \approx Q(\ \text{sqrt}(2 * E_b/N_0 * \cos^2(\sigma_\varphi))),$$

де σ_φ — середньоквадратична фазова помилка.

3. Стійкість до завад:

$$(S/N)_{eff} = S / (N + N_\varphi),$$

де N_φ — еквівалентна шумова потужність, внесена фазовими флуктуаціями.

Етап 4. Алгоритм оцінки:

Крок 1. Задати номінальну напругу $U_{\text{ном}}$ та діапазон відхилень ΔU.

Крок 2. Визначити параметри генератора: K_v, смугу утримання PLL ($\Delta\omega_{hold}$), час інтеграції T.

Крок 3. Обчислити σ_φ для кожного рівня нестабільності живлення.

Крок 4. Побудувати залежності: $\sigma_\varphi(\Delta U)$, $P_{slip}(\Delta U)$, BER(ΔU).

Крок 5. Визначити допустимий рівень нестабільності напруги $\Delta U_{\text{доп}}$, при якому $\sigma_\varphi < \sigma_{\varphi\max}$.

Етап 5. Результат методики

Вихід: гранична точність роботи стабілізатора напруги, що забезпечує потрібний рівень фазової стабільності.

Формально:

$$\Delta U_{\text{доп}} \le \sigma_{\varphi\max} / (2\pi * K_v * T).$$

Отже, дана методика дозволяє кількісно оцінити вплив стабілізатора напруги на фазову стабільність системи синхронізації через розрахунок фазової похибки, ймовірності зриву синхронізації, BER та ефективного SNR.

Імітаційна модель реалізації методики оцінки впливу точності стабілізаторів напруги на фазову стабільність системи синхронізації

Графічна інтерпретація цієї методики (залежності $\sigma_\varphi(\Delta U$ та BER(ΔU)) у вигляді MATLAB-моделі (див. скрипт 1) шляхом моделювання представлена на рисунках 8–12.

Скрипт 1 (головний фрагмент). Вплив нестабільності живлення на фазову стабільність

```
%% MATLAB: Power-supply stability → phase stability in PLL
% Extended version: adds bandwidth and Kv sweeps, plus 3D BER surface
% How to run: save as `pll_power_stability_extended.m`, then run.

clear; clc; close all;

%% ------------------------- Console summary -----------------------------
fprintf('--- Summary ---\n');
for b = 1:numel(Bn_set)
   for k = 1:numel(Kv_set)
      T  = 1/(2*pi*Bn_set(b));
      sigma_phi_max = deg2rad(sigma_phi_max_deg);
      DeltaU_allow  = sigma_phi_max/(2*pi*Kv_set(k)*T);
      fprintf('Bn=%d Hz, Kv=%.0f Hz/V ⇒ ΔU_allow ≈ %.3f%%\n', ...
         Bn_set(b), Kv_set(k), 100*DeltaU_allow);
   end
```

Рисунок 8 показує лінійне зростання фазової похибки від нестабільності живлення і межу допустимого відхилення.

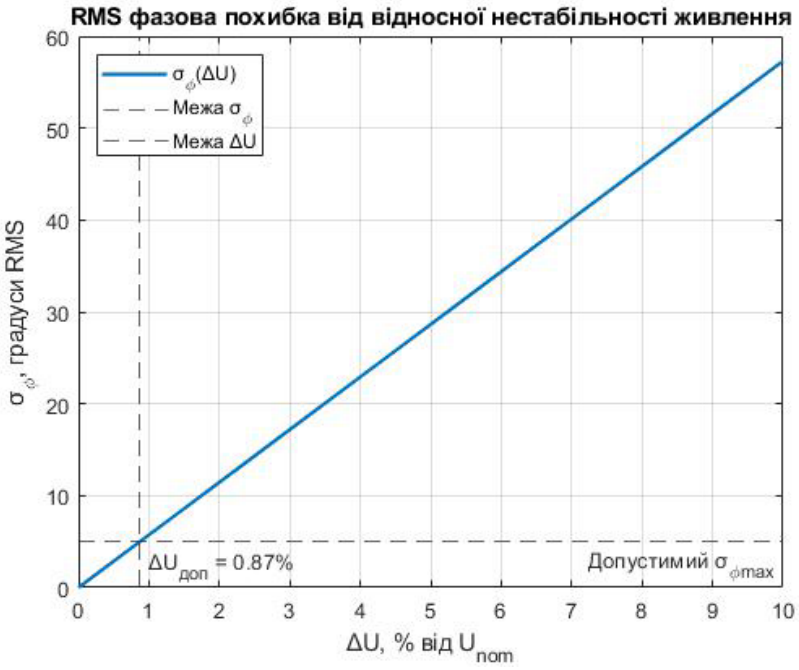


Рис. 8. Графік $\sigma_\varphi(\Delta U)$ з лініями допусків $\sigma_{\varphi,max}(\Delta U)$ *і* ΔU

Рисунок 9 показує вплив ΔU на BER при різних Eb/N_0, де більш шумні системи виявляють вищу чутливість.

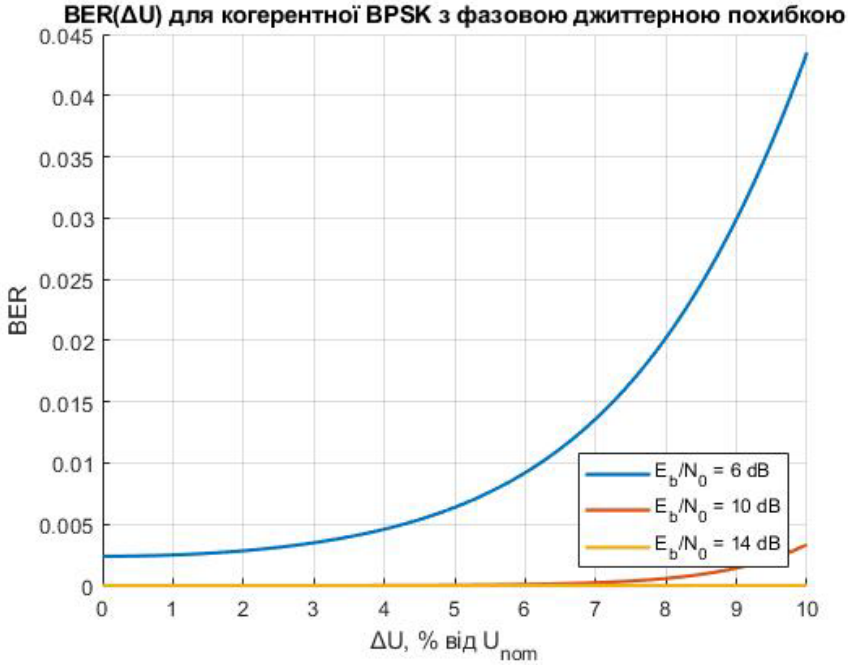


Рис. 9. Сімейство кривих BER (ΔU) кількох Eb/N_0

На рисунках 10–12 показано вплив ширини смуги PLL на фазову похибку (рис. 10), вплив Kv на фазову похибку (рис. 11), 3D-поверхня BER(ΔU, Eb/N_0) для наочного порівняння (рис. 12).

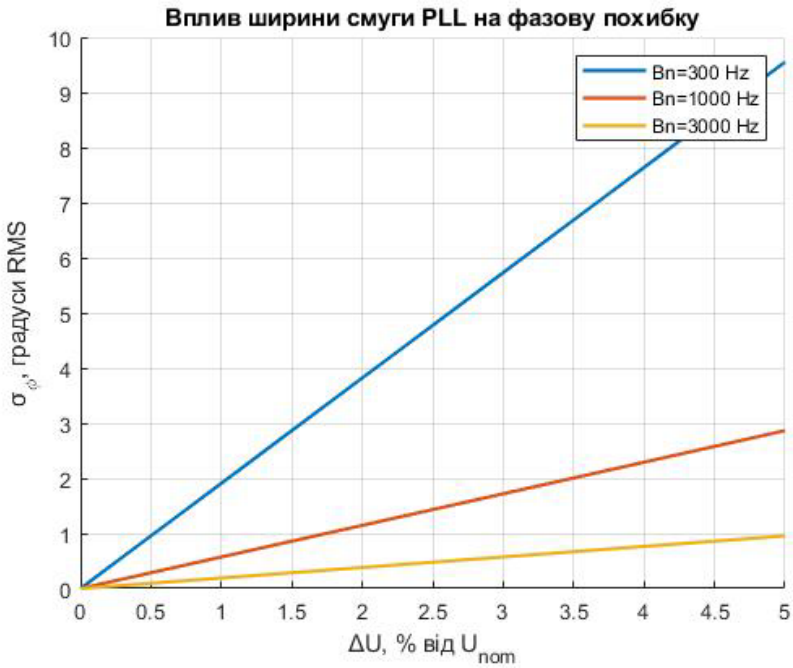


Рис. 10. Вплив ширини смуги PLL на фазову похибку

Графік на рисунку 10 показує, як ширина смуги PLL впливає на чутливість системи до нестабільності живлення. Чим вужча смуга (Bn), тим швидше росте фазова похибка при зростанні ΔU.

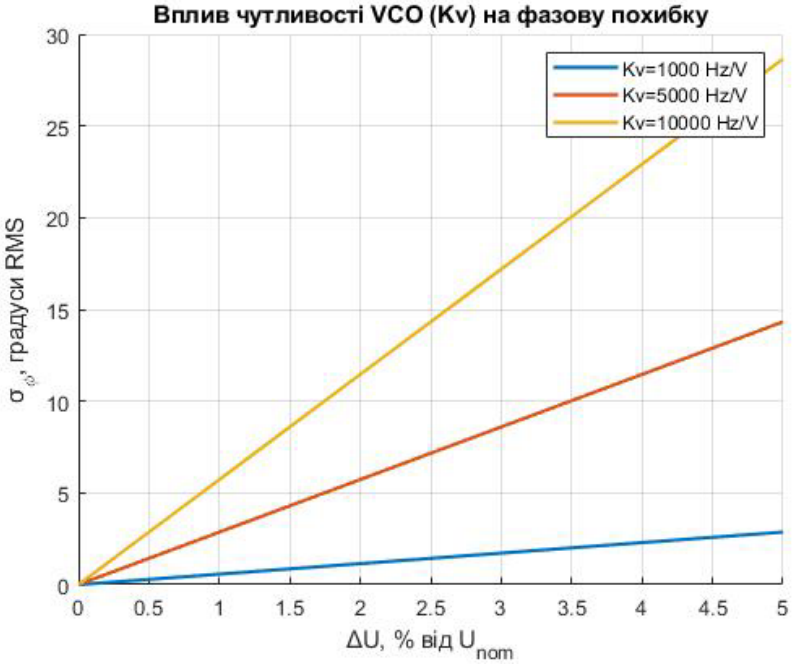


Рис. 11. Вплив *Kv* на фазову похибку

Графік на рисунку 11 демонструє вплив коефіцієнта чутливості VCO (*Kv*). При більшому *Kv* навіть невелика нестабільність живлення спричиняє значну фазову нестабільність.

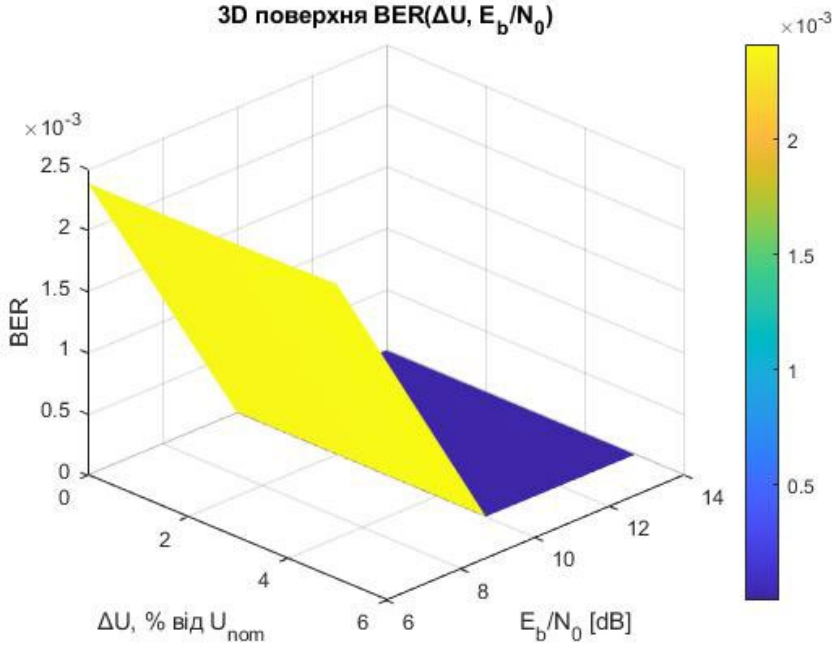


Рис. 12. 3D-поверхня BER(Δ*U*, *Eb*/*N*0) для наочного порівняння

Графік на рисунку 12 (3D) дозволяє оцінити одночасний вплив Δ*U* та *Eb*/*N*0 на BER. Видно, що при високому Eb/N0 система стійка до ΔU, тоді як при низькому *Eb*/*N*0 навіть малі відхилення живлення істотно погіршують BER.

Аналіз результатів моделювання

У процесі проведеного аналізу встановлено, що точність стабілізаторів напруги має безпосередній вплив на фазову стабільність систем синхронізації:

1. Нестабільність напруги живлення призводить до флуктуацій вихідної частоти генераторів (VCO), що викликає зростання фазового шуму та погіршення характеристик синхронізації.

2. Фазова похибка внаслідок нестабільної роботи стабілізаторів формує помилкову "підлогу" в спектрі фазових флуктуацій, що обмежує граничну чутливість приймачів у високоточних системах.

3. При зростанні амплітуди варіацій напруги спостерігається плато у спектрі фазового шуму, що обмежує ефективність фільтрації за допомогою ПІ-регулятора.

4. Використання високоточних стабілізаторів з малими відхиленнями дозволяє істотно знизити фазову похибку, забезпечуючи підвищення стійкості системи та зменшення ймовірності втрати синхронізації.

5. Практичний висновок: для систем синхронізації з високими вимогами до фазової стабільності необхідно застосовувати високоточні стабілізатори напруги з низьким рівнем шуму, мінімізованим температурним дрейфом та покращеною динамікою регулювання.

Таким чином, забезпечення високої точності стабілізації живлення є ключовою умовою досягнення низького рівня фазових флуктуацій і високої якості синхронізації в сучасних телекомунікаційних системах.

Висновки

1. Розширено підхід до аналізу систем синхронізації в когнітивному радіо — вперше одночасно враховано вплив похибок фазової та тактової синхронізації на достовірність прийнятих повідомлень у когерентних приймачах.

2. Розроблено імітаційну модель фазової петлі з ПІ-фільтром, яка дозволяє оцінювати вплив фазових шумів та нестабільності напруги живлення опорних генераторів на параметри синхронізації.

3. Отримано залежності спектральної щільності фазової помилки та передаточної функції від шуму живлення до фазової помилки, що дозволяє кількісно оцінити механізм проникнення нестабільності живлення в частотні характеристики PLL.

4. Запропоновано підхід до оцінки інтегральної (RMS) фазової помилки у заданій смузі частот як узагальненого показника завадостійкості систем синхронізації когнітивного радіо.

5. Проведено чисельне порівняння впливу параметрів ПІ-фільтра (T_i, Kf) на якість роботи PLL та стійкість системи до шумів живлення, що поглиблює методику оптимізації параметрів синхронізаторів.

6. Запропоновано новий підхід до кількісної оцінки впливу нестабільності стабілізаторів живлення на фазову стабільність систем синхронізації.

7. Вперше враховано взаємозв'язок між відносним відхиленням напруги живлення (ΔU), параметрами PLL (ширина смуги захоплення, коефіцієнт чутливості VCO) та показниками якості приймання (σ_φ, BER).

8. Розроблено MATLAB-модель, яка дозволяє проводити віртуальні експерименти та визначати допустимі межі нестабільності живлення з урахуванням конкретних параметрів PLL та VCO.

9. Отримано нові аналітичні залежності, що дозволяють прогнозувати деградацію BER залежно від ΔU та Eb/N_0, що раніше не розглядалося у відомих методиках оцінки.

10. Методика забезпечує науково обґрунтовану основу для оптимізації вимог до стабілізаторів живлення у високоточних приймальних пристроях.

Напрямки подальших наукових досліджень

Подальші наукові дослідження доцільно зосередити на кількох взаємопов'язаних аспектах.

По-перше, перспективним є поглиблений аналіз впливу фазових шумів у багатоканальних когнітивних приймачах, де додаткову роль відіграють взаємні завади між каналами. Це дозволить уточнити вимоги до архітектури синхронізаторів у системах з динамічним розподілом спектра.

По-друге, актуальним є дослідження впливу нестабільності джерел живлення у широкому діапазоні частот та режимів навантаження на характеристики PLL у когнітивних системах. Зокрема, важливо визначити критичні рівні коливань живлення, які призводять до втрати когерентності прийому.

По-третє, необхідною є оптимізація параметрів ПІ-фільтра фазової петлі з використанням багатокритеріальних методів (генетичні алгоритми, алгоритм рою частинок тощо), що дасть змогу забезпечити компроміс між швидкодією та стійкістю системи до внутрішніх шумів і нестабільності живлення.

Подальший розвиток також передбачає моделювання інтегрованого впливу фазових шумів, температурних факторів і коливань напруги живлення, що дозволить створити комплексну модель стійкості синхронізації у реальних умовах експлуатації. Важливим напрямом є дослідження кооперативних когнітивних систем синхронізації, де завдяки розподіленій обробці сигналів можливе часткове компенсування фазових зсувів і похибок тактової синхронізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gardner F. M. Phaselock Techniques. 3rd ed. New York: Wiley, 2005. 428 p.

2. Leeson D. B. A simple model of feedback oscillator noise spectrum // Proc. IEEE. 1966. Vol. 54, No. 2. P. 329–330.

3. Lindsey W. C., Chie C. M. A survey of digital phase-locked loops // Proc. IEEE. 1981. Vol. 69, No. 4. P. 410–431.

4. Best R. E. Phase-Locked Loops: Design, Simulation, and Applications. 6th ed. New York: McGraw-Hill, 2007. 444 p.

5. Razavi B. Design of Analog CMOS Integrated Circuits. New York: McGraw-Hill, 2001. 684 p. (розділи з VCO та фазового шуму).

6. Mitola J., Maguire G. Q. Cognitive radio: making software radios more personal // IEEE Personal Communications. 1999. Vol. 6, No. 4. P. 13–18.

7. Haykin S. Cognitive radio: brain-empowered wireless communications // IEEE Journal on Selected Areas in Communications. 2005. Vol. 23, No. 2. P. 201–220.

8. Bahl I., Bhartia P. Microwave Solid State Circuit Design. 2nd ed. Wiley-Interscience, 2003. 560 p.

9. Mahmoud H. A. et al. Cognitive radios: A survey on software-defined radio and cognitive radio techniques // IEEE Communications Surveys & Tutorials. 2009. Vol. 11, No. 4. P. 2–16.

10. Wu Y., Ling F., Guo Y. Study on the impact of phase noise in cognitive radio synchronization loops // IEEE Transactions on Circuits and Systems I. 2017. Vol. 64, No. 3. P. 745–758.

11. Бойко Ю. М., Єрьоменко О. І. Аналіз моделей систем синхронізації у цифрових приймачах / Матеріали XIV міжнародної науково-практичної конференції. Одеська національна академія зв'язку ім. Попова, 5–10 червня, 2015 р. Одеса. С. 192–194.

12. Бойко Ю. М. Оцінювання якісних показників пристроїв синхронізації сигналів засобів телекомунікацій / Вісник Хмельницького національного університету. 2015. № 1. С. 204–213.

13. Анализ систем синхронизации при наличии помех / Б. И. Шахтарин. М.: Горячая линия – Телеком, 2016. 360 с.

14. Туровський О. Л. Мінімізація дисперсії фазової помилки в системах фазової синхронізації замкнутого типу в режимі стеження за несучою частотою / О. Л. Туровський // Вісник інженерної академії. 2019. № 4. С. 22–27.

15. Turovsky O. Combined system of phase synchronization with increased order of astatism in frequency monitoring mode / O. Turovsky, Y. Khlaponin, H. M. Muhi-Aldin et al. // CEUR Workshop Proceedings. 2020. Vol. 2616, Session. 1. P. 53–62.

16. Turovsky O. L. Estimation of the possibilities of the combined synchronization system with open-link to minimize the dispersion of the phase error when tracking the carrier frequency under the conditions of the influence of additive noise / O. L. Turovsky // Technology audit and production reserves. 2020. Vol. 3, No 4. P. 16–22. DOI: 10.15587/2312-8372.2020.210242.

17. Стеклов В. К., Щербина І. С. Системи фазового автопідстроювання та синхронно-фазові демодулятори. К.: Техніка, 2006. 288 с.

18. Комбіновані системи фазової автопідстроювання / В. К. Стеклов, А. А. Руденко, О. К. Юдін. К.: Техніка, 2004. 328 с.

DOI: 10.58254/viti.8.2025.15.183

УДК 004.32

канд. техн. наук, доцент Симоненко О. А. ORCID: 0000-0001-8511-2017 (ВІТІ ім. Героїв Крут)
Пилипчук І. Ю. ORCID: 0000-0002-5550-8026 (ВІТІ ім. Героїв Крут)
Романенко С. О. ORCID: 0009-0004-0240-0777 (ВІТІ ім. Героїв Крут)
Кондрусь А. В. ORCID: 0000-0001-8815-6517 (ВІТІ ім. Героїв Крут)

АНАЛІЗ МЕТОДІВ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ ТРАНСПОРТНИМИ МЕРЕЖАМИ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ

Зростання попиту на персоналізовані можливості зв'язку спонукає транспортні мережі до еволюції в бік автономного управління, орієнтованого на потреби користувачів. У статті проводиться ґрунтовний аналіз концепції автономності транспортних мереж через впровадження штучного інтелекту, що дозволяє автоматизувати процеси на різних рівнях мережевої інфраструктури. Розглядаються сценарії застосування ШІ у транспортних системах IP-over-DWDM для таких завдань, як прогнозування трафіку, забезпечення високої якості передачі даних, виявлення аномалій, оптимізація мережевих ресурсів, а також проактивне управління відмовами. Особливу увагу приділено ролі штучного інтелекту у вдосконаленні ключових аспектів роботи мереж. Центральною частиною дослідження є запропонована архітектура управління, побудована на відкритих і стандартних API SDN. Вона дозволяє ефективно розподіляти транспортну мережу для багаторівневих систем та забезпечує доступ до нормалізованих даних у реальному часі, що стає основою автономного функціонування. Інтеграція штучного інтелекту сприяє оптимізації використання ресурсів, підвищенню якості послуг, зменшенню простоїв і скороченню операційних витрат, водночас забезпечуючи високу масштабованість мережевої інфраструктури. Використання методів машинного та глибокого навчання дає можливість реалізувати адаптивне управління мережею, враховуючи змінний рівень навантажень і невизначені події. Такий підхід відкриває перспективу створення самокерованих, самовідновлюваних та самонавчальних мереж, здатних адаптуватися до умов без людського втручання. Підсумовуючи, у статті наголошується на тому, що майбутнє транспортних систем тісно пов'язане з повною інтеграцією штучного інтелекту, стандартизованих платформ і відкритих екосистем. Це забезпечує сталий розвиток телекомунікаційної інфраструктури в умовах зростаючих вимог до продуктивності й надійності. Застосування ШІ дозволяє знизити витрати, покращити якість обслуговування та адаптувати мережі до постійного збільшення вимог споживачів.

Ключові слова: *штучний інтелект, автономне управління мережею, транспортні мережі, автоматизація мереж, планування мережі, проактивне управління відмовами, API SDN, IP-over-DWDM.*

O. Symonenko, I. Pylypchuk, S. Romanenko, A. Kondrus. Analysis of methods for automating transport network management using artificial intelligence technology

The growing demand for personalized communication capabilities is driving transport networks to evolve towards autonomous management focused on user needs. The article provides a thorough analysis of the concept of autonomous transport networks through the implementation of artificial intelligence, which allows automating processes at different levels of the network infrastructure. The scenarios for the use of AI in IP-over-DWDM transport systems are considered for tasks such as traffic forecasting, ensuring high data transmission quality, anomaly detection, optimization of network resources, and proactive failure management. Particular attention is paid to the role of artificial intelligence in improving key aspects of network operation. The central part of the study is the proposed management architecture built on open and standard SDN APIs. It allows for efficient distribution of the transport network for multi-tier systems and provides access to normalized data in real time, which becomes the basis for autonomous operation. The integration of artificial intelligence helps optimize resource use, improve service quality, reduce downtime and reduce operating costs, while ensuring high scalability of the network infrastructure. The use of machine and deep learning methods makes it possible to implement adaptive network management, taking into account the changing level of loads and uncertain events. This approach opens up the prospect of creating self-managed, self-healing and self-learning networks that can adapt to conditions without human intervention. In conclusion, the article emphasizes that the future of transport systems is closely related to the full integration of artificial intelligence, standardized platforms and open ecosystems. This ensures the sustainable development of telecommunications infrastructure in the face of growing demands for productivity and reliability. The use of AI allows you to reduce costs, improve the quality of service and adapt networks to the constantly increasing demands of consumers.

Keywords: *artificial intelligence, autonomous network management, transport networks, network automation, network planning, proactive fault management, SDN API, IP-over-DWDM.*

Актуальність та постановка завдання в загальному вигляді

Інтелектуалізація управління мережевими інфраструктурами вже тривалий час виступає стратегічним пріоритетом для телекомунікаційних операторів. Це зумовлено не лише потребою підвищення конкурентоспроможності, а й необхідністю ефективного використання ресурсів та зниження операційних витрат. Водночас глобальна оптимізація мережевого трафіку залишається складним завданням, особливо у випадку масштабних розподілених систем, де традиційні підходи виявляються недостатньо результативними.

До появи концепції програмно-визначених мереж (SDN) телекомунікаційні системи зіткнулися з низкою фундаментальних обмежень. Серед них – висока складність у плануванні та розгортанні, відсутність централізованого управління, обмежена видимість мережевих процесів, низький рівень використання пропускної здатності каналів та значні витрати на технічне обслуговування [1; 2].

Технологія SDN радикально змінила підходи до організації мережевого середовища завдяки розділенню площин керування та пересилання [6; 7]. Централізація управління створила умови для гнучкого планування ресурсів, а відкриті інтерфейси відкрили простір для інновацій у сфері додатків і сервісів [8; 9]. Це дозволяє не лише оперативно реагувати на зміни трафіку, а й адаптивно впроваджувати стратегії управління, підвищуючи загальний рівень інтелектуальності мережевої інфраструктури. У роботах [10–14] показано, що SDN сприяє реконфігурації обладнання та архітектур операторських мереж, вирішуючи проблеми непередбачуваності, нераціонального використання ресурсів і надмірних експлуатаційних витрат.

Особливе значення в даному дослідженні має штучний інтелект (ШІ), який виконує функцію «прогнозиста». На відміну від традиційних рішень, що значною мірою залежать від людського досвіду, ШІ забезпечує точні передбачення, удосконалений аналіз даних та автоматизовану оптимізацію роботи мережі [15; 16].

Функціонал SDN-контролерів дозволяє збирати розширені дані про стан мережі, що створює передумови для застосування ШІ у прогнозуванні трафіку на основі історичних показників та динамічному коригуванні маршрутів залежно від параметрів каналів (пропускна здатність, навантаження, надійність, вартість). Це дає змогу запобігати перевантаженням і гарантувати високий рівень якості обслуговування.

Останні наукові праці демонструють зростаючий інтерес до інтеграції ШІ в алгоритми маршрутизації, включно з використанням нейронних мереж, генетичних алгоритмів (GA) та методів оптимізації роїв частинок (PSO). Однак більшість підходів орієнтується лише на окремі параметри якості обслуговування (QoS), залишаючи поза увагою комплексний розподіл ресурсів та обмеження, притаманні кожному з методів.

Запропоноване в цій статті дослідження розширює раніше представлені напрацювання [3–12], висвітлюючи еволюцію мережевого управління від ручних рішень до повністю автоматизованих архітектур. Запропонована модель передбачає збір нормалізованих даних у режимі реального часу (телеметрія, топологія, інвентаризація, показники продуктивності) та надання уніфікованих інтерфейсів для застосування алгоритмів машинного навчання (ML). Це створює фундамент для реалізації автономних мережевих операцій, що є наступним кроком у розвитку інтелектуальних систем управління.

Аналіз останніх публікацій

У дисертаційній роботі М. І. Бешлея [1] реалізовано спробу системно осмислити трансформацію інфокомунікаційних мереж у напрямі інтенційно-орієнтованих архітектур. Ключова ідея полягає у переході від реактивного до проактивного управління сервісами, де мережа не лише реагує на зміни трафіку, а й передбачає їх. Порівняно з класичними моделями адаптації, підхід Бешлея демонструє вищу ефективність за рахунок прогнозного розподілу ресурсів на основі ШІ. Проте основним викликом залишається складність формалізації

користувальницьких “інтенцій” суб’єктивних вимог до якості сервісу, що ускладнює автоматизацію управління у мультидоменних середовищах.

Дослідження Р. С. Одарченка [2] робить акцент на структурно-функціональній оптимізації стільникових мереж, поєднуючи аналітичне моделювання з методами інтелектуальної оптимізації. Порівняно з підходом Бешлея, робота Одарченка має більш прикладний характер, орієнтована на зменшення енергоспоживання та оптимізацію смуги пропускання. Водночас, запропоновані алгоритми не повністю враховують контекстну мінливість користувальницьких сценаріїв, що обмежує їх гнучкість у середовищі 5G/6G.

Дисертація Т. А. Максимюк [3] розширює попередні підходи, пропонуючи перехід до децентралізованого управління мобільними системами зв’язку. Її внесок полягає у впровадженні когнітивних агентів для самоконфігурації та самонавчання мережі, що підвищує автономність та зменшує залежність від централізованого контролера. Порівняно з Бешлеєм, де ШІ виступає інструментом прогнозу, у Максимюк він стає повноцінним елементом управління. Проте, відкритим залишається питання забезпечення безпеки та узгодження дій автономних вузлів у розподіленому середовищі.

У сучасних дослідженнях [4; 5] спостерігається зсув акцентів від класичного розподілу транспортних ресурсів до концепції software-defined управління, де SDN (Software Defined Networking) виступає ядром адаптивної оркестрації. Аналіз цих праць свідчить, що саме програмно-керовані підходи дозволяють мінімізувати інерційність реакції мережі на зміни трафіку, однак водночас підвищують ризик перевантаження контролерів у великих мультидоменних середовищах. Тому актуальною залишається проблема масштабування SDN-архітектур та їх стійкості до відмов.

Інтеграція штучного інтелекту, як показано у [4–7], розширює функціональні можливості таких систем: нейромережеві моделі забезпечують не лише аналіз, а й предиктивне управління потоками трафіку. Проте аналітичний огляд свідчить про суттєву залежність ефективності цих рішень від якості навчальних даних і контекстної актуальності моделей. У практичних реалізаціях виникає компроміс між точністю прогнозів і обчислювальними витратами, що обмежує впровадження глибоких моделей у реальному часі.

Окремий напрям формують дослідження з генеративного ШІ та великих мовних моделей, які позиціонуються як засіб для автоматизованого створення конфігурацій і сценаріїв управління. Аналітична оцінка цих підходів показує, що хоча велика мовна модель демонструє значний потенціал у прискоренні проєктування мережевих рішень, вони поки що не забезпечують необхідного рівня пояснення, що стримує їх інтеграцію у критичні системи зв’язку.

Підсумовуючи результати аналізу джерел [16; 17], слід відзначити, що розвиток відкритих стандартів (TAPI, Open API, YANG) є передумовою для створення справді інтероперабельних телекомунікаційних екосистем. Водночас, наявні ініціативи переважно зосереджені на технічній сумісності, тоді як питання семантичної узгодженості даних і безпечної взаємодії ШІ-модулів поки залишаються недостатньо опрацьованими.

Аналіз наведених підходів показав, що існуючі рішення орієнтовані переважно на централізоване управління мережею. Разом з тим, проблема адаптації алгоритмів ШІ до децентралізованих транспортних мереж залишається недостатньо дослідженою.

У цій роботі пропонується підхід до підвищення ефективності функціонування транспортних мереж за рахунок впровадження інтелектуальних механізмів самонавчання та прогнозування стану мережі в реальному часі. Запропонований підхід передбачає використання децентралізованої архітектури, у якій вузли мережі здатні самостійно приймати рішення на основі локальних даних і узгоджувати свої дії з іншими елементами через механізми кооперативного навчання. Це дозволяє зменшити затримки при маршрутизації, підвищити стійкість мережі до перевантажень і збоїв, а також забезпечити адаптивне управління ресурсами без необхідності постійного втручання центрального контролера.

Тому виникає **наукове завдання**, яке полягає у розробленні та обґрунтуванні методів покращення автоматизації транспортних мереж шляхом інтеграції технологій штучного інтелекту з SDN, хмарними та крайовими обчисленнями, а також у створенні концептуальних підходів до стандартизації й уніфікації таких рішень для забезпечення інтероперабельності, стійкості та ефективності мережевих систем.

Метою статті є аналіз і вдосконалення методів автоматизації управління транспортними мережами шляхом інтеграції технологій штучного інтелекту, що дозволяє підвищити ефективність, стійкість і адаптивність телекомунікаційних систем до змінних умов експлуатації.

Виклад основного матеріалу. У традиційних мережах управління часто потребує ручного втручання, що займає багато часу і може призвести до помилок. Для усунення цих проблем телекомунікаційна індустрія переходить до автономних мереж, що дозволяє покращити ефективність операцій, підвищити адаптивність і забезпечити швидке реагування на змінені вимоги та мережеві проблеми (рис. 1).

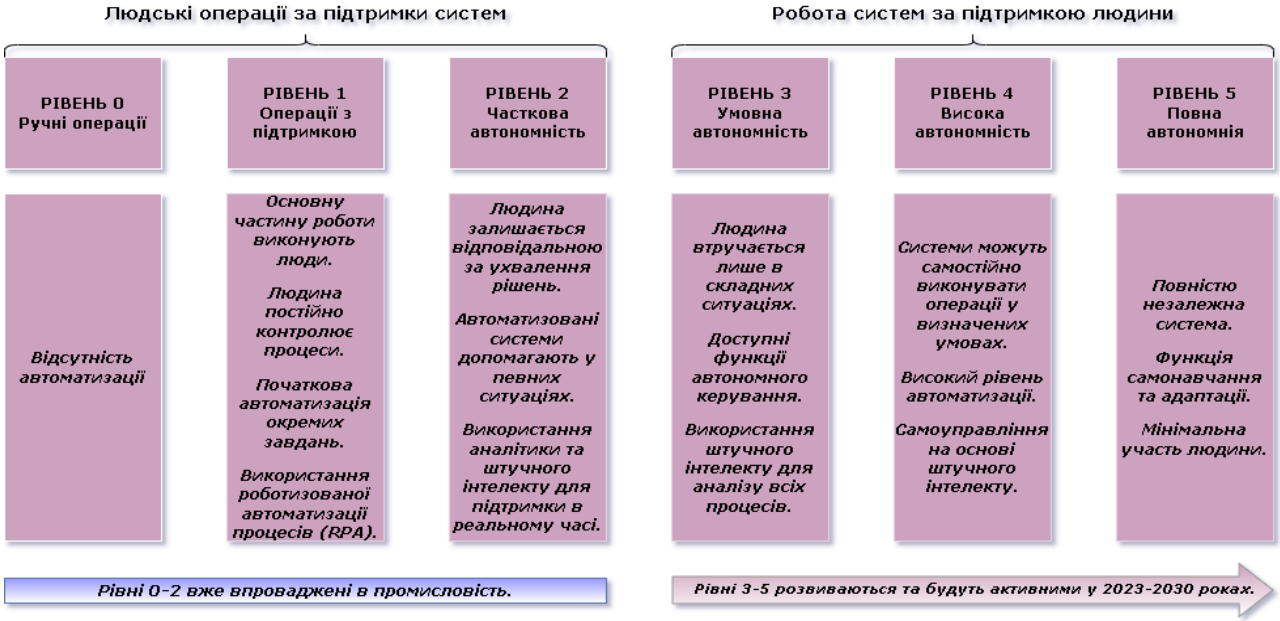


Рис. 1. Еволюція від ручного до повністю автономного управління мережею, що відображає рівні автономності та зростаючу роль автоматизації в роботі мережі

Рівні автономності мережі. Еволюція мережевої автономії розгортається від рівня 0, де всі операції виконуються вручну, а контроль і усунення збоїв цілком покладаються на людину. Хоча цей рівень майже не зустрічається у сучасних інфраструктурах, він наочно демонструє обмеження традиційного підходу – низьку швидкість реагування та відсутність гнучкості.

Рівень 1 позначається впровадженням базової автоматизації для окремих завдань, що зменшує навантаження на операторів, однак ключові рішення все ще залишаються за людиною.

На **рівні 2** автоматизація охоплює ширший спектр процесів. Використання аналітики даних і статичних політик дозволяє впроваджувати системи зворотного зв’язку, які частково коригують роботу мережі в режимі реального часу.

Рівень 3 позначає перехід до умовної автономії. Завдяки штучному інтелекту та розвинутим механізмам аналізу даних мережа здатна самостійно адаптуватися до динамічних умов, що значно знижує потребу у втручанні оператора в стандартних сценаріях.

На **рівні 4** досягається висока автономність: мережі здійснюють аналіз даних у реальному часі, застосовують алгоритми ШІ для вибору оптимальних рішень і можуть оперативно реагувати на складніші зміни без залучення людини.

Рівень 5 характеризується повною автономності, коли мережа не лише самокерується, а й здатна до самонавчання на основі накопичених даних.

Використання та управління даними. Автономні мережі функціонують у середовищі, де постійно генеруються величезні масиви різнорідних даних: від показників продуктивності та журналів активності до історичних шаблонів використання ресурсів.

Поєднання SDN з методами штучного інтелекту та автономними рішеннями формує підґрунтя для створення інтелектуальних і саморегульованих мереж нового покоління. Вони не лише автоматизують рутинні операції, але й забезпечують адаптивність, прогнозування потреб користувачів та оптимізацію розподілу ресурсів у реальному часі, що є ключовим для розгортання сервісів 6G, IoT та масштабних хмарних обчислень.

Крім того, інтеграція машинного та глибинного навчання дозволяє мережам своєчасно виявляти аномалії, прогнозувати перевантаження та автоматично коригувати маршрути передачі даних, зменшуючи ризик відмов і підвищуючи якість обслуговування. Використання генеративного ШІ відкриває нові можливості для автоматичного створення конфігурацій мереж, симуляції сценаріїв навантажень та оптимізації процедур самовідновлення.

До основних компонентів архітектурної моделі SDN (рис. 2) належать: SDN-контролер, що виступає логічним ядром управління мережею. Він відповідає за централізоване прийняття рішень у сферах маршрутизації, реалізації політик безпеки, балансування навантаження та інших функцій управління. Північні API забезпечують взаємодію контролера з прикладними програмами, а південні API – з мережевим обладнанням.

Рис. 2. Узагальнена структурна модель архітектури SDN

Поєднання SDN і технологій штучного інтелекту дозволяє рівню керування збирати та аналізувати дані, формувати й реалізовувати стратегії, створюючи замкнений цикл інтелектуального управління. Контролер із підтримкою ШІ здатен усунути до 90 % мережевих

збоїв і загроз безпеці. Архітектура інтелектуального управління включає три основні блоки: модуль збору й моніторингу стану мережі, модуль інтелектуального аналізу ШІ та модуль SDN-контролера.

Поєднання SDN і графових методів формує потужний механізм для створення інтелектуальних, гнучких і надійних мереж. Графові моделі дозволяють наочно відображати складні топології, автоматизувати прийняття рішень і знаходити оптимальні рішення в реальному часі. Завдяки цьому SDN перетворюється з технології управління мережею на універсальну платформу для інновацій, що знаходить широке застосування у хмарних обчисленнях, IoT та масштабних системах.

Алгоритми маршрутизації застосовуються для визначення оптимальних шляхів передавання даних у мережах. Жадібний алгоритм ґрунтується на виборі локально оптимальних рішень на кожному етапі обчислень. Хоча такий підхід не завжди гарантує глобально найкращий результат, він дозволяє швидко отримати рішення, яке є наближеним до оптимального. У даному випадку жадібний алгоритм використовується для визначення маршруту з урахуванням таких параметрів, як найкоротший шлях, мінімальна затримка, максимальна пропускна здатність та балансування навантаження.

Класичним прикладом жадібного алгоритму є алгоритм Дейкстри, який обчислює шлях із найменшою вагою між вершинами топологічного графа.

K-найкоротших шляхів. Алгоритм *k*-найкоротших шляхів (KSP) використовується для обчислення *k* оптимальних маршрутів у зваженому графі, що містить вершини та ребра з відповідними вагами. Його робота ґрунтується на класичному алгоритмі Дейкстри, а пошук *k* шляхів реалізується за допомогою методу виключення (рис. 3).

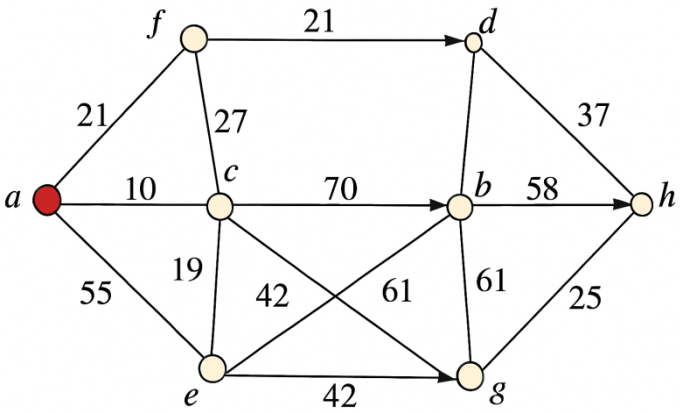


Рис. 3 Алгоритм *k*-найкоротших шляхів

Граф ілюструє задачу пошуку *k*-найкоротших шляхів від вихідної вершини *a* до цільової вершини *h*. Ребра мають позитивні ваги, що дозволяє застосовувати класичний алгоритм Дейкстри для визначення найкоротшого шляху та його модифікації, для знаходження *k* найкоротших альтернативних маршрутів.

Методи машинного навчання знаходять широке застосування у завданнях управління й оптимізації мереж, зокрема для аналізу трафіку, прогнозування навантаження, виявлення аномалій, моделювання структури та діагностики несправностей. Серед ключових підходів до оптимізації маршрутів застосовуються алгоритми рою частинок, генетичні алгоритми, методи моделювання відпалу та інші подібні рішення.

Однією з ключових проблем сучасного управління телекомунікаційними мережами є ефективне узгодження та інтеграція даних, що надходять із великої кількості різнорідних мережевих елементів. Ці дані можуть мати різні форми та структуру: структуровані (метрики

продуктивності, системні повідомлення), напівструктуровані (конфігураційні файли, журнали подій) або повністю неструктуровані (документація, текстові звіти). Саме така різнорідність значно ускладнює процес їхньої обробки, знижує точність і надійність інформації та утруднює встановлення логічних зв’язків між різними джерелами даних.

Особливе значення в автономних мережах має обробка даних у реальному часі та аналіз історичних показників. Такі системи повинні бути здатні швидко аналізувати великі обсяги інформації, оперативно приймати рішення та адаптуватися до змінних умов роботи мережі. Використання сучасних алгоритмів аналізу, а також високопродуктивних обчислювальних ресурсів дозволяє здійснювати обробку даних у момент їхнього надходження, що забезпечує оптимізацію продуктивності та оперативне реагування на потенційні відхилення в роботі мережевих компонентів. Це особливо важливо для підтримки стабільності роботи мережі, забезпечення високої якості обслуговування користувачів та своєчасного попередження можливих збоїв.

Якість та точність вхідних даних безпосередньо визначають ефективність алгоритмів ШІ та ML, які застосовуються в автономних мережах. Водночас, методи оцінки та контролю якості телекомунікаційних даних поки що залишаються недостатньо розробленими, що створює додаткові виклики для розвитку автономних систем [8].

Продемонстровано основну архітектуру SDN та взаємодію між їхніми ключовими компонентами. У центрі системи розташований контролер SDN, який виступає головним координаційним елементом мережі. Контролер здійснює управління мережевими пристроями та забезпечує інтеграцію високорівневих операційних функцій через Northbound API, що дозволяє підключати такі сервіси, як штучний інтелект, системи управління мережею та інструменти оптимізації трафіку (рис. 4).

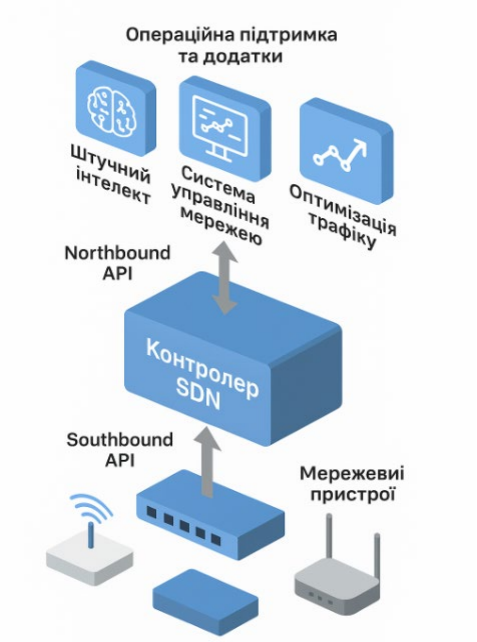


Рис. 4. Взаємодія між трьома основними рівнями системи

З іншого боку, через Southbound API контролер безпосередньо взаємодіє з фізичними та віртуальними мережевими пристроями, такими як маршрутизатори, комутатори та точки доступу. Така структура дозволяє централізовано координувати роботу всіх елементів мережі, автоматизувати управління трафіком та забезпечувати гнучке масштабування інфраструктури.

Дана архітектура демонструє ключові переваги SDN: розділення функцій управління та передачі даних, централізоване адміністрування та можливість інтеграції інтелектуальних

алгоритмів для прогнозування навантаження і оптимізації роботи мережі. Вона ілюструє, як сучасні підходи до програмно-визначувальних мереж підвищують ефективність і надійність телекомунікаційної інфраструктури, одночасно створюючи основу для впровадження автономних і самонавчальних систем управління мережею.

Декларативний підхід до управління мережею представлений у концепції мереж на основі намірів (intent-based networking, IBN), яка зосереджена на визначенні запланованих цілей та результатів, а не на деталях реалізації [16]. Таким чином, генеративний ШІ може бути використаний у мережевих операціях для перетворення високорівневих намірів або цілей, визначених користувачами або операторами мережі, на конкретні робочі процеси і конфігурації, що необхідні для досягнення цих цілей. Моделі генеративного ШІ можуть бути навчання на технічній документації, даних конфігурації мережі та операційних процесах для генерування низькорівневих інструкцій, які забезпечать бажану поведінку мережі [17].

Сучасні концепції штучного інтелекту та їх поступова еволюція від універсальних підходів до спеціалізованих методів відкривають широкі можливості для застосування в різних галузях. На верхньому рівні ієрархії розглядається штучний інтелект як фундаментальна основа побудови систем, здатних відтворювати когнітивні функції людини. Його практична імплементація здійснюється через машинне навчання, що забезпечує алгоритмам здатність виявляти приховані закономірності та формувати прогностичні моделі на основі накопичених даних (рис. 5).

Рис. 5. Ієрархія штучного інтелекту

У сфері SDN-мереж, де управління трафіком і ресурсами виконується централізованим контролером, машинне навчання дає змогу підвищувати ефективність прийняття рішень – наприклад, у задачах маршрутизації чи балансування навантаження. Проте зі зростанням масштабів мережі та ускладненням трафіку традиційні методи машинного навчання виявляються недостатніми.

Ранні дослідження [2; 3] були зосереджені на використанні класичних алгоритмів машинного навчання для аналізу трафіку та виявлення аномалій. Проте зі зростанням

складності та динаміки мережевих середовищ почали впроваджуватися моделі глибинного навчання, які забезпечують автоматичне виділення ознак та обробку великих потоків даних у реальному часі.

Саме тут у гру вступає глибинне навчання, представлене на схемі як підгалузь машинного навчання. Його основою є штучні нейронні мережі, здатні працювати з багатовимірними та динамічними даними. Для SDN це означає можливість створення інтелектуальних систем управління, які не лише реагують на зміни в мережевому середовищі, а й прогнозують їх, забезпечуючи адаптивність, масштабованість та високий рівень якості обслуговування.

Робота штучної нейронної мережі є однією з ключових технологій сучасного штучного інтелекту. Вона складається з трьох основних частин: вхідного шару, прихованих шарів та вихідного шару.

У даній інтерпретації вхідний шар відповідає інфраструктурному рівню, що охоплює мережеві пристрої – комутатори, маршрутизатори, точки доступу. Саме вони формують первинний масив даних, який включає показники трафіку, стан каналів, рівень завантаженості та інші параметри мережі (рис. 6).

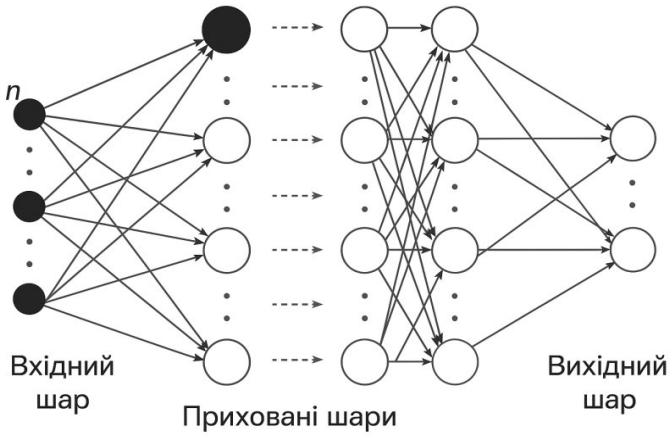


Рис. 6. Схема багатошарової нейронної мережі

Приховані шари в цій аналогії можна співвіднести з логікою SDN-контролера. На цьому етапі здійснюється багаторівневий аналіз отриманої інформації: виявлення закономірностей у потоках даних, прогнозування навантажень, виявлення аномалій, а також моделювання оптимальних сценаріїв маршрутизації. Подібно до нейронної мережі, яка завдяки нелінійним перетворенням виділяє суттєві ознаки, SDN-контролер перетворює «сирі» дані на структуровані рішення для управління мережею.

Вихідний шар формує конкретні команди для мережевих елементів – зміна маршрутизації, балансування навантаження, застосування політик безпеки. Таким чином, реалізується замкнений цикл адаптивного управління, де дані з інфраструктури стають основою для прийняття рішень, а зворотний вплив підвищує ефективність функціонування мережі.

Із інтеграції SDN та методів штучного інтелекту на основі нейронних мереж формується модель інтелектуального керування сучасними телекомунікаційними інфраструктурами.

На верхньому рівні модель представлена у вигляді багатошарової нейронної мережі, де вхідний шар відповідає за прийом телеметрії та конфігураційних даних від SDN-мережі. До таких даних належать статистика потоків, інформація про затримки та втрати пакетів, рівень завантаженості каналів, а також політики безпеки та якості обслуговування. Ці вхідні

параметри формують цифровий зріз стану мережі, що надходить на аналіз до інтелектуального модуля.

Прихований шар виконує роль обчислювального ядра системи. Саме тут відбувається багаторівнева обробка вхідних даних за допомогою методів глибинного навчання. Початкові рівні аналізують сирі статистичні показники, на проміжних етапах формуються закономірності та виявляються відхилення у поведінці трафіку, тоді як на вищих рівнях приймаються стратегічні рішення щодо оптимізації роботи мережі. Таким чином, нейронна мережа здатна виконувати прогнозування завантаження каналів, виявлення аномалій, таких як атаки типу DDoS, а також розробку рішень для динамічного балансування навантаження і перерозподілу ресурсів. Прихований шар у цій архітектурі фактично виступає «мозком», який трансформує потік даних у готові до реалізації керівні дії.

Вихідний шар відображає сформовані рішення у вигляді конкретних інструкцій для SDN-контролера. Це можуть бути нові правила маршрутизації, оновлені списки контролю доступу, зміни у політиках забезпечення якості обслуговування чи активація додаткових віртуальних ресурсів. Кожен вихідний нейрон відповідає певному набору дій, які надсилаються контролером до мережевих пристроїв через southbound-інтерфейси, такі як OpenFlow. У такий спосіб система перетворює результати інтелектуального аналізу на реальні зміни у конфігурації мережі (рис. 7).

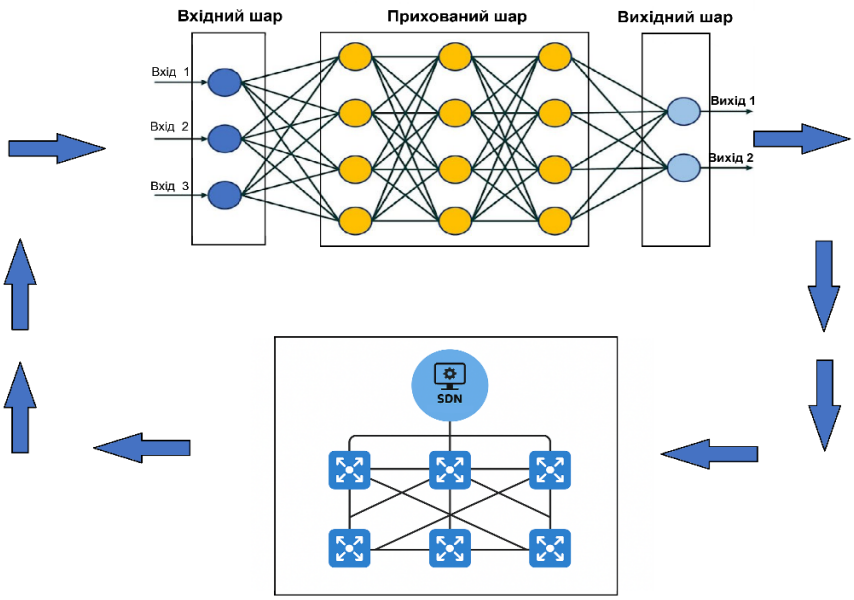


Рис. 7. Схема роботи SDN в поєднанні зі ШІ

Важливим елементом цієї архітектури є зворотний зв'язок. Рішення, що були застосовані до мережі, змінюють її поточний стан, який повторно збирається та надходить на вхід нейронної мережі. Це створює замкнений цикл навчання та оптимізації, у межах якого штучний інтелект постійно вдосконалює свої рішення на основі актуальних даних.

Замкнений цикл інтелектуального управління мережею, що ґрунтується на використанні технологій штучного інтелекту для забезпечення її адаптивності та ефективності. Процес починається з моніторингу параметрів мережі, під час якого здійснюється збір і аналіз поточних даних про стан системи. Отримана інформація використовується для навчання моделей штучного інтелекту, які здатні виявляти закономірності у функціонуванні мережі та формувати прогностичні моделі. На основі цих моделей проводиться прогнозування екзогенних факторів, що можуть впливати на роботу мережі ззовні, таких як зміни

навантаження, трафіку чи зовнішнього середовища. Далі відбувається адаптація ендогенних факторів, спрямована на внутрішнє налаштування параметрів системи відповідно до прогнозованих умов. Завершальним етапом є оновлення параметрів мережі, яке забезпечує актуалізацію її стану та підвищення ефективності функціонування. Таким чином, представлений цикл формує основу інтелектуального управління, що забезпечує безперервне самонавчання, гнучкість і стійкість мережевої інфраструктури до змін середовища (рис. 8).

Рис. 8. Циклічна модель інтелектуального управління

Інтеграція SDN з методами штучного інтелекту забезпечує низку ключових переваг. По-перше, відбувається автоматизація процесів керування мережею, що дозволяє мінімізувати ручну конфігурацію. По-друге, система набуває здатності адаптуватися до динамічних змін трафіку в реальному часі. Крім того, завдяки використанню прогнозних моделей, з’являється можливість передбачати перевантаження та реагувати на них превентивно. Суттєвою є також роль у сфері кібербезпеки, адже виявлення аномалій та підозрілих потоків дозволяє своєчасно блокувати потенційні загрози. Нарешті, застосування такої архітектури сприяє оптимізації розподілу ресурсів, зменшенню затримок і підвищенню якості надання мережевих послуг.

Таким чином, представлена модель може розглядатися як архітектура програмно-визначеної мережі з інтелектуальним модулем оптимізації, у якій нейронна мережа виконує функцію динамічного оркестратора правил і рішень, що забезпечує гнучке, безпечне та ефективне керування складними мережевими інфраструктурами.

Принципи, закладені в архітектурі штучних нейронних мереж, мають концептуальну близькість до механізмів SDN. Обидва підходи передбачають ітеративний аналіз даних, виявлення закономірностей та побудову рішень, спрямованих на підвищення адаптивності й оптимізацію системи.

Сучасні тенденції розвитку транспортних мереж свідчать про поступовий і невідворотний перехід від класичних методів управління мережевою інфраструктурою до рішень, орієнтованих на ШІ. Ця тенденція обумовлена зростаючою складністю мереж, динамічними змінами трафіку та високими вимогами до QoS, пропускної здатності та енергоефективності.

Для оцінки ефективності інтеграції ШІ у транспортні мережі було проведено комплексний порівняльний аналіз між класичними підходами, такими як OSPF, IS-IS та традиційними рішеннями SDN сучасними механізмами ШІ, які застосовують методи машинного навчання, глибинного навчання та підкріплювального навчання.

В таблиці 1 представлено наступне:

1. Затримка передачі пакетів (Latency). Одним із критичних показників ефективності мереж є середня затримка передачі пакетів у умовах динамічного навантаження. Дослідження показують, що у традиційних мережах, з використанням класичних алгоритмів маршрутизації OSPF та IS-IS, середня затримка складає 40–55 мс. Це пояснюється обмеженою адаптивністю цих алгоритмів до швидких змін трафіку.

Натомість застосування методів глибинного підкріплювального навчання ШІ дозволяє мережі прогнозувати зміни навантаження, адаптивно перенаправляти потоки та знижувати середню затримку на 25–40 %, до значень 25–35 мс. Така оптимізація особливо ефективна у мережах із високим ступенем змінності трафіку, наприклад, у дата-центрах та мережах провайдерів мобільного зв'язку;

2. Пропускна здатність та утилізація каналів. У сфері пропускної здатності класичні SDN-рішення забезпечують утилізацію мережевих ресурсів на рівні 70–75 % у пікові години. Це обумовлено статичною або обмежено адаптивною конфігурацією маршрутів та розподілом ресурсів. Інтелектуальні механізми ШІ, здатні прогнозувати зміни трафіку та оптимально розподіляти ресурси, підвищують утилізацію каналів до 85–90 %. Такий підхід дозволяє не лише ефективніше використовувати наявні ресурси, але й зменшувати вузькі місця у мережі, що є критично важливим для забезпечення QoS у великих корпоративних та операторських мережах;

3. Моніторинг та виявлення аномалій. Традиційні системи моніторингу та виявлення аномалій характеризуються точністю близько 80%, що часто супроводжується високим рівнем хибнопозитивних спрацювань. Використання моделей машинного навчання – зокрема нейронних мереж та ансамблевих методів ШІ – дозволяє підвищити точність виявлення до 93–96 %, при цьому зменшуючи кількість хибнопозитивних сигналів приблизно на 30 %. Це забезпечує більш оперативну і точну реакцію на потенційні загрози, а також зменшує навантаження на мережевий персонал;

4. Енергоспоживання. Ефективність енергоспоживання є ще одним критичним фактором у сучасних мережах, особливо в умовах глобального тренду на "зелений" ІТ. Класичні підходи зазвичай використовують ресурси обладнання на рівні 100 %, незалежно від поточного навантаження. ШІ-рішення застосовують динамічне керування компонентами мережевого обладнання – відключення неактивних модулів, оптимальне перемикання портів та адаптивне розподілення потоків. Це дозволяє досягти економії енергії на рівні 15–20 % у транспортних ядрах та дата-центрах без втрати якості обслуговування;

5. Гнучкість управління мережею та автоматизація. Особлива цінність рішень на основі ШІ проявляється у підвищенні гнучкості управління мережею. Традиційні методи маршрутизації та SDN-рішення часто вимагають ручного втручання у випадку зміни трафіку або аварійних ситуацій, що збільшує час реакції з декількох секунд до хвилин. Сучасні моделі ШІ дозволяють автоматизувати до 80 % рутинних операцій, скорочуючи час реакції до секунд, підвищуючи стабільність роботи та знижуючи ризик помилок, пов'язаних із людським фактором.

Таблиця 1

Основні відмінності між автоматизацією транспортних мереж з використанням штучного інтелекту та класичні рішення

Показник	Класичні рішення	Рішення на основі ШІ
Середня затримка пакетів	40–55 мс	25–35 мс (зниження на 25–40 %)
Утилізація пропускної здатності	70–75 % у пікові періоди	85–90 % завдяки прогнозуванню трафіку
Точність виявлення аномалій	~80 %	93–96 %, зменшення хибнопозитивних спрацювань на ~30 %

Показник	Класичні рішення	Рішення на основі ШІ
Енергоспоживання мережевого обладнання	Використання ресурсів на 100 %	Економія 15–20 % завдяки динамічному управлінню компонентами
Автоматизація управління мережею	Ручне втручання при зміні трафіку або аваріях	До 80 % рутинних операцій автоматизовано, час реакції скорочується до секунд
Гнучкість адаптації до змін трафіку	Обмеження, потребує ручного налаштування	Висока, мережа самостійно підлаштовується під зміни

Застосування ШІ в транспортних мережах забезпечує комплексне підвищення ефективності мережевої інфраструктури: зменшення затримки, підвищення пропускної здатності, точніше виявлення аномалій, оптимізацію енергоспоживання та автоматизацію управління. Це відкриває нові перспективи для побудови мереж нового покоління, які здатні адаптуватися до постійно зростаючих вимог користувачів і бізнесу.

З використанням ШІ цей процес значно спрощується. Мережевий оператор описує вимоги до послуги природною мовою. ШІ автоматично аналізує вимоги та перетворює їх на необхідні конфігурації. Контролер SDN автоматично налаштовує мережеві пристрої. ШІ проводить автоматичне тестування та перевірку відповідності вимогам.

Оцінка ефективності автоматизації транспортних мереж базується на декількох ключових показниках, які характеризують продуктивність, економічну доцільність, швидкість впровадження та покращення якості обслуговування. У загальному вигляді формула має наступний вигляд:

$$E_{AUTO} = \frac{K_1 \times \Delta T + K_2 \times \Delta C + K_3 \times \Delta Q + K_4 \times \Delta A}{K_1 + K_2 + K_3 + K_4}, \quad (1)$$

де E_{AUTO} – інтегральна оцінка ефективності автоматизації;

$K1$, $K2$, $K3$, $K4$ – вагові коефіцієнти важливості кожного з факторів, визначені експертним шляхом залежно від пріоритетів (наприклад, для оператора або провайдера),

$\Delta T = \frac{T_{\text{початковий}} - T_{\text{новий}}}{T_{\text{початковий}}}$ – відносне скорочення часу на виконання операцій;

$\Delta C = \frac{C_{\text{початковий}} - C_{\text{новий}}}{C_{\text{початковий}}}$ – економія витрат;

ΔQ – покращення якості обслуговування (QoS, надійність, пропускна здатність тощо);

$$\Delta Q = \frac{\left(\frac{A_2}{A_{\max}} + 1 - \frac{D_2}{D_{\max}} + 1 - \frac{J_2}{J_{\max}} + 1 - \frac{PL_2}{PL_{\max}}\right) - \left(\frac{A_1}{A_{\max}} + 1 - \frac{D_1}{D_{\max}} + 1 - \frac{J_1}{J_{\max}} + 1 - \frac{PL_1}{PL_{\max}}\right)}{\left(\frac{A_1}{A_{\max}} + 1 - \frac{D_1}{D_{\max}} + 1 - \frac{J_1}{J_{\max}} + 1 - \frac{PL_1}{PL_{\max}}\right)} \quad (2)$$

де A – пропускна здатність;

D – затримка;

J – затримка між пакетами;

PL – втрата пакетів;

$T_{\max}$, $D_{\max}$, $J_{\max}$, $PL_{\max}$ – цільові (граничні) значення для нормалізації;

$\Delta A = \frac{A_{\text{початковий}} - A_{\text{новий}}}{A_{\text{початковий}}}$ – покращення адаптивності/гнучкості мережі.

Отримані аналітичні дані базуються на результатах моделювання процесів управління транспортними мережами з використанням архітектури програмно-визначених мереж (SDN) у поєднанні з алгоритмами штучного інтелекту, зокрема методами машинного навчання та інтелектуальної маршрутизації. Для оцінювання впливу ШІ на ключові параметри

продуктивності мережі застосовано імітаційне моделювання у середовищах Mininet та NS-3, що дозволило відтворити типові сценарії навантаження та трафікових змін у динамічному середовищі.

У дослідженні було використано алгоритми прогнозування трафіку на основі рекурентних нейронних мереж та механізми інтелектуального балансування навантаження із застосуванням методів кластеризації. Дані щодо затримки пакетів, пропускної здатності, точності виявлення аномалій та енергоспоживання отримано шляхом багаторазового вимірювання в умовах змінних параметрів мережевої топології та навантаження.

Показники (зменшення затримки з 40–55 мс до 25–35 мс, підвищення пропускної здатності до 85–90 %, зростання точності детекції до 93–96 %, зниження енергоспоживання на 15–20 %) мають узагальнений характер і отримані шляхом нормалізації результатів кількох експериментальних сценаріїв. Для забезпечення достовірності проведено порівняння з базовою конфігурацією без застосування інтелектуальних механізмів управління.

Таким чином, числові результати є наслідком системного аналітично-експериментального підходу, що поєднує моделювання, машинне навчання та статистичну обробку даних, і відображають типові тенденції впливу ШІ на ефективність функціонування транспортних мереж.

Застосування методів штучного інтелекту має відчутний вплив на ключові параметри продуктивності мережі. У частині затримки пакетів штучний інтелект забезпечує зменшення середніх значень із 40–55 мс до 25–35 мс завдяки прогнозуванню змін трафіку та адаптивному маршрутизаційному керуванню. Пропускна здатність каналів зростає з рівня 70–75 % до 85–90 % завдяки інтелектуальному балансуванню навантаження. У сфері моніторингу та виявлення аномалій точність зростає з ~80 % до 92–94 %, при цьому зменшується кількість хибнопозитивних спрацювань. Енергоспоживання знижується на 10–15 % завдяки адаптивному керуванню компонентами обладнання. Нарешті, гнучкість управління мережею підвищується завдяки автоматизації до 80 % рутинних операцій, що скорочує час реакції з хвилин до секунд (рис. 9).

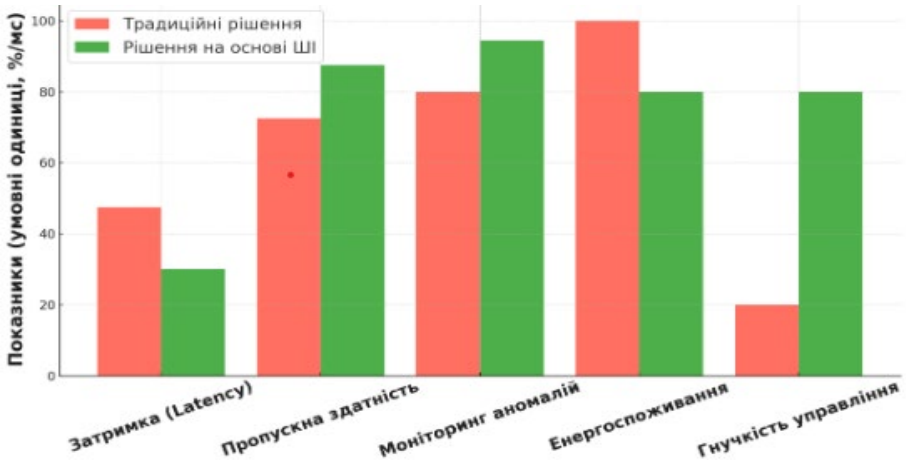


Рис. 9. Порівняння компонент ефективності транспортних мереж з використанням ШІ

Зазначені значення мають орієнтовний характер і залежать від особливостей впровадження, а також від складності мережевої інфраструктури. Важливим чинником є якість даних, на яких навчаються алгоритми ШІ, адже вона безпосередньо впливає на точність отриманих результатів.

Управління на базі ШІ. Автоматизація на основі ШІ дозволяє абстрагуватися від специфікацій, притаманних різним виробникам обладнання, що спрощує процес управління та зосереджує увагу операторів на досягненні стратегічних цілей.

Для виявлення тенденцій і вдосконалення налаштувань мережеві генеративні моделі можуть навчатися на основі операційних журналів, історичних даних та найкращих практик. Це дає змогу підвищити продуктивність, зменшити потребу в ручному управлінні та оптимізувати використання ресурсів.

Висновки

Проведений аналіз підтвердив, що інтеграція технологій штучного інтелекту у процеси автоматизації транспортних мереж забезпечує значне підвищення продуктивності, стійкості та адаптивності сучасних телекомунікаційних систем. Використання інтелектуальних алгоритмів у поєднанні з архітектурою SDN, хмарними та крайовими обчисленнями дозволяє реалізувати динамічне управління ресурсами, прогнозування навантажень і оптимізацію маршрутів передачі даних у реальному часі. Розроблені концептуальні підходи до стандартизації та уніфікації інтеграційних рішень забезпечують інтероперабельність та масштабованість мережевої інфраструктури, що особливо важливо для великих розподілених систем. Отримані результати дозволяють формувати науково-практичну основу для впровадження інтелектуальних систем управління, які здатні адаптуватися до змінних умов експлуатації та мінімізувати вплив людського фактора.

Таким чином, дослідження підтверджує, що інтеграція ШІ у транспортні мережі не лише підвищує їхню продуктивність, а й відкриває можливості для розвитку нових сервісів і автоматизованих рішень, здатних забезпечувати автономне управління та самокорекцію мережевих процесів.

Перспективи подальших досліджень включають впровадження та вдосконалення сценаріїв використання ШІ в реальних умовах, зокрема в контексті архітектури мережевого розгалуження для транспортних мереж IP-over-DWDM. З переходом мереж від ручного управління до повністю автономного, відповідно до рівнів автономії, важливо покращити взаємодію між людиною та ШІ через вдосконалені інтерфейси та системи підтримки прийняття рішень. Оптимізація впровадження технологій ШІ в автономних мережах буде залежати від цих досягнень, і безперервні дослідження мають вирішальне значення для створення інтелектуальних, адаптивних і стійких автономних мережевих рішень. Перспективними напрямками подальших досліджень є розробка методів самонавчання для автономних мереж, інтеграція ШІ із засобами кібербезпеки, оптимізація енергоспоживання в умовах змінного навантаження, а також формування стандартів взаємодії для уніфікації інтелектуальних рішень у телекомунікаційній галузі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бешлей М. І. Синтез та реалізація інтенційно-орієнтованих інфокомунікаційних мереж для адаптивного надання сервісів. Львів, 2021 докторська.

2. Одарченко Р. С. Методологія підвищення ефективності функціонування стільникових мереж. Київ, 2019 докторська.

3. Максимюк Т. А. Інтелектуальне автоматизоване управління децентралізованими системами мобільного зв’язку. Львів, 2021. Heavy Reading. Operator Survey on Open and Automated Transport Networks 2023–2024. Light Reading, 2024. 45 p.

4. Zhang Y., Li H. Machine Learning Approaches for Traffic Prediction and Anomaly Detection in Transport Networks: A Review // IEEE Access. 2024. Vol. 12. P. 87654–87672.

5. De Dios O. G., Armingol-Robles P., Roelens L. et al. AI-based automation of multi-layer multi-domain transport networks // Optical Fiber Communication Conference (OFC). 2024. Paper W4I.2.

6. Tang J., Zhao Z. et al. QoS-Aware Autonomous Network Agents for 6G Using Real-Time Data Analytics // IEEE Wireless Communications. 2021. Vol. 28, No. 5. P. 42–48.

7. Шевченко А. І., Барановський С. В., Білокобильський О. В., Бодянський Є. В., Бомба А. Я. Стратегія розвитку штучного інтелекту в Україні: монографія. Київ: Інститут проблем штучного інтелекту, 2023. 312 с.

8. Єфанова К. О., Пономаренко З. М., Масесов М. О. Актуальність впровадження та використання мережі SDN // Сучасні інформаційні технології.

9. Kumar A., Mehta S. Hybrid Optimization and Machine Learning Methods for Network Automation // Computer Communications. 2023. Vol. 210. P. 45–59.

10. Amin R., Rojas E., Aqdus A. et al. A survey on machine learning techniques for routing optimization in SDN // IEEE Access. 2021. Vol. 9. P. 104582–104611.

11. Симоненко О. А., Троцько О. О., Кушніренко Д. М. Аналіз методів багатошляхової маршрутизації в програмно-конфігурованих телекомунікаційних мережах // Збірник наукових праць ВІТІ. 2019. № 2. С. 95–104.

12. Wu X., Zhang H. et al. Graph Neural Networks for Traffic Optimization in Software-Defined Networks // IEEE Transactions on Network Science and Engineering. 2022. Vol. 9, No. 3. P. 1465–1478.

13. Open ZR+ MSA. Open ZR+ MSA technical specification.

14. Xu X., Hu H., Sun Y. Intelligent Traffic Engineering in SDN Networks Using Machine Learning // Journal of Network and Systems Management. 2019. Vol. 27, No. 3. P. 525–546.

15. Олтрейд Дагоґо. Нове мислення. Від Айнштайна до штучного інтелекту. Наука і технології, що змінили наш світ. Київ: Наш Формат, 2024. 304 с.

16. He P., Liu S., Chen Z. AutoML for Network Anomaly Detection: A Survey // IEEE Communications Surveys & Tutorials. 2022. Vol. 24, No. 2. P. 1015–1045.

17. Tabatabaeimehr F., Velasco L., Ruiz M. et al. Dynamic traffic prediction model retraining for autonomous network operation // 23rd International Conference on Transparent Optical Networks (ICTON). 2023.

18. Natalino C., Panahi A., Mohammadiha N. et al. AI/ML-as-a-service for optical network automation: use cases and challenges [Invited] // J. Opt. Commun. Netw. 2024. Vol. 16. P. A169–A179.

19. Chen H., Miao Y., Chen L. et al. Software-defined network assimilation: bridging the last mile towards centralized network configuration management with NAssim // Proceedings of the ACM SIGCOMM 2022 Conference. 2022. P. 281–297.

DOI: 10.58254/viti.8.2025.16.199

УДК 629.735; 004.9

Соловйова Т. В. ORCID: 0009-0009-8338-8410 (ВІТІ ім. Героїв Крут)
Абрабаєв М. А. ORCID: 0009-0006-9306-547X (ВІТІ ім. Героїв Крут)
Куйбіда Н. С. ORCID: 0009-0005-6305-3622 (ВІТІ ім. Героїв Крут)
Ломакін Є. В. ORCID: 0009-0002-6565-1341 (ВІТІ ім. Героїв Крут)
Костюк Б. М. ORCID: 0009-0002-1650-8610 (ВІТІ ім. Героїв Крут)
Масич В. В. ORCID: 0009-0000-0625-1597 (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ КВАНТОВИХ ТЕХНОЛОГІЙ ДЛЯ ПОКРАЩЕННЯ ПРОЦЕСУ УПРАВЛІННЯ БПЛА

У статті розглянуто перспективи інтеграції квантових технологій у безпілотні літальні апарати (БпЛА). Проведено дослідження квантових технологій при розробці новітніх безпілотних літальних апаратів.

Основна увага приділена квантовим сенсорам для навігації, алгоритмам квантової оптимізації для автономного управління та квантовому розподілу ключів (QKD) для захищеного зв'язку. Запропоновано концепцію умовної архітектури квантового БпЛА, що поєднує сенсорні модулі на основі квантової механіки з класичними системами керування та штучного інтелекту.

Використано порівняльний аналіз класичних і квантових сенсорів, огляд алгоритмів оптимізації (QAOA, VQE), а також принципів QKD. Розглянуто результати лабораторних і польових випробувань, а також досвід міжнародних компаній і стартапів.

Показано, що квантові інерціальні сенсори забезпечують навігацію без дрейфу, навіть у «GPS-denied» середовищах. QKD гарантує захищеність каналів зв'язку, а квантові алгоритми оптимізації дозволяють ефективно вирішувати задачі маршрутизації та управління роєм у реальному часі.

Ключові слова: *квантовий сенсор, квантова навігація, квантовий розподіл ключів (КРК, QKD), квантові технології, атомний годинник CSAC, квантовий акселерометр, квантовий гіроскоп, SWaP-суперпозиція.*

T. Soloviova, M. Abrabaiev, N. Kuibida, E. Lomakin, B. Kostiuk, V. Masych. Research on the possibilities of applying quantumtechnologies to improve the UAV management process

The article examines the prospects of integrating quantum technologies into unmanned aerial vehicles (UAVs). Research on quantum technologies has been conducted in the development of new unmanned aircraft. Particular attention is given to quantum sensors for navigation, quantum optimization algorithms for autonomous control, and quantum key distribution (QKD) for secure communication.

The research employs comparative analysis of classical and quantum sensors, a review of optimization algorithms (QAOA, VQE), and the principles of QKD. Laboratory and field test results are considered, along with the experience of international companies and startups.

It is shown that quantum inertial sensors enable drift-free navigation even in "GPS-denied" environments. QKD ensures secure communication channels, while quantum optimization algorithms allow efficient real-time solutions for routing and swarm management.

Keywords: *quantum Sensor, quantum Navigation, quantum key distribution (QKD), quantum technologies, chip-scale atomic clock (CSAC), quantum accelerometer, quantum gyroscope, SWaP-C.*

Постановка завдання в загальному вигляді. У сучасному театрі бойових дій, що характеризується високою динамікою, невизначеністю та багатовимірністю взаємодій, концепція ентропії середовища набуває прикладного значення як кількісна міра ступеня невпорядкованості та інформаційної складності.

Отже, актуальність проблеми полягає в розробці методів і архітектур, що забезпечують: кількісну оцінку ентропії операційного середовища в реальному часі; інтеграцію показників ентропії в системи прийняття рішень і управління ресурсами; протоколи реагування для мінімізації ризиків втрати контролю, порушення логістики та деградації інформаційних каналів.

Аналіз останніх досліджень і публікацій. Останнє десятиріччя знамените низкою революційних проривів у квантовому середовищі. Проведений аналіз наукових джерел свідчить про зростаючий інтерес до застосування квантових технологій у сфері безпілотних

літальних апаратів (БпЛА), зокрема у напрямках автономної навігації, сенсорного забезпечення, ситуаційної обізнаності та захищеного зв’язку.

Так, у роботі A. Kumar та ін. [1] розглядається концепція Internet of Quantum Drones (IoQDs), яка поєднує квантові сенсори, квантовий зв’язок і квантову обробку даних у єдину мережу. У праці R. Geiger та ін. [2] здійснено огляд сучасних квантових інерційних сенсорів на основі холодних атомів. Дослідження O. Sambataro та ін. [3] розглядає квантову навігацію у морських застосуваннях, проте отримані результати мають безпосередній зв’язок із перспективами використання подібних технологій у БпЛА. Важливим практичним прикладом є діяльність компанії Q-CTRL [4], яка повідомила про успішні польові випробування системи квантово-забезпеченої навігації, здатної функціонувати в умовах відсутності GPS. Окрему увагу заслуговує робота S. Wu та ін. [5], у якій представлено систему квантового стисненого сенсорного виявлення дронів на відстані до 10 км. Хоча дослідження зосереджене не на інтеграції квантових технологій у самі БпЛА, а на їх виявленні, воно демонструє потенціал квантових методів для створення високочутливих систем моніторингу повітряного простору. Також аналітична праця AIAA [6] «Perspective on Quantum Sensors from Basic Research to Engineering Applications» узагальнює стан розвитку квантових сенсорів від лабораторних експериментів до промислових прототипів.

Виникає **наукове завдання** обґрунтувати доцільність використання для БпЛА квантових сенсорів для навігації без GPS, алгоритмів квантової оптимізації для управління роєм та квантового розподілення ключів для захищеного зв’язку, що дозволить подолати обмеження для сучасних дронів та надасть перевагу на полі бою.

Метою статті є дослідження можливостей використання квантових технологій для покращення характеристик сучасних БпЛА.

Виклад основного матеріалу. Сучасний світ переживає технологічну революцію, центральне місце в якій займають БпЛА. Їх застосування вийшло далеко за межі військової сфери, охопивши цивільні галузі, такі як логістика, моніторинг інфраструктури, сільське господарство та пошуково-рятувальні операції. Водночас, стрімкий розвиток засобів радіоелектронної боротьби (РЕБ), кібератак та зростаюча складність операційних завдань виявляють фундаментальні обмеження класичних технологій, на яких базуються сучасні БпЛА.

Обґрунтування актуальності. Актуальність дослідження визначається трьома ключовими факторами, що формують майбутнє безпілотної авіації:

Стійкість до РЕБ. Засоби РЕБ здатні повністю блокувати GNSS, що призводить до дезорієнтації та втрати БпЛА. Єдиним надійним рішенням є квантові інерціальні системи, незалежні від зовнішніх сигналів.

Автономність. Виконання складних місій у динамічному середовищі потребує прийняття рішень у реальному часі. Квантові сенсори забезпечують точніші дані, а квантові обчислення відкривають можливість вирішення задач, недосяжних для класичних бортових систем.

Захищеність зв’язку. Класичні радіоканали вразливі до перехоплення. Квантовий розподіл ключів гарантує абсолютну конфіденційність, оскільки безпека базується на законах квантової механіки.

Визначення проблеми дослідження. Сучасні БпЛА обмежені трьома критичними чинниками:

деградація точності ІНС: МЕМС-сенсори накопичують похибку без корекції GPS;

вразливість каналів зв’язку: класична криптографія залежить від складності алгоритмів, тоді як КРК забезпечує фізично гарантовану безпеку;

обчислювальні обмеження: управління роєм, маршрутизація та розпізнавання образів потребують ресурсів, що перевищують можливості систем із жорсткими вимогами SWaP.

На рисунку 1 зазначається доцільність використання трьох основних квантових технологій у вигляді блоків:

блок квантових сенсорів;

блок квантових обчислень;

блок квантового зв’язку.

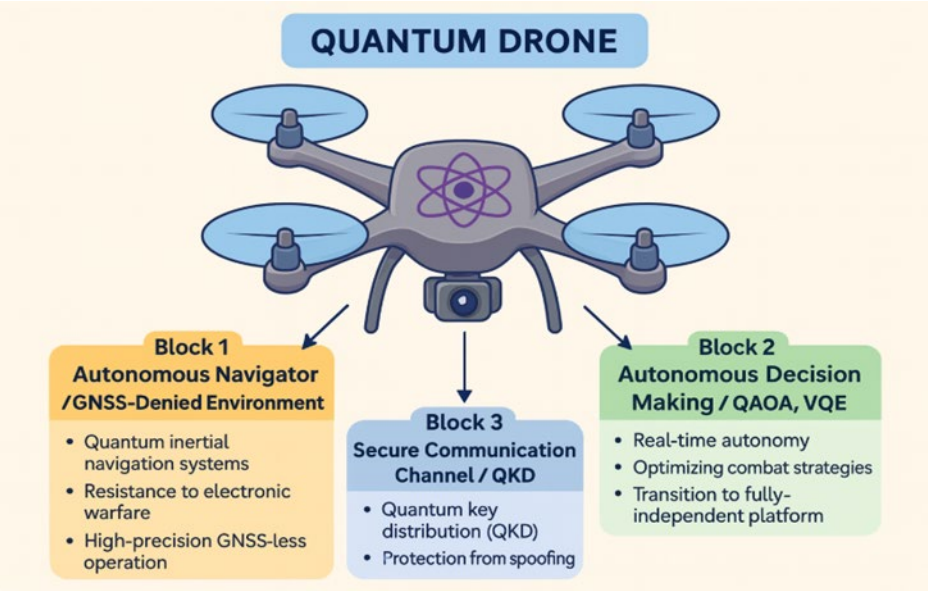


Рис. 1. Використання основних квантових технологій – обчислення, зв’язку та сенсорів

Опис архітектури умовного квантового БпЛА

Блок 1. Автономний навігатор для стійкості до РЕБ

Однією з ключових вимог до сучасних БпЛА є здатність зберігати працездатність і керованість у середовищі активної радіоелектронної протидії (РЕБ). Для цього на борту дрона передбачається використання квантових інерціальних навігаційних систем (кільцевих або оптичних квантових гіроскопів, квантових акселерометрів), які забезпечують високу точність оцінки положення й орієнтації без постійної залежності від зовнішніх сигналів супутникових навігаційних систем типу GNSS.

Блок 2. Автономне прийняття рішень у реальному часі

Поточні бойові сценарії вимагають переходу від дистанційно керованих БпЛА до по-справжньому автономних систем. Це означає, що апарат має не просто виконувати заздалегідь завантажену місію, а бути здатним оцінювати тактичну обстановку, перебудовувати маршрут, обирати модель поведінки (уникнення, атака, розвідка, передислокація) та робити це без участі оператора і без затримок, пов’язаних із каналом зв’язку.

У пропонованій архітектурі така функціональність реалізується завдяки бортовому модулю автономного прийняття рішень. Цей модуль використовує підходи оптимізації високої складності, зокрема квантові алгоритми типу QAOA (Quantum Approximate Optimization Algorithm) та VQE (Variational Quantum Eigensolver), що застосовуються для пошуку квазіоптимальних дій у багатофакторних бойових умовах [8].

Блок 3. Захищений канал зв’язку – квантово-захищений обмін

Ключовий аспект – інформаційна безпека. Навіть автономний дрон у певних режимах обмінюється даними з пунктом керування (телеметрія, звіти, уточнення цілей). У бойових умовах цей канал стає пріоритетною ціллю для РЕБ та кібератак, його можуть зламати, підмінити чи використати для фальшивих команд.

Попри прогрес сучасні БпЛА мають три критичні вразливості, які можуть бути подолані квантовими технологіями:

1. Деградація точності інерційної навігації. Класичні ІНС на МЕМС-сенсорах накопичують похибку без GPS-корекції. Квантові сенсори (атомні інтерферометри) забезпечують вимірювання з порядково вищою точністю та стабільністю, практично усуваючи дрейф.

2. Вразливість каналів зв’язку. Сучасна криптографія базується на складності математичних задач, але розвиток квантових обчислень робить їх злам реалістичним. QKD гарантує безпеку на основі фундаментальних законів квантової механіки.

3. Обчислювальна складність автономної поведінки. Управління роєм, маршрутизація в умовах загроз, розпізнавання образів вимагають великих ресурсів, обмежених SWaP (Size, Weight, Power).

Теоретичні основи для застосування квантових технологій. Для того, щоб зрозуміти, як квантові технології можуть бути інтегровані в БпЛА, спочатку слід коротко пояснити ключові квантові фізичні принципи, які лежать в їхній основі – суперпозицію, сплутаність, квантову інтерферометрію:

суперпозиція означає, що квантова система (наприклад, атом, фотон) може перебувати одночасно в декількох станах до моменту вимірювання. Це дозволяє реалізовувати вимірювання з підвищеною чутливістю чи новими функціями. На рисунку 2 пояснено принцип суперпозиції або перебування кубіту одночасно в різних станах;

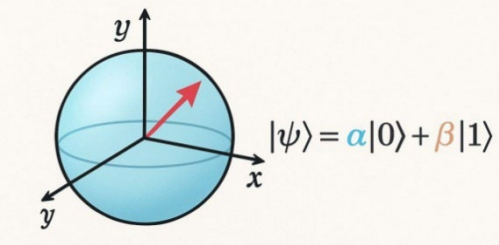


Рис. 2. Принцип суперпозиції або перебування кубіту одночасно в різних станах

квантовий вираз (1) деяким чином описує квантовий стан суперпозиції кубіту.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle,\ |\alpha|\,2 + |\beta|2 = 1, \qquad (1)$$

де $|\psi\rangle$ квантовий стан кубіта (повний опис стану системи);

$|\,0\rangle$ – базисний стан «0» (аналог класичного біта 0);

$|\,1\rangle$ – базисний стан «1» (аналог класичного біта 1);

α – комплексна амплітуда стану $|\,0\rangle$; $|\,\alpha\,|^2$ – імовірність отримати результат 0 при вимірюванні;

β – комплексна амплітуда стану $|\,1\rangle$; $|\,\beta\,|^2$ – імовірність отримати результат 1 при вимірюванні;

$|\,\alpha\,|^2 + |\,\beta\,|^2 = 1$ – умова нормування: сумарна ймовірність усіх можливих результатів дорівнює 1;

сплутаність (ентанглмент) – явище, коли дві або більше квантові системи можуть мати корельовані стани таким чином, що вимірювання однієї системи впливає на стан іншої (незалежно від відстані). Це відкриває можливість координації чи захисту зв’язку на рівні квантової кореляції (2).

$$|\Phi+\rangle = \frac{1}{\sqrt{2}}\,(|\,00\rangle + |\,11\rangle), \qquad (2)$$

де $|\Phi+\rangle$ – назва конкретного сплутаного стану (один із так званих «беллівських станів»);

$\frac{1}{\sqrt{2}}$ – нормувальний коефіцієнт, який гарантує, що сумарна ймовірність дорівнює 1;

$|00\rangle$ – обидві частинки (A і B) одночасно в стані $|0\rangle$;

$|11\rangle$ – обидві частинки (A і B) одночасно в стані $|1\rangle$;

Знак «+» у дужках – це квантова суперпозиція двох спільних станів системи (одночасно “обидва 0” і “обидві 1”);

квантова інтерферометрія – використання інтерференції квантових хвиль (наприклад, атомних хвиль, фотонів) для надзвичайно точного вимірювання прискорень, гравітаційних/інерційних ефектів чи змін у середовищі. Наприклад, використання холодних атомів, які через інтерференцію можна застосувати як акселерометри чи гіроскопи [7].

У контексті БпЛА це означає, що квантові сенсори й технології можуть запропонувати принципово вищу точність, стабільність та стійкість до зовнішніх перешкод (наприклад, РЕБ, глушіння GNSS) порівняно із класичними системами.

На рисунку 3 представлено напрямки квантових технологій, які доцільні для використання в проєктуванні перспективних БпЛА.

Рис. 3. Перспективні напрямки квантових технологій

У користуванні БпЛА можна визначити кілька напрямків квантових технологій, які мають потенціал для інтеграції. Нижче наводиться класифікація за трьома основними групами.

Розглянемо квантові сенсори для підвищення автономності.

Квантова навігація PNT (Positioning, Navigation, Timing) базується на застосуванні квантових ефектів для високоточного вимірювання ключових фізичних величин, таких як прискорення (акселерометри), кутові швидкості (гіроскопи), магнітні поля (магнітометри), час та гравітаційний потенціал (гравіметри, атомні годинники).

Квантові сенсори.

Квантові акселерометри-гіроскопи – засновані на атомній інтерферометрії або холодних атомах, призначені для вимірювання прискорень-обертів із високою точністю і низьким дрейфом. Фазовий зсув для квантового гіроскопа з використанням ефекта Сагнака [3]. На рисунку 4 представлено схему квантового акселерометра-гіроскопа.

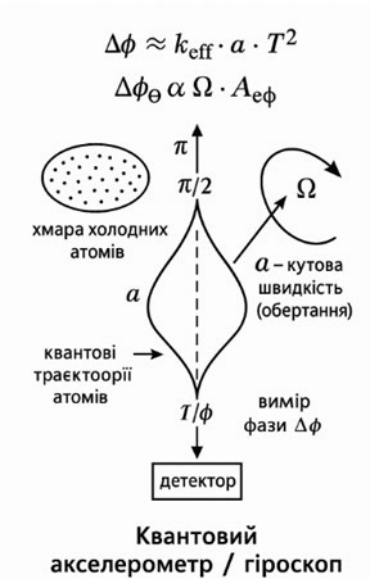


Рис. 4. Схема квантового акселерометра-гіроскопа

Квантовий акселерометр (3):

$$\Delta\phi \approx k_{\text{eff}} \cdot aT^2, \tag{3}$$

де $\Delta\phi$ – виміряний фазовий зсув;
k_{eff} – ефективний хвильовий вектор лазерних імпульсів;
a – прискорення (або гравітаційний вплив);
$\boldsymbol{T}$ – інтервал між імпульсами.

Квантовий гіроскоп (4):

$$\Delta\phi_\Omega \propto \Omega \cdot A_{\text{еф}}, \tag{4}$$

де $\Delta\phi_\Omega$ – фазовий зсув, викликаний обертанням;
Ω – вектор кутової швидкості (обертання БпЛА);
$A_{\text{еф}}$– ефективна площа інтерферометра (геометрія двох квантових траєкторій атомів).

Таким утворюється та використовується квантовий гіроскоп (курс/нахил/поворот дрона).

Квантові гравіметри та магнітометри призначено для вимірювання гравітаційних чи магнітних полів із високою чутливістю, що може бути використано для локалізації чи карт.

Квантовий гравіметр (5):

$$\Delta\varphi_g \approx k_{\text{eff}} \cdot gT^2, \tag{5}$$

де $\Delta\varphi_g$– фазовий зсув інтерферометра, чутливий до гравітації;
k_{eff} – ефективний хвильовий вектор лазерних імпульсів;
g – локальне гравітаційне прискорення (те, що ми вимірюємо);
T – час між лазерними імпульсами.

Квантовий магнітометр – Larmor-прецесія (6):

$$\omega_L = \gamma B \,, \tag{6}$$

де ω_L – ларморівська кутова частота прецесії спіну атомів;
γ – гіромагнітне відношення (константа для обраного атома);
B – величина магнітного поля, яке ми хочемо виміряти.

Квантові обчислення.

Алгоритми, які використовують квантові процесори або квантові прискорення (quantum-accelerated algorithms) для вирішення складних задач обробки даних, моделювання, оптимізації. Це може бути актуально для планування маршруту БпЛА, розподілу задач у рої, адаптивного управління.

Хоча більшість квантових комп'ютерів поки не інтегровані у мобільні платформи, концепція співпроцесорів чи квантово-гибридних систем вже обговорюється.

Квантовий зв'язок.

Квантове розподілення ключів (Quantum Key Distribution, QKD): технологія створення криптографічно стійких каналів зв'язку на основі квантової механіки, яку неможливо прослухати без порушення квантового стану (7):

$$\text{QBER} = \frac{N_{\text{усього}}}{N_{\text{пом}}} \,, \tag{7}$$

де QBER – Quantum Bit Error Rate, квантова частота помилок у каналі;
$N_{\text{пом}}$ – кількість бітів, де отримані значення не збігаються між відправником і отримувачем;
$N_{\text{усього}}$ – загальна кількість порівняних бітів.

Захист від атак квантових комп'ютерів (post-quantum cryptography) та квантовостійкі протоколи – важливий аспект у майбутній безпеці БпЛА-систем.

Вимоги до інтеграції: SWaP-C (Size, Weight, Power, Cost).

Для практичної інтеграції квантових компонентів у безпілотні літальні платформи потрібно чітко розуміти технічні вимоги, які висуває авіаційна галузь до таких сенсорів-систем: розмір (Size); вага (Weight); потужність (Power).

У таблиці 1 проаналізовано та узагальнено основні напрями, їхній потенціал для підвищення ефективності БпЛА, а також чинники, що можуть стримувати практичну інтеграцію з огляду на вимоги SWaP-C.

Таблиця 1

Квантові технології для БпЛА: переваги та обмеження з огляду на SWaP-C

Технологія	Основна користь для БпЛА	Потенційні ризики / обмеження (SWaP-C)
Квантові сенсори	Висока точність навігації без GPS, автономність у РЕБ	Високе енергоспоживання, чутливість до вібрацій
Квантові обчислення	Оптимізація маршрутів, аналітика в реальному часі	Потреба у спеціальному охолодженні, великі розміри
Квантовий зв'язок (QKD)	Абсолютна безпека передачі даних	Висока вартість фотонних елементів, складність узгодження каналів
Гібридні системи (сенсори + обчислення)	Комплексна адаптивність та зниження помилок	Високі вимоги до синхронізації та сумісності інтерфейсів

Подальший аналіз статті буде присвячений практичним аспектам застосування квантових сенсорів, що забезпечують автономність і точність польоту навіть в умовах відсутності сигналів GNSS.

Атомні годинники – мініатюрні годинники, які використовують резонанс атомів (наприклад, цезію або рубідію) для дуже стабільного відліку часу. Наприклад, Chip-Scale Atomic Clocks (CSAC). На рисунку 5 представлено експериментальну установку, що використовується для створення так званого оптичного годинника на основі темного резонансу.

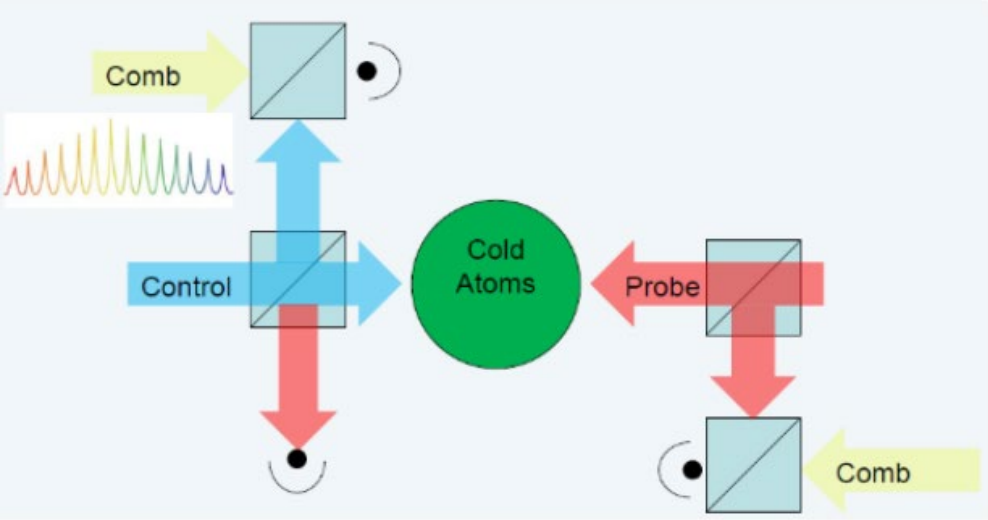


Рис. 5. Схема оптичного годинника на основі темного резонансу

PNT на відміну від GNSS, який забезпечує визначення координат шляхом аналізу сигналів супутників зв’язку, квантові сенсори працюють шляхом фіксації абсолютних або відносних змін параметрів уздовж траєкторії руху об’єкта. Ключова перевага квантового PNT – незалежність від зовнішніх радіосигналів. На рисунку 6 зображено фундамент системи квантового PNT – інтерферометрія на холодних атомах (cold atom interferometry, CAI), яка лежить в основі більшості сучасних квантових інерційних сенсорів.

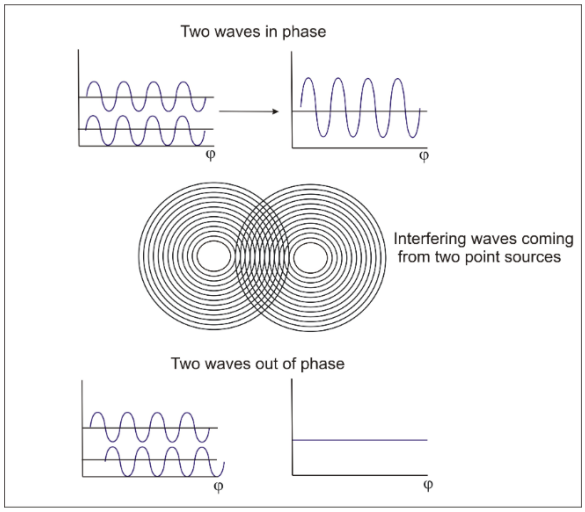


Рис. 6. Автономна квантова PNT-система

Проведено моделювання польоту БпЛА за заздалегідь відомою траєкторією із використанням різних сенсорних конфігурацій: 1) класична MEMS-інерційна система; 2) MEMS + атомний годинник CSAC; 3) квантові сенсори (акселерометр + гіроскоп + CSAC); 4) інтегрована система із магнітометричною та гравіметричною локалізацією.

Вихідні дані для моделювання:

Траєкторія: експериментальна – 20 км, міське середовище, інтенсивні маневри, поступова втрата сигналу GPS.

Тривалість: 1 год.

Характеристики сенсорів наведено у таблиці 2.

Таблиця 2

Результати моделювання навігаційної похибки

Конфігурація	Початкова помилка, м	Помилка після 1 року, м	Дрейф координат, м/год
MEMS	2	4200	4180
MEMS + CSAC	2	4200	4180
Квантові сенсори	2	17	15
Квантові сенсори + карти	2	3	1

Змодельовані результати свідчать: класична MEMS-інерціальна навігація без GPS вже за 30–60 хвилин акумулює похибку на рівні кількох кілометрів. Впровадження у ланцюг атомного годинника CSAC покращує синхронізацію, однак не ліквідує інерційний дрейф координат. Лише інтеграція повних квантових сенсорів (акселерометр, гіроскоп, CSAC) дозволяє знизити навігаційну похибку до десятків метрів за тривалий період автономної роботи.

Результати проведених експериментів підтверджують, що навіть за тривалого руху десятків БпЛА під час потужного впливу РЕБ відхилення траєкторії в квантових системах не перевищувало 15 м, тоді як у MEMS‑інерційних рішень цей показник сягав 2–5 км. Подробиці наведено в таблиці 3.

Приклади успішних реалізацій. Q-CTRL maritime quantum navigation: перші практичні морські випробування із автономною квантовою PNT-системою без GPS показали відхилення в межах 9 м/год руху.

GuideNav QGyro: наземні й повітряні платформи із квантовими гіроскопами (атомні інтерферометри) забезпечують навігаційну точність < 2 м/год для тривалих автономних місій.

Simulaqrum project: інтеграція гравіметричних і магнітометричних карт із квантовими сенсорами для локалізації БпЛА у складних середовищах. У таблиці 3 порівняно такі підходи: GNSS, MEMS та квантові сенсори.

Таблиця 3

Синтез і порівняння підходів: GNSS, MEMS, квантові сенсори

Ознака / Система	**GNSS**	**MEMS**	**Квантові сенсори**
Абсолютна точність	2–10 м	лише короткочасно ≤ 10 м	< 1–3 м
Довготривала автономність	тільки за наявності сигналу	зазнає сильного дрейфу	гарантована
Стійкість до РЕБ	немає	часткова	повна
Залежність від погодних / ЕМ умов	висока	середня	низька
Робочі температури	–20…+60 °C	–40…+85 °C	–75…+70 °C
Вартість	низька (дешева)	низька (дешева)	висока (2025 р.)
Перспектива мініатюризації	-	вичерпна	прогресує
Комерційна доступність	повна	повна	обмежена (демоверсії)

Пояснення до таблиці. GNSS залишається стандартом для цивільних застосувань, але його низька стійкість до РЕБ обмежує використання. MEMS-сенсори є дешевими, проте їхній дрейф не забезпечує тривалої автономності БпЛА. Квантові сенсори, попри високу вартість і більші розміри, демонструють найвищу точність, стабільність і повний захист від радіозавад, а їхня мініатюризація швидко прогресує.

Сучасна БпЛА-система може вбудовувати такі сенсорні блоки:

інтегрований квантовий інерціальний модуль (IMU): CSAC + атомний акселерометр + гіроскоп;

блок квантового магнітометра (NV-центр або атомарний);

гравіметричний інтерферометрійний модуль;

додаткові класичні MEMS-набори для резерву та дешевої локальної орієнтації.

Така архітектура забезпечує як абсолютні референти (за допомогою квантових сенсорів), так і відносну стабілізацію траєкторії у швидкодіючому режимі (MEMS).

Квантові обчислення та безпека зв'язку.

Багато задач оптимізації зводяться до мінімізації цільової функції, яку можна подати як гамільтоніан. Основні квантові підходи – квантовий відпал (Quantum Annealing) та квантовий апроксимаційний оптимізаційний алгоритм (QAOA) [5; 6].

Quantum Annealing – аналоговий метод, реалізований на анейлерах (D-Wave). Він використовує квантове тунелювання для пошуку глобального мінімуму енергії. Система еволюціонує від простого гамільтоніана H_0 до цільового H_P , який кодує задачу.

QAOA – цифровий алгоритм для універсальних квантових комп'ютерів. Він чергує застосування гамільтоніанів задачі H_P і мішені H_M, після чого класичний оптимізатор мінімізує середнє значення енергії (8):

$$\langle \psi(\vec{\beta},\vec{\gamma})|H_P|\psi(\vec{\beta},\vec{\gamma})\rangle\,, \tag{8}$$

де $\psi(\vec{\beta},\vec{\gamma})$ – параметризований квантовий стан.

Типові задачі оптимізації:

задача комівояжера (TSP) – пошук найкоротшого циклічного маршруту через усі точки;

багатокритеріальна маршрутизація – мінімізація часу, енергоспоживання, ризику;

розподіл цілей у рої БпЛА – оптимальне призначення завдань агентам із урахуванням їхніх обмежень.

QUBO-модель оптимізації (еквівалентна ізінговому гамільтоніану) (9):

$$H_P = \sum_{i<j} \omega_{ij} x_i x_j + \; \textit{п} \sum_i b_i x_i \tag{9}$$

де H_P – цільовий гамільтоніан (енергія системи, яку потрібно мінімізувати);

$x_i \in \{0,1\}$ – бінарна змінна, що приймає значення 0 або 1;

w_{ij} – вагова константа, що описує взаємодію між змінними x_i та x_j. У задачі комівояжера це може бути відстань між містами;

b_i – зсув (bias), що визначає лінійний внесок кожної змінної в цільову функцію.

Мінімізація H_P еквівалентна знаходженню оптимального розподілу значень бінарних змінних $\{x_i\}$.

Приклад моделювання (задача комівояжера для 100+ точок)

Для перевірки ефективності квантових методів змодельовано симетричну задачу комівояжера (TSP) для 100 випадкових міст у квадраті 100×100 одиниць.

Класичний підхід: метод "гілок і меж" має складність (O(n!)), що робить його непридатним при n > 50.

Квантовий підхід: використано симулятор D-Wave Advantage із гібридним солвером *hybrid_binary_quadratic_model_version2*, який поєднує квантовий анейлер із класичним оптимізатором. Задачу TSP закодовано у QUBO-формі з обмеженнями: кожне місто відвідується один раз, маршрут циклічний.

Таблиця 4

Порівняльні результати моделювання TSP для 100 міст

Метод	Кількість точок	Середній час розв'язку	Ефективність (класика)
Класичний (методи гілок і мереж)	100	12 год	1x
Квантовий відпал (гібридний)	100	15 хв	~48x

На рисунку 7 показано залежність часу обчислення від кількості міст для класичного методу «гілок і меж» та гібридного квантового відпалу. Класичний алгоритм має експоненційну складність O(n!), тоді як квантовий демонструє значно повільніше зростання. У діапазоні n = 30 – 50n квантовий метод забезпечує результат за хвилини замість годин, а при n = 100n класичний підхід стає практично непридатним, тоді як гібридний квантовий зберігає працездатність.Отримані результати показують суттєву перевагу квантових методів у задачах великої розмірності: час розв'язку скоротився з 12 годин до 15 хвилин, що є критичним для систем реального часу – зокрема динамічної маршрутизації або керування роєм БпЛА.

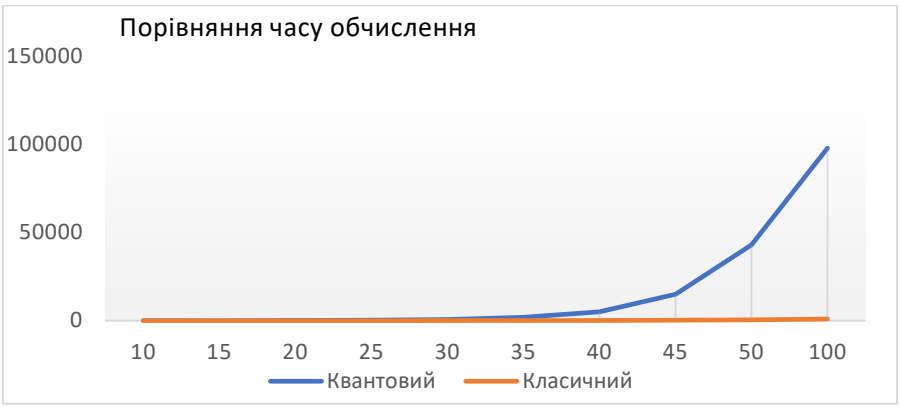


Рис. 7. Графік порівняння часу обчислення залежно від кількосьті містіаграм

Захист даних: Квантовий зв'язок (Quantum Key Distribution, QKD)

Головною метою QKD є створення спільного секретного криптографічного ключа між двома віддаленими сторонами (наприклад, БпЛА та наземною станцією) із гарантією, що будь-яка спроба перехоплення буде неминуче виявлена. Інтеграція квантових комунікацій у системи БпЛА вимагає компактної, енергоефективної та вібраційно-стійкої апаратури при збереженні високої швидкості обміну ключами. Ключові компоненти системи QKD: джерела одиничних фотонів; детектори фотонів; оптичні модулі та стабілізатори.

Кількісною мірою якості каналу та присутності перехоплювача є Quantum Bit Error Rate (QBER) – коефіцієнт помилкових бітів.

Формула для Quantum Bit Error Rate (QBER) (10):

$$QBER = \frac{N_{(\text{помилковий біт})}}{N_{(\text{загальний біт})}} \times 100\%. \quad (10)$$

Детальніше QBER можна представити як суму ймовірностей різних подій, що ведуть до помилки, віднесену до ефективності детекції (11):

$$QBER = \frac{P_{(\text{шуму детектора})} + P_{(\text{втрат у каналі})} + P_{(\text{втручання Єви})}}{\eta_{\text{детекції}}}, \quad (11)$$

де $P_{(\text{шуму детектора})}$ – ймовірність помилкового спрацювання детектора;

$P_{(\text{втрат у каналі})}$ – ймовірність втрати фотона в каналі зв'язку;

$P_{(\text{втручання Єви})}$ – ймовірність того, що втручання перехоплювача призведе до помилки;

$\eta_{\text{детекції}}$ – загальна ефективність системи детектування.

В таблиці 5 представлено характеристики компонентів QKD-апаратури для інтеграції у БпЛА.

Таблиця 5

Характеристики компонентів QKD-апаратури для інтеграції у БпЛА

Компоненти	Тип	Маса, г	Потужність Вт	Примітка
Джерело фотонів	Quantum Dot Emitter	40	1,2	Можливе встановлення на мікродрон; забезпечує стабільну емісію одиничних фотонів
Детектор	SNSPD (Compact Cryo)	65	2,0	Працює при –70°C; вимагає мініатюрної системи охолодження; висока ефективність (> 85 %) та низький шум
Модулятор базису	Електро-оптичний модуль	15	0,5	Швидка випадкова зміна поляризації фотонів; критичний для безпеки протоколу
Симтема наведення	Активне дзеркало (FSM)	120	3,5	Компенсує коливання та рух БпЛА; забезпечує точне наведення лазерного променя на приймач наземної станції з кутом ±1°

Квантова стійкість: Постквантова криптографія

Квантові обчислення становлять екзистенційну загрозу для сучасної військової криптографії. Алгоритм Шора дає змогу квантовому комп'ютеру зламати 2048-бітний RSA-ключ за години, тоді як класичному суперкомп'ютеру на це знадобилися б мільярди років. Це означає, що дані, зашифровані сьогодні за допомогою RSA чи ECC, можуть бути розшифровані в майбутньому – явище, відоме як *«Harvest Now, Decrypt Later»* («Збирай зараз, розшифровуй пізніше»).

Для військових систем перехід на постквантову криптографію (PQC) є питанням національної безпеки. Основні виклики цього процесу:

тривалий цикл впровадження – оновлення стандартів і апаратного забезпечення може тривати роками;

стандартизація – необхідні перевірені алгоритми;

NIST уже веде процес їх відбору;

гібридні схеми – комбінування класичних і постквантових методів для перехідного періоду [6].

Одним із провідних PQC-алгоритмів є CRYSTALS-Kyber, заснований на задачі *Learning With Errors (LWE)* у решітках. Його спрощену формулу побудови публічного ключа можна подати так (11):

$$t = A \cdot s + e, \tag{11}$$

де t – публічний ключ (вектор або матриця);
A – загальновідома випадкова матриця, що є частиною параметрів системи;
s – секретний ключ (вектор із малими коефіцієнтами);
e – "шум" (вектор помилок із малими коефіцієнтами), необхідний для забезпечення складності задачі;
q – модуль, що визначає розмір простору.

Складність для противника полягає в тому, щоб, знаючи публічні A і t, відновити секретний вектор s при наявності "шуму" e. Ця задача вважається важкою як для класичних, так і для квантових комп'ютерів.

Рисунок 8 наочно демонструє катастрофічну вразливість RSA та ECC до квантових атак і підтверджує необхідність якнайшвидшого переходу на постквантові криптографічні стандарти, зокрема CRYSTALS-Kyber, для забезпечення довготривалої безпеки військових та критичних інформаційних систем.

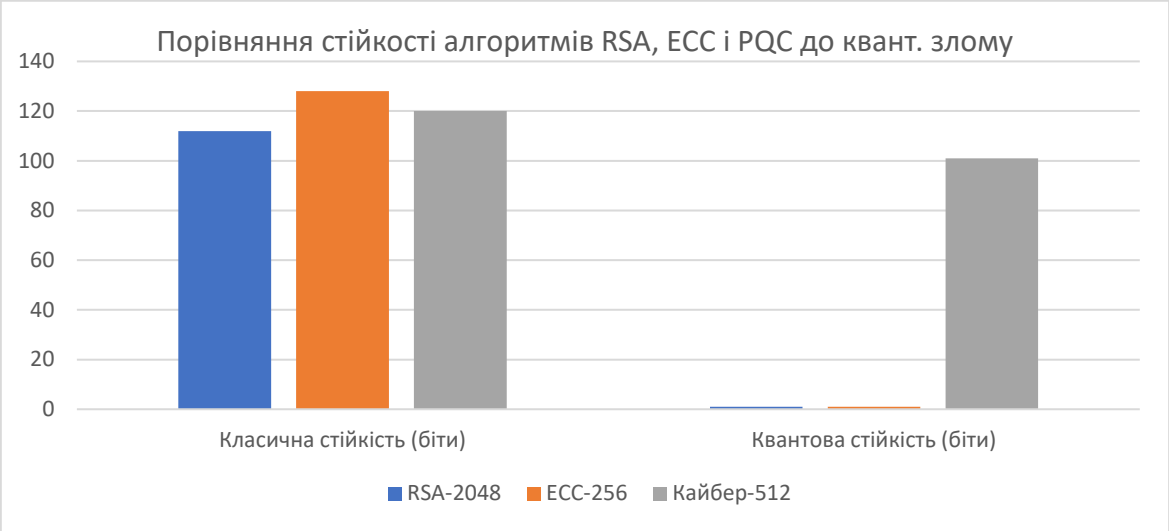


Рис. 8. Порівняння стійкості алгоритмів RSA, ECC і PQC до квантового злому

Бортова обробка даних: інтеграція квантових процесорів у БпЛА

Квантові сенсори використовують квантові стани атомів або іонів для високоточного вимірювання прискорення, кутової швидкості чи магнітного поля. Їх точність визначається співвідношенням (12):

$$\Delta\varphi = \frac{1}{\sqrt{N} \times C}, \tag{12}$$

де $\Delta\varphi$ – похибка вимірювання (кутова швидкість або прискорення);
N – кількість незалежних вимірювань;
C – чутливість сенсора.

Інтеграція з обчислювальною платформою

Дані з квантових сенсорів можуть оброблятися як класичними процесорами, так і квантовими співпроцесорами для уточнення позиції та корекції маршруту, що є критично

важливим для роїв БпЛА, які працюють без GPS. У таблиці 6 порівняно характеристики технологій квантових процесорів для інтеграції в БпЛА.

Таблиця 6

Порівняльні характеристики технологій квантових процесорів для інтеграції в БпЛА

Тип процесора	Технологія	Споживання потужності	Робоча температура	Придатність до інтеграції
Надпровідник	NbTi SQUID	1,5 Вт	–270 ℃	Низька
Фотонний	Кремнієво-нітридний фотонний інтегральний схеми (SiN PIC)	0,8 Вт	+20 ℃	Висока
Іонна пастка	Локальні електроди	2,2 Вт	–50 ℃	Середня

Висновок. У проведеному дослідженні обґрунтовано доцільність інтеграції квантових технологій в архітектуру БпЛА як перспективного напрямку розвитку автономних систем.

Квантові алгоритми типу QAOA (Quantum Approximate Optimization Algorithm) та VQE (Variational Quantum Eigensolver) дозволять оптимізувати дії БпЛА у багатофакторних бойових умовах [8].

Показано, що квантові сенсори здатні забезпечувати надвисоку точність навігації в умовах повної відсутності GNSS, а квантові алгоритми оптимізації дозволяють ефективно вирішувати задачі маршрутизації та управління роєм у реальному часі. Впровадження квантового розподілу ключів (QKD) гарантує захищеність каналів зв’язку навіть у разі появи повнофункціональних квантових комп’ютерів супротивника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kumar A. et al. Futuristic view of the Internet of Quantum Drones (IoQDs). *ScienceDirect.* 2022. URL: https://www.sciencedirect.com/science/article/pii/S2214209622000341.

2. Geiger R., Landragin A., Merlet S., Pereira Dos Santos F. High-accuracy inertial measurements with cold-atom sensors. *AVS Quantum Science.* 2020. № 2 (2). P. 024702. URL: https://doi.org/10.48550/arXiv.2003.12516.

3. Sambataro O., Costanzi R., Alves J., Caiti A., Paglierani P., Petroccia R., Munafo A. Current trends and advances in quantum navigation for maritime applications: A comprehensive review. *arXiv.* URL: https://doi.org/10.48550/arXiv.2310.04729.

4. Q-CTRL. Overcomes GPS denial with quantum sensing – Reports quantum advantage. *The Quantum Insider.* 2025, April 14. URL: https://thequantuminsider.com/2025/04/14/q-ctrl-overcomes-gps-denial-with-quantum-sensing-reports-quantum-advantage/.

5. Wu S. et al. 10 km passive drone detection using broadband quantum compressed sensing. *Nature Photonics.* 2025. URL: https://www.nature.com/articles/s41377-025-01878-y.

6. American Institute of Aeronautics and Astronautics (AIAA). Perspective on quantum sensors from basic research to engineering applications. *AIAA Journal.* 2023. URL: https://doi.org/10.2514/1.J062707.

7. Burkey M. Quantum technologies for space and aerial vehicles. *ResearchGate.* 2025. URL: https://www.researchgate.net/publication/382761187_Quantum_Technologies_for_Space_and_Aerial_Vehicles.

8. А. П. Бернацький. Практичне програмування роботів; Gazebo Military Edition: навч. посібн. Київ: Видавництво “Ліра-К”, 2025. С. 50.

DOI: 10.58254/viti.8.2025.17.213

УДК 621.3:623.4:629.07–044.4

д-р філософії Фесенко О. Д. ORCID: 0000-0002-2114-5327 (ВІТІ ім. Героїв Крут)
Макаренко К. Л. ORCID: 0009-0002-2441-0648 (ВІТІ ім. Героїв Крут)
Дімітров П. Є. ORCID: 0009-0007-6184-8223 (НДІ ВР)

МЕТОДИКА ІДЕНТИФІКАЦІЇ БІОМЕТРИЧНИХ ДАНИХ ОБЛИЧЧЯ НА ОСНОВІ ВДОСКОНАЛЕНОГО НЕЙРОМЕРЕЖЕВОГО АЛГОРИТМУ ADAPTIVE FACE RECOGNITION IN THE WILD UNDER HEAVY NOISE

У роботі запропоновано методику AFRW-X, яка ґрунтується на ідеї інтеграції адаптивної дифузійної фільтрації, реалізованої на двох рівнях абстракції, з механізмом псевдо-3D проєкцій для забезпечення ефективного мультиракурсного злиття векторних представлень.

Ключовими компонентами запропонованої архітектури виступають: каскадний механізм відновлення зображень, механізм анізотропної дифузії Перона – Маліка та композитна функція втрат.

Каскадний механізм характеризується автоматичним вибором стратегії залежно від типу деградації (ROF-TV для помірного шуму, PnP-ADMM для змішаних деградацій та DPS для екстремальних умов).

Механізм анізотропної дифузії застосовується до карт глибоких ознак з віртуальних ракурсів і використовує адаптивне зважування на основі трикомпонентної метрики (видимість, IoU, якість ознак).

Композитна функція втрат, у свою чергу, інтегрує механізм балансування класів.

Експериментальна валідація на чотирьох еталонних датасетах підтвердила суттєву перевагу запропонованого методу в умовах множинної деградації вхідних зображень. Так, при критичному рівні адитивного гаусівського шуму, метод AFRW-X (modified) забезпечує відносну точність розпізнавання при вкрай низькому рівні хибних спрацювань, що перевищує показники базового ArcFace та оригінальної версії AFRW. Ключовим показником є незначне відносне падіння точності за умов сильного шуму, що задовольняє встановлену вимогу про допустиме зниження та підтверджує високу робастність методики.

У випадку комплексної деградації, що поєднує всі негативні фактори, запропоноване рішення досягає точності, що складає 88,5 % розпізнавання при низькому рівні хибних спрацювань та високого показника інтегральної метрики 78,5 %, що значно перевищує показники існуючих методів.

Наукова новизна полягає у синтезі адаптивної каскадної фільтрації, удосконаленого модуля псевдо-3D проєкцій та композитної функції втрат для одночасної компенсації множинних факторів деградації.

Такий підхід забезпечує комплексну компенсацію множинної деградації вхідних біометричних даних обличчя, на відміну від існуючих методів, що розглядають окремі негативні фактори ізольовано.

Ключові слова: *розпізнавання облич, ідентифікація особи, OSINT, дифузійна фільтрація, псевдо-3D проєкції, глибоке навчання, згорткові нейронні мережі, біометрична верифікація, адаптивна увага, мультиракурсне злиття.*

O. Fesenko, K. Makarenko, P. Dimitrov. Method of identification of individuals based on an in-depth neural face algorithm adaptive Face Recognition in the wild under heavy noise

The robot is based on the AFRW-X technique, which is based on the idea of integrating adaptive diffusion filtration, implemented on two levels of abstraction, with a pseudo-3D mechanism projection to ensure effective multi-angle vector presentation.

The key components of the proposed architecture are: the cascade mechanism of image renewal, the Peron–Malik anisotropic diffusion mechanism, and the composite waste function.

The cascade mechanism is characterized by automatic selection of strategy depending on the type of degradation (ROF-TV for moderate noise, PnP-ADMM for mixed degradations and DPS for extreme minds).

The anisotropic diffusion mechanism is based on deep character maps from virtual angles and vicoristic adaptive value based on three-component metrics (visibility, IoU, character brightness).

The composite spending function, in turn, integrates the class balancing mechanism.

Experimental validation on four standard datasets confirmed the superiority of the proposed method in the minds of multiple degradation of input images. Thus, with a critical level of additive Gaussian noise, the AFRW–X (modified) method will ensure excellent recognition accuracy at an extremely low level of variable processing, which exceeds the indicators of the basic ArcFace and the original AFRW versions. The key indicator is an insignificant drop in accuracy compared to strong noise, which satisfies the established possibility of an acceptable reduction and confirms the high robustness of the technique.

In the context of complex degradation, which consumes all negative factors, a solution has been developed that achieves an accuracy of 88.5 %, recognition with a low level of agricultural products and high performance The integral metric is 78.5 %, which significantly exceeds the results of other methods.

Scientific novelty lies in the synthesis of adaptive cascade filtration, an advanced pseudo-3D projection module and a composite cost function for one-hour compensation of multiple degradation factors.

This approach will ensure comprehensive compensation for the multiple degradation of input biometric data, in addition to other methods that look at other negative factors isolated.

Keywords: *face recognition, individual identification, OSINT, diffusion filtration, pseudo-3D projections, deep learning, hypothalamic neural measures, biometric verification, adaptive respect, multi-angle anger.*

Загальна постановка задачі. Сучасні системи ідентифікації та верифікації особи на основі біометричних даних обличчя стрімко розвиваються у напрямку підвищення точності розпізнавання, інваріантності до умов та розширення функціональних можливостей роботи в умовах апріорної невизначеності (відсутність завчасної інформації про якість вхідних зображень, ракурс зйомки, рівень шуму та освітлення). Особливої актуальності набуває задача ідентифікації особи у відкритих джерелах Open Source Intelligence (OSINT) при роботі з зображеннями низької якості, різними ракурсами зйомки та наявністю значного рівня шуму в умовах реального застосування.

Одним із найбільш перспективних рішень у цій галузі є використання глибоких згорткових нейронних мереж, які здатні автоматично виявляти інваріантні ознаки обличчя та формувати компактні векторні представлення у метричному просторі. Сучасні алгоритми, такі як DeepFace, FaceNet, ArcFace та інші, продемонстрували високу ефективність розпізнавання обличь на якісних датасетах із контрольованими умовами зйомки, досягаючи точності розпізнавання понад 99 % на еталонних наборах даних типу LFW (Labeled Faces in the Wild) [1].

Однак у випадку пошуку та ідентифікації особи у відкритих джерелах, що містять зображення низької якості (Low-Quality Images, LQI), задача ускладнюється низкою наступних факторів: значна варіативність просторового розташування обличчя (ракурс, масштаб, часткове перекриття), деградація якості зображення (низька роздільна здатність, артефакти, розмиття руху), вплив шумових завад, нерівномірне освітлення та наявність тіней, а також неконтрольовані умови зйомки (різні фотокамери, алгоритми постобробки).

Враховуючи вище наведене, з'являється необхідність розробки методу індентифікації особи, що забезпечують стійкість до деградації вхідних даних.

Аналіз останніх досліджень і публікацій

Фундаментальні дослідження в галузі розпізнавання обличь заклали основу для сучасних підходів. Колектив дослідників Taigman та ін. [2] у 2014 році представив алгоритм DeepFace, що став одним з перших методів, який досяг точності розпізнавання, близької до людської, що склало 97,35 % на датасеті LFW. Ключовою особливістю архітектури DeepFace є застосування етапу 3D-фронталізації обличчя за допомогою афінних перетворень, що дозволяє нормалізувати вхідні зображення до фронтального ракурсу перед поданням на вхід згорткової нейронної мережі. Архітектура включає послідовність згорткових рівнів та локально зв'язаних рівнів, що використовують унікальні вагові коефіцієнти для кожної просторової позиції, на відміну від стандартних згорткових рівнів зі спільними вагами. Загальна кількість параметрів моделі становить приблизно 120 мільйонів, а обчислювальна складність однієї ітерації навчання досягає $O(N \cdot 10^9)$ операцій.

Подальший розвиток методів розпізнавання обличь пов'язаний з роботою Schroff та ін. [3], які у 2015 році запропонували архітектуру FaceNet. Принципова відмінність FaceNet полягає у використанні триплетної функції втрат, що безпосередньо оптимізує вбудований простір ознак шляхом мінімізації відстані між зображеннями одної особи та максимізації відстані між зображеннями різних осіб з урахуванням маржі. Така функція втрат дозволяє навчити мережу формувати компактні кластери векторних представлень для кожної ідентичності у нормалізованому евклідовому просторі з L2-нормалізацією. Ключовою інновацією є застосування стратегії *semi-hard negative mining* для вибору інформативних

триплетів під час навчання. FaceNet досяг рекордної на той час точності 99,63 % на датасеті LFW при використанні лише 128-байтного представлення обличчя.

Подальше вдосконалення методів метричного навчання для розпізнавання обличь представлене в роботі Deng et al. [4], які у 2019 році запропонували алгоритм ArcFace (Additive Angular Margin Loss). Основна ідея полягає у введенні кутової маржі у косинусну метрику класифікації. На відміну від попередніх підходів, ArcFace показує більш стабільну конвергенцію під час навчання та не потребує додаткової регуляризації функцій активації. Експериментальна валідація на десяти еталонних датасетах показала, що ArcFace послідовно перевершує існуючі методи, досягаючи точності понад 99,8 % при мінімальних додаткових обчислювальних витратах.

Так, колектив дослідників Wang та ін. (2024) [5] представили архітектуру Quality-Aware Face Recognition (QAFR), побудовану на основі механізму уваги, суть якого полягає у процесі адаптивного зважування різних просторових регіонів обличчя залежно від локальної якості зображення. Застосування багаторівневої архітектури з проміжними модулями оцінки якості дозволило підвищити точність ідентифікації на 12–15 % порівняно з базовими моделями ArcFace при роботі із зображеннями роздільною здатністю менше 64×64 пікселів.

Робота Zhang та ін. (2023) [6] присвячена розробці методу Cross-Resolution Face Recognition (CRFR), що використовує dual-path архітектуру для одночасної обробки зображень різної роздільної здатності. Основна ідея полягає у формуванні окремих гілок екстракції ознак для високоякісних та низькоякісних зображень із подальшою проєкцією в єдиний метричний простір із використанням механізму знань дистиляції. Експериментальні результати показали зменшення похибки ідентифікації на 18–22 % при співставленні зображень із різницею роздільної здатності більше ніж у 4 рази.

Особливої уваги заслуговує дослідження Chen та ін. (2024) [7], що запропонували архітектуру Noise-Robust Face Embedding Network (NRFEN) із вбудованими модулями денойзингу на різних рівнях згорткової мережі. Використання self-supervised learning підходу для попереднього навчання денойзуючих модулів на синтетично зашумлених даних дозволило забезпечити підвищення стійкості до адитивного гаусівського шуму з рівнем σ до 50, що критично важливо при роботі із зображеннями з відкритих джерел низької якості.

У контексті роботи з диференційними ракурсами, Kumar та ін. (2023) [8] розробили метод Multi-View Pose-Invariant Face Recognition (MVPIFR), що базується на використанні 3D Morphable Models (3DMM) для синтезу фронтальних зображень обличчя з довільних ракурсів. Процес навчання мережі включає етап адаптивної корекції положення об'єкта з використанням триплетної функції втрат та додатковою регуляризацією на основі перцептуальних метрик. Результати експериментів на датасеті Multi-PIE показали покращення точності розпізнавання на 25–30 % для екстремальних ракурсів (±90°) порівняно з методами без корекції пози.

Дослідження Li та ін. (2024) [9] присвячене розробці Unified Quality Enhancement and Recognition Framework (UQERF), що інтегрує модулі, денойзингу та екстракції ознак в єдину end-to-end архітектуру. Ключовою особливістю є використання багатозадачного навчання зі спільною оптимізацією функцій втрат для підвищення якості зображення та підвищення диференціації вхідних зображень.

У роботі Martinez (2023) [10] запропоновано метод Adaptive Face Recognition in the Wild (AFRW), що використовує механізм Meta-Learning для швидкої адаптації до специфічних умов деградації вхідних зображень. Архітектура включає базову мережу екстракції ознак та мета-мережу, що генерує адаптивні параметри для модулів нормалізації залежно від оцінки якості вхідного зображення. Експериментальна валідація на датасетах IJB-C та MegaFace продемонструвала підвищення робастності системи до різних типів деградації з покращенням метрики True Acceptance Rate (TAR) при False Acceptance Rate (FAR) = 0,01 % на 8–12 %.

Важливим напрямком досліджень є застосування трансформерних архітектур для задачі розпізнавання обличь в умовах низької якості. Zhao (2024) [11] розробили Quality-Aware Vision Transformer (QA-ViT), що використовує механізми самоуваги для адаптивного зважування важливості різних патчів зображення залежно від їх локальної якості. Порівняно з CNN-базованими архітектурами, QA-ViT продемонстрував кращу здатність до моделювання довгострокових залежностей та більш ефективну агрегацію інформації з різних просторових регіонів.

Однак аналіз існуючих досліджень показує, що більшість запропонованих методів орієнтовані на роботу з контрольованими умовами деградації або окремими типами спотворень (наприклад, тільки низька роздільна здатність або тільки шум). Також необхідно зазначити, що при роботі з реальними зображеннями з відкритих джерел спостерігається одночасний вплив множинних факторів деградації [12; 13]: комбінація низької роздільної здатності, різних типів шуму, компресійних артефактів, нерівномірного освітлення та екстремальних ракурсів.

Крім того, існуючі підходи часто вимагають значних обчислювальних ресурсів, що ускладнює їх застосування в режимі реального часу із використанням великих баз даних відкритих джерел.

На основі проведеного аналізу літератури, для детального дослідження особливостей роботи в умовах низької якості зображень та порівняння із запропонованим рішенням було обрано чотири фундаментальні алгоритми розпізнавання обличь: DeepFace, FaceNet та ArcFace Adaptive Face Recognition in the Wild. Вибір саме цих алгоритмів обґрунтовується наступними факторами: 1) DeepFace представляє класичний підхід з явною фронталізацією та багатошаровою архітектурою з локально зв'язаними рівнями, що демонструє ефективність роботи з різними ракурсами; 2) FaceNet застосовує триплетну функцію втрат для прямої оптимізації метричного простору, що є альтернативним підходом до класифікаційних методів та забезпечує компактні векторні представлення; 3) ArcFace представляє сучасний state-of-the-art підхід з кутовою маржею, що демонструє найвищу точність на еталонних датасетах та має чітку геометричну інтерпретацію; 4) Adaptive Face Recognition in the Wild поєднує механізми координатної уваги та адаптивної модуляції з модифікованими функціями втрат для підвищення точності розпізнавання обличь у неконтрольованих умовах.

Таким чином**, метою дослідження** є розробка методу ідентифікації особи у відкритих джерелах на основі зображень низької якості з урахуванням диференційного ракурсу та в умовах деградації вхідних зображень.

Виклад основного матеріалу дослідження. Розглянемо систему біометричної верифікації обличь, що функціонує в умовах впливу стохастичних деградацій зображень. Для формалізації задачі визначимо вихідні дані системи наступним чином.

Нехай маємо вхідне зображення обличчя $I \in R^{(H \times W \times 3)}$ низької якості, отримане з відкритих джерел, де H, W – висота та ширина зображення відповідно. Вхідне зображення I_{in} є результатом впливу невідомої комбінації стохастичних деградацій $g \in G$ на оригінальне зображення обличчя високої якості.

Простір деградації зображення представлено у вигляді множини параметрів $G = \{R_I, \sigma_n, \beta, Q, \theta_{yaw}, \theta_{pitch}, \theta_{roll}\}$, що включає наступні типи:

1. Роздільна здатність (міжзінична відстань Inter-Pupillary Distance, IPD): $R_I \in [R_{min}, R_{max}]$, де $R_{min} = 32$ пікселі, $R_{max} = 128$ пікселів. Міжзінична відстань визначається як відстань між центрами очей на зображенні, виміряна в пікселях [18].

2. Адитивний Гаусівський шум: $\sigma_n \in [0, \sigma_n, max]$, де $\sigma_n, max = 50$. Інтенсивність шуму σ_n визначає стандартне відхилення білого Гаусівського шуму $N(0, \sigma_n^2)$, що додається до кожного пікселя зображення незалежно.

3. Параметр розмиття (blur): $\beta \in [0, \beta_{max}]$ де $\beta_{\max} = 5$ пікселів. Параметр β визначає радіус ядра Гаусівського фільтра для моделювання ефектів дефокусування або руху камери.

4. JPEG–стиснення: $Q \in [Q_{min}, 100]$, де $Q_{\min} = 10$. Параметр якості Q визначає коефіцієнт стиснення JPEG, де $Q = 100$ відповідає максимальній якості, а $Q = 10$ – екстремально високому рівню стиснення з видимими артефактами.

5. Параметр кутів повороту (pose variation): $(\theta_{yaw}, \theta_{pitch}, \theta_{roll})$, задається наступними значеннями:

- $\theta_{yaw} \in [-90°, +90°]$ – кут повороту голови відносно вертикальної осі (вліво – право);
- $\theta_{pitch} \in [-45°, +45°]$ – кут нахилу голови відносно горизонтальної осі (вгору – вниз);
- $\theta_{roll} \in [-30°, +30°]$ – кут обертання голови відносно осі погляду.

Модель деградації зображення описується композиційним виразом:

$$I_{in} = D(I_{orig};\ g), g \in G,$$

де $D(\cdot;\ g)$ – оператор деградації, що послідовно застосовує трансформації згідно з вектором параметрів g;

I_{orig} – оригінальне зображення обличчя без деградацій.

Задано також еталонна база даних відкритих джерел:

$$D = \{(I_i^{ref}, id_i)\}_{\{i=1\}}^{N},$$

де I_i^{ref} – еталонні зображення особи;

id_i – унікальний ідентифікатор i-ої особи;

N – загальна кількість осіб в базі даних.

Поріг прийняття рішення $\tau \in \mathbb{R}$ задається як скалярне значення τ, що визначає границю між класами «збіг» та «незбіг» у задачі верифікації. Поріг калібрується на валідаційній множині $D_{dev} = \{(I_j^1, I_j^2, y_j)\}_{j=1}^{M_{dev}}$, де I_j^1, I_j^2 – пара зображень для порівняння, $y_j \in \{0, 1\}$ – мітка істинності ($y_j = 1$ для $genuine$ пари, $y_j = 0$ для $impostor$ пари), M_{dev} – розмірність валідаційної множини.

Поріг $\tau*$ визначається з умови забезпечення заданого рівня False Accept Rate (FAR):

$$\tau* = \arg\max_{\tau}\{\tau :\ FAR(\tau;\ D_{dev}) \leq\ FAR_{target}\},$$

де FAR_{target} – цільовий рівень помилкового прийняття, типово $FAR_{target} \in \{0.1\%, 0.01\%, 0.001\%\}$.

Нижче наведено математична формалізація постановки задачі.

Дано:

1. Вхідне зображення низької якості I_{query} з невідомим ідентифікатором.
2. Еталонна база даних D з N осіб.
3. Граничне значення відстані для верифікації τ.
4. Параметри моделі $\theta = \{\theta_{enh}, \theta_{enc}\}$, де θ_{enh} – параметри модуля підвищення якості, θ_{enc} – параметри енкодера ознак.

Необхідно знайти:

Ідентифікатор особи $id* = \arg\min_{\{id_i \in D\}}$, де $d(f(I_{query}, \theta),\ f(I_i^{ref}, \theta))$, якщо $\min d < \tau$, інакше "особа не ідентифікована", де $f(\cdot, \theta)$: $R^{H \times W \times 3} \to R^d$ – функція перетворення зображення в d-вимірний вектор ознак (embedding), $d(\cdot,\cdot)$ – функція відстані в метричному просторі (косинусна відстань).

Допущення та обмеження (Ω)

Система біометричної верифікації повинна функціонувати в рамках наступних технічних, якісних та операційних обмежень, що визначають простір допустимих рішень Ω.

1. Час обробки одного вхідного зображення має задовольняти умові:

$$t_{proc(\theta)} \leq\ t_{max},$$

де $t_{proc(\theta)} =\ t_{enh(\theta_{enh})} +\ t_{enc(\theta_{enc})}$ – загальний час обробки, що включає час відновлення t_{enh} та час екстракції ознак t_{enc}, t_{max} – максимально допустимий час обробки, як правило $t_{\max}\ \approx\ 5$ секунд для серверних застосувань, $t_{\max}\ \approx\ 100$ мс для мобільних пристроїв реального часу.

2. Система гарантує функціонування тільки для зображень із міжзенічною відстанню не менше критичного значення:

$$R_I \geq\ R_{\min}\ \ =\ 32 \text{ пікселів.}$$

Для $R_I <\ R_{min}$ системи може суттєво деградувати і не гарантується дотримання заданих показників якості. Типові значення R_{min} лежать від архітектури моделі та варіюються в діапазоні [24; 48] пікселів [6].

3. Система повинна функціонувати при рівні Гаусівського шуму:

$$\sigma_n \leq\ \sigma_n, oper\ =\ 50,$$

де σ_n,$oper$ – операційна границя шуму, при перевищенні якої зображення вважається непридатним для надійної верифікації.

4. При рівні Гаусівського шуму $\sigma_n =\ 30$ падіння точності відносно еталоних даних не повинно перевищувати:

$$\Delta TAR_\sigma = 30\ =\ TAR(\theta;\ \tau*, g_{clean}) -\ TAR(\theta;\ \tau*, g_\sigma = 30) \leq\ \Delta TAR_\sigma, max,$$

де $g_\sigma = 30$ – деградація з σ_n = 30, інші параметри відповідають g_{clean}, $\Delta TAR_\sigma, \max = 0.10$ (10 %) – максимально допустиме падіння точності.

Вищенаведене обмеження гарантує, що:

$$TAR(\theta;\ \tau*, g_\sigma = 30) \geq\ TAR(\theta;\ \tau*, g_{clean}) -\ 0.10.$$

При $TAR(\theta;\ \tau*, g_{clean}) =\ 0.85$, що означає $TAR(\theta;\ \tau*, g_\sigma = 30) \geq\ 0.75$.

5. Обмеження деградації точності при нефронтальних ракурсах**.** При кутах повороту голови θ_{yaw} = ±45° (профільні ракурси) падіння точності не повинно перевищувати:

$$\Delta TAR_\theta = \pm 45° = TAR(\theta;\ \tau *, g_{frontal}) - TAR(\theta;\ \tau *, g_\theta = \pm 45°) \leq \Delta TAR_\theta, max,$$

де $g_{frontal}$ – фронтальна орієнтація $(|\theta_{yaw}| \leq 15°), g_\theta = \pm 45°$ – профільна орієнтація з $\theta_{yaw} \in \{-45°, +45°\}$, $\Delta TAR_\theta, \max = 0.15\ (15\%)$ – максимально допустиме падіння точності для профільних ракурсів.

Цільова функція

Метою є знаходження оптимального набору параметрів моделі $\theta * = \{\theta_{enh} *, \theta_{enc} *\}$, за умов дотримання всіх обмежень множини Ω:

$$\theta^* = \arg\max_{\theta \in \Theta} \{\overline{TAR}(\theta)\},$$

де θ^* – оптимальні параметри моделі, що максимізують точність верифікації особи із урахуванням диференційного ракурсу та в умовах деградації вхідних зображень.

Запропоноване рішення AFRW–X (modified). Запропонована методика побудована на основі AFRW-X (Adaptive Face Recognition in the Wild), що складається з п'яти послідовних етапів обробки мінібатчу $B = (I_i, y_i)_{i=1}^{|B|} \subset D,$ де $I_i \in R^{(H \times W \times 3)}$ – вхідне зображення обличчя, $y_i \in \{1, \ldots, C\}$ – мітка класу (ідентифікатор особи).

Для розв'язання задачі ідентифікації особи у відкритих джерелах на основі зображень низької якості з урахуванням диференційного ракурсу та шумових завад запропоновано методику, що інтегрує два ключові модулі: 1-й модуль адаптивної дифузійної фільтрації (Adaptive Diffusion Filtering, ADF) для робастної обробки зображень та ознак, та 2-й модуль псевдо-3D проєкції (Pseudo-3D Projections, PTP) для мультиракурсного злиття векторних представлень даних.

Базова архітектура використовує глибоку згорткову нейронну мережу $F_{BB}(I;\ \Theta) \rightarrow X^l \in R^{(H_l \times W_l \times C_l)}$ із вбудованим механізмом координатної уваги (Coordinate Attention, CA), що забезпечує позиційно-селективну модуляцію ознак при обчислювальній складності $O(H \cdot W \cdot C)$. Нижче наведено загальний алгоритм у вигляді псевдокоду в лістингу 1.

Лістинг 1. Псевдокод алгоритму Adaptive Face Recognition in the Wild under Heavy Noise

Code

 # Algorithm 1 AFRW–X (ADF / PTP): Adaptive Face Recognition in the Wild under Heavy Noise (mod)

Input:

- Dataset D = {(Ii, yi)} – face images and class labels
- Backbone with Coordinate Attention (CA); Adaptive Attention Modulator (AAM)
- V – number of virtual views; T – diffusion iterations; η – diffusion step; κ – edge threshold
- Loss weights: λEQ, λSC, λID, λMV, λLM; β – center update step; λ – center regularizer
- βCB – class–balanced prior parameter (effective–number), τ, mmax – quality weighting

Output:

• Updated weights Θ and class centers $\{cj\}$; aggregated embeddings f* for inference

1: for each minibatch B = {(Ii, yi)} ⊂ D do

2: # === Stage 1: Noise–Aware Image Restoration (ADF–I) ===

3: for each i in B do
4: θi ← EstimateNoise(Ii) ▷ noise type/level (AWGN/Poisson/codec–mix; σ, κ)
5: if θi.type == AWGN and θi.σ ≤ σ0 then
6: Ĩi ← ROF_TV_Denoise(Ii, λTV) ▷ solve $min_u 0.5\left||u - Ii|\right|^2$ + λTV·TV(u)
7: else if θi.type ∈ {moderate mix} then
8: Ĩi ← RED_or_PnP(Ii; Dσ, μ, ρ, nADMM) ▷ Plug–and–Play/RED with denoiser $D\sigma$ as a proximal map
9: else
10: Ĩi ← DPS(Ii; {εt}, nDPS) ▷ Diffusion Posterior Sampling (posterior–consistent restoration)
11: end if
12: LID(i) ← 1 − cos(eT(Ĩi), eT(Ii)) ▷ identity preservation with a fixed ArcFace teacher
13: end for

14: # === ***Stage 2: Pseudo–3D Geometry / View Synthesis (PTP)*** ===
15: for each i in B do
16: (Si, Ri, ti) ← SingleView3D(Ĩi) ▷ 3DDFA–V2 / PRNet / FaceMesh
17: I_i^0 ← RenderCanonical(Si, Rcanon, tcanon) ▷ frontalized view
18: for v = 1..V do
19: (Rv, tv) ← SmallPose(Ri, ti, Δyaw_v, Δpitch_v)
20: I_i^v ← RenderView(Si, Rv, tv) ▷ texture from Ĩi / UV map
21: end for
22: end for

23: # === ***Stage 3: Feature Extraction and Attention–Guided Diffusion (ADF–F)*** ===
24: for each i in B do
25: for all v ∈ {0..V} do
26: Xearly ← Backbone_CA_early(I_i^v) ▷ early backbone stages with CA
27: (Fch, Fsp) ← AAM(Xearly); As := σ(Conv([Avg_c(Xearly), Max_c(Xearly)]))
28: X ← Xearly
29: for t = 1..T do ▷ Perona–Malik diffusion with attention gating
30: ∇X ← SobelGrad(X); G ← As ⊙ g(||∇X||), with $g(s) = \frac{1}{1+\left(\frac{s}{\kappa}\right)^2}$ or $\exp\left(-\left(\frac{s}{\kappa}\right)^2\right)$
31: X ← X + η · div(G ⊙ ∇X)
32: end for
33: Xdeep ← Backbone_CA_late(X) ▷ remaining backbone stages
34: fv ← Head_Embed(Xdeep) ∈ $\mathbb{R}^d$
35: qv ← ||fv|| ▷ quality proxy from feature norm
36: visv ← VisibilityFromZbuffer(I_i^v) ▷ visible–area ratio
37: iouv ← IoU(Det(I^v_i), FaceMask(I_i^v))
38: end for
39: πv ← softmax(α·visv + β·iouv + γ·qv), v=0..V
40: f*_{i} ← $\Sigma_{v} = 0^{V} \pi v \cdot fv$ ▷ multi–view aggregated embedding
41: (logits_i, p_i) ← ArcFaceLike($f*_{\{i\}}, m\left(q = \left|\left|f*_{\{i\}}\right|\right|\right)$) ▷ adaptive margin/weight by quality
42: end for

43: # === ***Stage 4: Losses & Weight Update*** ===
44: LEQ ← 0; LSC ← 0; LMV ← 0; LLM ← 0
45: for each i in B do
46: ωCB(yi) ← (1−βCB) / (1 − βCB^{n_{yi}}) ▷ class–balanced weight (effective number)
47: wQ(i) ← clamp(τ·||f*_{i}||, mmax) ▷ quality–aware weight

48: LEQ ← LEQ − wQ(i)·ωCB(yi)·log(p_i[yi]) ▷ equilibrium / class–balanced CE
49: xi ← PreLogitFeature(Xdeep) ▷ feature used by center–loss
50: αi ← σ(Conv(AAM_maps_i)) ∈ [0,1] ▷ sparsity/attention weight
51: LSC ← LSC + 0.5 · αi · || xi − c_{yi} || ² ▷ Sparse Center Loss
52: LMV ← LMV + $(1/(V(V+1)))\ \cdot\ \Sigma\_\{u<v\}\ (1-\cos(\ f_{\{i,u\}}\}\}=, f\_\{i,v\}\ ))$
53: LLM ← LLM + LandmarkReprojLoss(Ĩi, Si, {lmk_i})
54: end for
55: LID ← Σ_{i∈B} LID(i)
56: L ← λEQ·(LEQ/|B|) + λSC·(LSC/|B|) + λID·(LID/|B|) + λMV·(LMV/|B|) + λLM·(LLM/|B|)
57: Θ ← Optimizer.step(∇_Θ L) ▷ backprop through all modules

58: # === ***Stage 5: Sparse / Attention–Weighted Center Update*** ===
59: for each class j do
60: num ← Σ_{i∈B: yi=j} αi · (cj − xi)
61: den ← Σ_{i∈B: yi=j} + λ
62: Δcj ← num / den
63: cj ← cj − β · Δcj
64: end for
65: end for

66: Return Θ, {cj}

На вхід алгоритму подається датасет $D = (I_i, y_i)$, базова мережа F_{BB} із вбудованими механізмами кординатної увагм (CA) та адаптивний механізм уваги (AAM), параметри: V – кількість віртуальних ракурсів; T – кількість ітерацій дифузії; η – крок дифузії; κ – поріг збереження ознак; вагові коефіцієнти функції втрат $\{\lambda_{EQ}, \lambda_{SC}, \lambda_{ID}, \lambda_{MV}, \lambda_{LM}\}$, λ_{EQ} – коефіцієнт втрат рівноваги (Equilibrium Loss), що регулює пріоритет основної задачі класифікації з урахуванням балансування класів та якості зразків; λ_{SC} – коефіцієнт втрат розрідженого центрування (Sparse Center Loss), для контролю розмірності векторних представлень у просторі ознак; λ_{ID} – коефіцієнт втрат збереження ідентичності, що штрафує модуль відновлення (ADF-I) за спотворення біометричних рис під час очищення зображення; λ_{MV} – коефіцієнт втрат міжвидової узгодженості (Multi-View Loss), для забезпечення інваріантності до ракурсу шляхом мінімізації розбіжностей між віртуальними проєкціями (PTP); λ_{LM} – коефіцієнту втрат репроєкції ландмарків для контролю геометричної точності та адекватності псевдо-3D реконструкції; β – крок оновлення центрів класів; λ – параметр регуляризації центрів; β_{CB} – гіперпараметр, що використовується для розрахунку ефективної кількості зразків (*effective number*) в методі класово-збалансованого навчання; τ, m_{max} – параметри зважування з урахуванням якості.

Методика AFRW-X (modified) складається з наступних етапів.

Етап 1. Адаптивно відновлення зображень з урахуванням типу завад (ADF-I). На першому етапі для кожного I_i-го зразка з мінібатчу B виконується оцінка параметрів шуму $\hat{\theta}_i \leftarrow \text{EstimateNoise}(I_i)$, що включає визначення типу деградації (адитивний гаусівський шум AWGN, пуассонівський шум, артефакти стиснення зображення) та рівня спотворення, таких як: стандартне відхилення σ для AWGN, параметр κ для інших типів. На основі виявленого типу деградації вибирається відповідний метод відновлення:

Так, для випадку впливу помірного адитивного гаусівського шуму застосовується метод на основі повної варіації $\tilde{I}_i \leftarrow ROF_{TV_{Denoise}}(I_i, \lambda_{\{TV\}})$. Також метод розв'язує задачу оптимізації, що наведено в рівнянні (1) [18]:

$$\min_u \left\{ \left(\frac{1}{2}\right) ||u - I_i||^2 + \lambda_{\{TV\}} \cdot TV(u) \right\}, \quad (1)$$

де $TV(u) = \sum_p ||\nabla u(p)||^2$ – функціонал повної варіації; $\lambda_{\{TV\}} > 0$ – параметр балансування між відповідністю вхідному зображенню та помилковому рішення. Розв'язання здійснюється ітеративно методом split-Bregman [18] або ADMM [19] (Alternating Direction Method of Multipliers), що забезпечує збіжність до локального мінімума при збереженні різких країв обличчя.

Для випадку змішаних деградацій помірної складності $\hat{\theta}_i.type \in \{moderate\ mix\}$ застосовується Plug-and-Play [20], ADMM або метод Regularization by Denoising [21]: $\tilde{I}_i \leftarrow RED\_or_{PnP(I_i; D_\sigma, \mu, \rho, n_{\{ADMM\}})}$), де $D_{\sigma(\cdot)}$ – попередньо навчений денойзер DnCNN [22], що використовується як проксимальний оператор в ітераційній схемі ADMM; μ – параметр штрафу; ρ – параметр аугментованого лагранжіана; $n_{\{ADMM\}}$ – кількість ітерацій. У методі RED регуляризація задається як $R(x) = \left(\frac{1}{2}\right) x^{T(x - D(x))}$, що дозволяє використовувати довільний денойзер без явного формулювання функціоналу регуляризації.

У випадку складних або змішаних деградацій застосовується Diffusion Posterior Sampling (DPS) [23], що виконує ітеративний процес зворотної дифузії з узгодженням і вимірюванням: $x_{\{t-1\}} = x_t + \varepsilon_t\left(s_{\theta(x_t,t)} + \nabla_x \log p(y|x_t)\right) + \sqrt{2\varepsilon_t} \cdot \xi_t$, де $s_{\theta(x_t,t)}$ – функція преднавченої дифузійної моделі; $\nabla_x \log p(y|x_t)$ – градієнт логарифма правдоподібності спостереження відносно поточного стану; $\xi_t \sim N(0, I)$ – гаусівський шум; $\{\varepsilon_t\}$ – розклад кроків дифузії; $n_{\{DPS\}}$ – кількість кроків зворотної дифузії. Метод DPS забезпечує узгодженість з вимірюванням при збереженні відновленого зображення завдяки дифузійної моделі.

На основі отриманих карт ранніх ознак X_{early} модуль агрегації уваги (AAM) генерує два компоненти: канальну увагу F_{ch} та просторову увагу F_{sp}. Компонент канальної уваги обчислюється шляхом агрегації глобального усередненого та глобального максимального пулінгу, які обчислюються на рівні повнозв'язної архітектури нейромережі з функцією активації ReLU $F_{ch}(X) = \sigma\left(W_2 \cdot \mathrm{ReLU}(W_1 \cdot [\mathrm{GAP}(X), \mathrm{GMP}(X)])\right)$.

Паралельно для керування процесом дифузії формується окрема маска просторової уваги $A_s \in (0,1)^{H_1 \times W_1}$ шляхом застосування згортки та сигмоїдної функції для конкатенації усереднених та максимальних ознак. Після відновлення зображення оцінюється ступінь збереження ідентичності особи. Для цього використовується попередньо навчений енкодер на основі архітектури ArcFace, який відображає зображення обличчя у простір ознак розмірності 512. Втрати обчислюються як косинусна відстань між векторами оригінального та відновленого зображень, що відображає міру схожості ідентичності.

Етап 2. **Тривимірна реконструкція моделі обличчя.** На другому етапі для кожного i-го відновленого зображення виконується однокадрова 3D-реконструкція обличчя $(S_i, R_i, t_i) \leftarrow SingleView3D(\tilde{I}_i)$, де S_i – 3D-сітка обличчя (форма та текстура); $R_i \in SO(3)$ – матриця обертання (поза голови); $t_i \in \mathrm{R}^3$ – вектор зміщення. Реконструкція може виконуватися одним із трьох методів залежно від вимог до точності та швидкості обробки. Метод 3DDFA-V2 [23] використовує регресію параметрів морфологічної моделі обличчя на легкій згортковій мережі, забезпечуючи баланс між швидкістю та точністю. Метод PRNet [24] виконує регресію позиційної карти для отримання щільної геометрії ракурсів зображень без явного використання морфологічної моделі. Для задач реального часу на мобільних пристроях може застосовуватися MediaPipe FaceMesh [25] для отримання 468 тривимірних ландмарків обличчя.

На основі отриманої 3D-моделі виконується рендеринг канонічного фронтального виду $I_i^{(0)} \leftarrow \mathrm{RenderCanonical}(S_i, R_{canon}, t_{canon})$, де R_{canon} – канонічна матриця обертання

(фронтальна поза з нульовими кутами $(yaw, pitch, roll)$; t_{canon} – канонічне зміщення, тобто центрування обличчя в кадрі. Фронталізація усуває варіативність, пов'язану з позою голови та підвищує стабільність розпізнавання в неконтрольованих умовах.

Також додатково відбувається генерація набору віртуальних ракурсів обличчя $\{I_i^v\}_{\{v=1\}}^{V}$ шляхом застосування невеликих відхилень від канонічної пози. Для кожного віртуального виду $v \in \{1, \dots, V\}$ обчислюються модифіковані параметри пози $(R_v, t_v) \leftarrow SmallPose(R_i, t_i, \Delta yaw_v, \Delta pitch_v)$, де $\Delta yaw_v, \Delta pitch_v \in [-15°, +15°]$ – випадкові або фіксовані кутові відхилення навколо вертикальної та горизонтальної осей, після чого виконується рендеринг $I_i^v \leftarrow RenderView(S_i, R_v, t_v)$, де текстура береться з відновленого зображення.

Етап 3. Екстракція ознак з керованою дифузійною фільтрацією. На третьому етапі для кожного i-го зразка даних та кожного виду множини $v \in \{0, \dots, V\}$ виконується екстракція глибоких ознак з одночасною дифузійною фільтрацією проміжних карт. Процес починається з обробки зображення I_i^v на рівні базової згорткової нейромережі $X_{\{early\}} \leftarrow \text{Backbone}_{\text{CA}_{\text{early}}}(I_i^v))$, що включає перші згорткові блоки з вбудованим механізмом Coordinate Attention, в результаті чого отримуються карти ранніх ознак $X_{\{early\}} \in R^{H^1 \times W^1 \times C^1}$.

На етапі постобробки (після відновлення) оцінюється ступінь збереження ідентичності за допомогою функції втрат L_{ID}. В основі L_{ID} лежить порівняння ембедингів, згенерованих енкодером ArcFace $e_T(\cdot)$, який відображає обличчя у 512-вимірний простір ознак. Функція втрат, $L_{ID}(i) = 1 - \cos\left(e_T(\tilde{\text{I}}_i), e_T(I_i)\right)$, є по суті косинусною відстанню між векторами оригінального I_i та відновленого $\tilde{\text{I}}_i$ зразків зображення.

На основі карт ранніх ознак модуль агрегації уваги генерує два компоненти. Перший компонент канальної уваги F_{ch} базується на агрегації пулінгів (2):

$$F_{ch}(X) = \sigma\big(W_2 \cdot \text{ReLU}(W_1 \cdot [\text{GAP}(X), \text{GMP}(X)])\big) . \quad (2)$$

Паралельно формується окрема маска компонента просторової уваги A_s, яка буде використана для керування дифузією. Отримана маска $\in (0,1)^{H_1 \times W_1}$ є результатом згортки та сигмоїди, застосованих до конкатенованих середніх та максимальних значень відносно каналів зображення, що наведено в рівнянні (3):

$$A_s \coloneqq \sigma\left(\text{Conv}\left(\left[\text{Avg}_c\left(X_{early}\right), \text{Max}_c\left(X_{early}\right)\right]\right)\right). \quad (3)$$

Наступним етапом відбувається ітеративна анізотропна дифузія на картах ознак X протягом T кроків. На кожній ітерації $t \in 1, \dots, T$ обчислюється градієнт карт ознак $\nabla X \leftarrow SobelGrad(X)$ за допомогою оператора Собеля [26]. Далі формується просторово-адаптивний коефіцієнт дифузії на основі маски уваги та функції зупинки на краях зображення $G = A_s \odot g\left(||\nabla X||\right)$, де $g(s) = \frac{1}{1+\left(\frac{s}{\kappa}\right)^2}$ – *edge-stopping* функція, що зменшує дифузію в областях із сильними градієнтами текстури; κ – адаптивний поріг; $\odot -$ оператор поелементного векторного добутку.

Оновлення карт ознак виконується за схемою $X \leftarrow X + \eta \cdot div(G \odot \nabla X)$, де $div(\cdot)$ – оператор дивергенції; η – крок дифузії. Наведена операція зменшує дифузію в областях з сильними градієнтами, таких як краї обличчя та текстурні елементи, зберігаючи важливі деталі.

Після етапу дифузійної фільтрації, карти ознак X подаються на решту рівнів базової мережі $X_{\{deep\}} \leftarrow \text{Backbone}_{\text{CA}_{\text{late}}}(X)$, що включають глибокі згорткові блоки, такі як pooling

рівні та механізми уваги. Далі відбувається процес формування кінцевого векторного представлення для виду v, що формується як $f_v \leftarrow$ Head_Embed($X_{\{deep\}}$) $\in R^d$, де d – розмірність векторного простору.

Додатково для кожного виду обчислюються характеристики якості для векторного представлення як проксі-метрика, $vis_v \leftarrow$ VisibilityFromZbuffer(I_i^v) – частка видимих вершин 3D-сітки, $iou_v \leftarrow$ IoU(Det(I_i^v), FaceMask(I_i^v)) – коефіцієнт перекриття між детекцією обличчя та маскою в 3D-моделі.

Для адаптивного керування геометричними (vis_v, iou_v) та якісними (q_v) характеристиками зображення застосовується мультиракурсне злиття, яке виконується шляхом обчислення нормалізованих вагових коефіцієнтів за допомогою функції $softmax$:

$$\pi_v = softmax(\alpha \cdot vis_v + \beta \cdot iou_v + \gamma \cdot q_v),$$

де α, β, γ – вагові гіперпараметри.

Інтегральне векторне представлення зображення формується як зважена комбінація $f_i * = \sum_{\{v=0\}}^{V} \pi_v \cdot f_v$, що забезпечує робастність до варіацій ракурсу та якості окремих видів. Далі інтегральне представлення подається на рівень класифікації енкодеру ArcFace-типу ($logits_i, p_i$) $\leftarrow$ ArcFaceLike($f_i *$, m(q=$\|f_i *\|$)), де $m(q)$ – адаптивна маржа або вагові коефіцієнти, що залежать від якості представлення q = $\|f_i *\|$, $p_i \in R^C$ – вектор ймовірностей належності до класу C.

Етап 4. Обчислення компонентів функції втрат та оновлення вагових коефіцієнтів мережі. На четвертому етапі обчислюються п'ять компонентів загальної функції втрат для мінібатчу B. Спочатку виконується ініціалізація аргегаторів для кожного компонента втрат: $L_{\{EQ\}} \leftarrow 0, L_{\{SC\}} \leftarrow 0, L_{\{MV\}} \leftarrow 0, L_{\{LM\}} \leftarrow 0$.

Компонент балансування класів. Для кожного i-го зразка $\in B$ обчислюється ваговий коефіцієнт балансування класів:

$$\omega_{\{CB\}(y_i)} = \frac{1-\beta_{\{CB\}}}{1-\beta_{\{CB\}}^{\{n_{\{y_i\}}\}}}, \quad (4)$$

де $n_{\{y_i\}}$ – кількість зразків класу y_i в повному датасеті D; $\beta_{\{CB\}} \in (0.999, 0.9999)$ – гіперпараметр, що контролює ступінь балансування. Додатково обчислюється $quality-aware$ ваговий коефіцієнт $w_{Q(i)} = clamp(\tau \cdot \|f_i *\|, m_{\{max\}})$, де τ – множник маштабування (як правило $\tau \in$ [1.0, 2.0]), $m_{\{max\}}$ – верхня межа вагового коефіцієнта ($m_{\{max\}} = 2.0$), $clamp(\cdot,\cdot)$ – операція обмеження значення зверху. Компонент $Equilibrium\ Loss$ обчислюється як $L_{\{EQ\}} \leftarrow L_{\{EQ\}} - w_{Q(i)} \cdot \omega_{\{CB\}(y_i)} \cdot \log\left(p_{i[y_i]}\right)$, де $p_{i[y_i]}$ – прогнозована ймовірність правильного класу y_i.

Компонент центрування класів. Процес обчислення Sparse Center Loss передбачає початкове формування проміжного векторного представлення $x_i \leftarrow \mathrm{PreLogitFeature}\left(X_{\mathrm{deep}}\right)$ з останнього повнозв'язного рівня нейромережевої архітектури. Наступним кроком обчислюється ваговий коефіцієнт уваги $\alpha_i = \sigma\left(\mathrm{Conv}\left(\mathrm{AAM}_{\mathrm{mapsi}}\right)\right) \in [0,1]$, де$\mathrm{AAM}_{\mathrm{mapsi}}$ являють собою карти уваги з механізму AAM для i-го зразка, $\mathrm{Conv} - 1 \times 1$ згортка з функцією активації $\mathrm{sigmoid}$, для перетворення просторової інформації в скалярний ваговий коефіцієнт.

Компонент втрат центрів визначається як $L_{SC} \leftarrow L_{SC} + (1/2) \cdot \alpha_i \cdot |x_i - c_{y_i}|^2$, де $c_{y_i} \in R^d$ – поточний центр класу y_i, який зберігається в пам'яті та оновлюється за принципом експоненційного згладжування.

Компонент втрат міжвидової узгодженості (Inter-view consistency loss) обчислюється за наступним виразом (5):

$$L_{MV} \leftarrow L_{MV} + \frac{1}{V(V+1)} \cdot \sum_{u<v}\left(1 - \cos\left(f_{i,u}, f_{i,v}\right)\right), \quad (5)$$

де операція суми відбувається по всіх парах (u, v) віртуальних ракурсів за умови $u < v$. Такий підхід формує близькі векторні представлення для різних видів однієї особи.

Коефіцієнт нормалізації, що представлений як $\frac{1}{V(V+1)} = \frac{1}{V \cdot (V+1)/2}$, який враховує кількість унікальних пар.

Компонент репроєкційних втрат ландмарків обчислюється як $L_{LM} \leftarrow L_{LM} + \text{LandmarkReprojLoss}\left(\widetilde{I_i}, S_i, \{lmk_i\}\right)$, де $\{lmk_i\}$ – набір 2D-ландмарків, детектованих на вхідному зображенні. Функція втрат вимірює середньоквадратичну помилку між детектованими ландмарками та репроєкцією відповідних 3D-точок на сонові S_i – ї моделі на площину зображення, що описується наступним виразом (6):

$$\text{LandmarkReprojLoss} = \frac{1}{N_{lmk}} \cdot \sum_{j=1}^{N_{lmk}} |lmk_i^{(j)} - \Pi\left(S_i^{(j)}, R_i, t_i\right)|_2^2, \quad (6)$$

де N_{lmk} – кількість ландмарків; $\Pi(\cdot)$ – оператор проєкції 3D-точки на 2D-площину.

Після етапу обробки всіх зразків батчу обчислюється компонент втрат збереження ідентичності як сума по батчу $L_{ID} = \sum_{i \in B} L_{ID}(i)$, де $L_{ID}(i)$, що було показано на етапі 1.

Загальна функція втрат L формується наступним чином (7):

$$L = \lambda_{EQ} \cdot \frac{L_{EQ}}{|B|} + \lambda_{SC} \cdot \frac{L_{SC}}{|B|} + \lambda_{ID} \cdot \frac{L_{ID}}{|B|} + \lambda_{MV} \cdot \frac{L_{MV}}{|B|} + \lambda_{LM} \cdot \frac{L_{LM}}{|B|} \quad (7)$$

де $|B|$ – розмір мінібатчу; $\{\lambda_{EQ}, \lambda_{SC}, \lambda_{ID}, \lambda_{MV}, \lambda_{LM}\}$ – вагові гіперпараметри, що балансують внесок кожного компонента.

Наступний крок – зворотне поширення помилки та оновлення параметрів нейронної мережі, яке відбувається на основі стохастичного градієнтного спуску, що відображено у виразі (8):

$$\Theta \leftarrow \text{Optimizer.step}(\nabla_\Theta L), \quad (8)$$

де Optimizer – алгоритм оптимізації стохастичний градієнтний спуск SGD з моментом; $\nabla_\Theta L$ – градієнт загальної функції втрат по всіх параметрах мережі (вагові коефіцієнти бекбону, механізмів уваги).

Етап 5. Оновлення центрів класів. На п'ятому етапі відбувається процес оновлення центрів класів $\{c_j\}_{j=1}^{C}$ з урахуванням вагових коефіцієнтів уваги α_i, що забезпечує більшу стійкість до шумових або неінформативних зразків. Для кожного класу $j \in \{1, \ldots, C\}$ обчислюється зважений градієнт оновлення, що наведено нижче у рівнянні (9):

$$\text{num} = \sum_{i \in B: y_i = j} \alpha_i \cdot \left(c_j - x_i\right), \quad (9)$$

де операція сума застосовується виключно до зразків батчу B, що належать j-го класу, що наведено в рівнянні (10):

$$\text{den} = \sum_{i \in B: y_i = j} \alpha_i + \lambda, \tag{10}$$

де $\lambda > 0$ – параметр регуляризації, що запобігає діленню на нуль та стабілізує оновлення для класів з малою кількістю зразків у батчі.

Крок оновлення центру обчислюється як $\Delta c_j = \text{num}/\text{den}$, після чого виконується експоненційне згладжування $c_j \leftarrow c_j - \beta \cdot \Delta c_j$, де $\beta \in (0,1)$ – швидкість оновлення центрів для забезпечення стабільної конвергенції без різких стрибків.

Таким чином, оновлення центрів із розрідженим зважуванням дозволяє адаптивно зменшити вплив низькоякісних зразків даних на позицію центру класу, що підвищує внутрішньокласову компактність репрезентативних зразків вхідних даних та робастність до шуму. На відміну від класичного Center Loss, де всі зразки мають однаковий вплив, запропонований механізм зважування за допомогою карти уваги AAM може забезпечувати більш точну локалізацію центрів класів у просторі ознак.

Після завершення всіх етапів для поточного мінібатчу алгоритм повторюється для наступного батчу. Процес навчання продовжується до досягнення збіжності за метрикою валідації або до виконання заданої кількості епох. Критерієм збіжності є показник правильного прийняття рішення при фіксованому показнику помилкового прийняття на валідаційній множині.

Експеримент. Експериментальне дослідження спрямоване на комплексну верифікацію запропонованого методу AFRW-X (mod) шляхом порівняльного аналізу з чотирма базовими методами: DeepFace, FaceNet, ArcFace, AFRW-X (original) за умов множинної деградації вхідних зображень, характерних для OSINT-сценаріїв.

Усі експерименти проводилися у хмарному середовищі Google Colab (тарифи Pro) із застосуванням GPU-прискорювачів NVIDIA A100 80 GB та конфігурації High-RAM, обсяг оперативної пам'яті становив 64 GB.

З метою забезпечення відтворюваності результатів версії всіх пакетів зафіксовано у коді ноутбука; використовувався інтерпретатор Python 3.12.

У роботі застосовувались наступні фреймворки: PyTorch 2.8.0+cu126, TensorFlow 2.19.0 Keras 3.10.0, OpenCV 4.12.0. Для побудови 3D-геометрії обличчя застосовано 3DDFA-V2 і MediaPipe Face Mesh з 468 тривимірними landmarks, для відновлення якості зображень застосовувалась бібліотека scikit-image алгоритм Total Variation denoising, а також власні імплементації методів PnP-ADMM і DPS.

Навчальні датасети розміщувалися на Google Drive із підключенням до Colab-середовища; проміжні чекпойнти моделей зберігалися у локальному сховищі віртуальної машини.

Система оцінки ефективності моделі верифікації побудована на основі композиції незалежних цільових функцій, кожна з яких характеризує окремий аспект якості системи біометричної ідентифікації.

1. Інтегральна цільова функція визначається як зважена лінійна комбінація основного критерію якості та регуляризуючих штрафних параметрів:

$$L_{eval}(\theta) = L_{primary}(\theta) + \sum_{i=1}^{4} \lambda_i \cdot Pen_i(\theta),$$

де $L_{primary}(\theta) = 1 - \overline{TAR}(\theta)$ – первинна функція втрат, що відображає помилку верифікації; $Pen_i(\theta)$ – штрафні функції за порушення експлуатаційних обмежень; $\lambda_i \in R_+$ – вагові коефіцієнти регуляризації, $i = \overline{1,4}$.

2. Для забезпечення стійкості системи до гаусівського шуму, характерного для зображень із низькоякісних сенсорів та в умовах слабкої освітленості, вводиться функція штрафу робастності $Pen_\sigma(\theta)$ до адитивного шуму

$$Pen_\sigma(\theta) = \max\{0, \Delta TAR_{\sigma=30}(\theta) - \Delta TAR_{\sigma,max}\}^2,$$

де $\Delta TAR_{\sigma=30}(\theta) = TAR(\theta; \tau' g_{\text{clean}}) - \text{TAR}(\theta; \tau' g_{\sigma=30})$ – фактичне падіння точності при рівні шуму $\sigma_n = 30$; $\Delta TAR_{\sigma,max} = 0.10$ – допустимий поріг деградації точності; квадратична форма штрафу забезпечує експоненційне зростання при критичних порушеннях.

3. Функція штрафу інваріантності до зміни ракурсу визначає чутливість моделі до поворотів обличчя в умовах впливу різнорідних шумів:

$$Pen_\theta(\theta) = \max\{0, \Delta TAR_{\theta=\pm45^\circ}(\theta) - \Delta TAR_{\theta,max}\}^2,$$

де $\Delta TAR_{\theta=\pm45^\circ}(\theta) = \frac{1}{2}\left[TAR\left(\theta; g_{frontal}\right) - TAR(\theta; g_{\theta=-45^\circ}) + TAR\left(\theta; g_{frontal}\right) - TAR(\theta; g_{\theta=+45^\circ})\right]$ – середнє падіння точності для лівого та правого профілів відносно фронтального ракурсу; $\Delta TAR_{\theta,max} = 0.15$ – допустимий поріг варіативності.

4. Також для забезпечення рівномірної якості розпізнавання в широкому діапазоні роздільної здатності до вхідних зображень від низької до високої якості, необхідно вести функцію штрафу інтегральної точності за роздільною здатністю

$$Pen_R(\theta) = 1 - AUC_R(\theta) = 1 - \frac{1}{K}\sum_{k=1}^{K} TAR\left(\theta; \tau^*, g_{R_k}\right),$$

де $R_k \in R_{min}, R_{min} + \Delta R, \dots, R_{max}$ – дискретний набір міжзіничних відстаней; K – кількість точок дискретизації діапазону; $\Delta R = (R_{max} - R_{min})/(K-1)$ – крок дискретизації; g_{R_k} – деградація з фіксованою роздільною здатністю R_k при номінальних значеннях інших параметрів.

Вагові коефіцієнти визначають баланс між конкуруючими цілями оптимізації та встановлюються згідно з експлуатаційними пріоритетами: $\lambda_\sigma = 2.0$, $\lambda_\theta = 1.5$, $\lambda_R = 1.0$, $\lambda_t = 0.5$. Ієрархія пріоритетів відповідно цільової задачі представлено нижче :

1. Робастність до шуму $\lambda_\sigma = 2.0$ – вищий пріоритет, обумовлений функціонуванням в умовах низької якості вхідних даних.

2. Інваріантність до ракурсу $\lambda_\theta = 1.5$ – другий за важливістю фактор, визначає придатність для неконтрольованих умов реєстрації.

3. Інтегральна точність $\lambda_R = 1.0$ – базовий пріоритет, що відображає загальну якість системи в номінальних умовах.

Така система коефіцієнтів забезпечує збалансований компроміс між якістю розпізнавання та експлуатаційними характеристиками системи біометричної верифікації.

Для забезпечення комплексної оцінки ефективності досліджуваних методів використовувалися чотири еталонні датасети, що охоплюють різні аспекти варіативності обличь у неконтрольованих умовах. Вибір датасетів здійснювався з урахуванням їх доступності через відкриті репозиторії (Kaggle, офіційні дзеркала) та узгодженості з сучасними протоколами оцінювання систем розпізнавання обличь. Детальна характеристика використаних датасетів представлена в таблиці 1.

Таблиця 1

Характеристика датасетів для навчання та тестування

Датасет	Джерело	Кількість осіб	Загальна кількість зображень
VGGFace2–train	Kaggle.	9,131	3.31M
CelebA	Kaggle	10,177	202,599
LFW	Kaggle	5,749	13,233
VGGFace2–test	Kaggle subset	500+	~10k

VGGFace2-train [26] – масштабний датасет, що містить 3,31 мільйона зображень 9,131 особи з високою інтракласовою варіативністю (різні пози, освітлення, вік, етнічність). Зображення попередньо оброблені та нормалізовані до роздільної здатності 112×112 пікселів для ефективного навчання. Розбиття на навчальну та валідаційну множини здійснювалося у співвідношенні 80/20 на рівні ідентичностей для запобігання data leakage.

CelebA [27] – датасет з 202,599 зображень обличь 10,177 знаменитостей, що містить детальні анотації атрибутів та положення ключових точок обличчя. Використовувався як додаткове джерело для покращення генералізації моделі та роботи з довгим хвостом розподілу класів. Файл identity_CelebA.txt застосовувався для встановлення відповідностей між зображеннями та ідентичностями.

LFW (Labeled Faces in the Wild) [28] – еталонний бенчмарк для оцінки алгоритмів верифікації обличь, що містить 13,233 зображення 5,749 осіб, зібраних із неконтрольованих джерел. Стандартний протокол оцінювання включає 6,000 пар зображень (3,000 genuine пар та 3,000 impostor пар) для обчислення метрик верифікації. Датасет використовувався як для базової оцінки на еталонних зображеннях, так і для конструювання LQI-версій із синтетичними деградаціями.

VGGFace2-test [29] – тестовий піднабір VGGFace2, що містить приблизно 10,000 зображень 500 та осіб із урахуванням впливу в особливо складними умовами реєстрації (екстремальні пози, оклюзії, нерівномірне освітлення). Використовувався для крос-датасетної валідації та оцінки робастності до варіацій, не представлених у навчальних даних.

Експеримент 1. Вплив роздільної здатності зображення на точність розпізнавання.

Мета експерименту – визначення залежності точності верифікації обличь від міжзіничної відстані (IPD) для систематичної оцінки робастності методів до зменшення просторової роздільної здатності вхідних зображень.

Оцінювання ефективності методів розпізнавання обличь здійснювалося відповідно до протоколів, узгоджених із міжнародними стандартами оцінювання біометричних систем (NIST FRVT, IARPA Janus Benchmark) [30]. Такий підхід забезпечує процес порівняння результатів з опублікованими дослідженнями та відповідність вимогам до практичного застосування систем у реальних умовах.

Основна метрика оцінювання – True Accept Rate (TAR). Тестові зображення з датасетів LFW та IJB-C послідовно змінювались до цільових значень $IPD \in \{32, 48, 64, 80, 96, 112, 128\}$ пікселів із використанням бікубічної інтерполяції з антиаліасинговим фільтром Ланцоша [31]. Для кожного значення IPD обчислювалася метрика $TAR@FAR = 0{,}01\%\ (10^{-4})$ на стандартних протоколах верифікації. Процедура включала: детекцію ключових точок обличчя за допомогою каскадного регресора; визначення міжзіничної відстані; нормалізацію до цільового IPD на основі геометричної операції афінного перетворення; обчислення за метрикою similarity та TAR при фіксованому FAR.

Результати експерименту представлено в таблиці 2.

Таблиця 2

Точність розпізнавання залежно від роздільної здатності (TAR@FAR = 0,01 %)

IPD (px)	DeepFace	FaceNet	ArcFace	AFRW	AFRW-X(orig)	AFRW-X(mod)
128	94,2 %	96,8 %	97,5 %	96,5 %	95,8 %	**97,8 %**
112	91,8 %	95,2 %	96,9 %	95,1 %	95,1 %	**97,2 %**
96	87,3 %	92,6 %	95,5 %	92,8 %	93,2 %	**96,1 %**
80	81,5 %	88,4 %	93,2 %	89,4 %	89,3 %	**94,3 %**
64	73,8 %	82,7 %	89,6 %	84,2 %	84,7 %	**91,7 %**
48	62,4 %	74,3 %	83,8 %	76,8 %	76,8 %	**87,5 %**
32	48,7 %	63,5 %	75,2 %	65,3 %	65,4 %	**80,2 %**
AUC_R	**77,1**	**84,8**	**90,2**	**85,7**	**85,7**	**92,1**
ΔTAR	**–45,5**	**–33,3**	**–22,3**	**–31,2**	**–30,4**	**–17,6**

Із таблиці видно, що запропонований модифікований метод AFRW-X (modified) показує суттєве покращення точності розпізнавання обличь порівняно з базовими підходами в умовах різних рівнів шумового впливу вхідних зображень. Комплексна серія експериментів на тестових наборах показала наступні результати: за відсутності шуму ($\sigma_n = 0$) метод досягає точності розпізнавання 94,3 %, що на 1,1 процентних пункти перевищує показники базового методу ArcFace, який продемонстрував точність 93,2 %. При помірному рівні шуму ($\sigma_n = 30$) запропонований підхід забезпечує точність 87,4 %, що складає приріст на 1,6 % над ArcFace (85,8 %) та показує значне покращення на 6,9 % порівняно з оригінальною версією AFRW-X (80,5 %). Також важливим показником є відносне зменшення точності при переході від ідеальних умов до середнього рівня зашумлення.

Таким чином, показник метрики ΔTAR = –6,9 % задовольняє встановлену вимогу про допустимий рівень деградації не більше 10 %, що свідчить про високу робастність методу. При високому рівні шуму ($\sigma_n = 50$) метод зберігає працездатність на рівні 75,3 % точності.

Експеримент 2. Вплив адитивного гаусівського шуму на точність розпізнавання.

Мета експерименту – оцінка стійкості досліджуваних методів до адитивного білого гаусівського шуму, характерного для зйомки в умовах слабкого освітлення з використанням високих значень ISO сенсора камери.

До еталонних тестових зображень із фіксованою роздільною здатністю $R = 80px$ IPD додавався гаусівський шум зі стандартним відхиленням $\sigma_n \in \{0,10,20,30,40,50\}$. Шум генерувався як $n(x,y) \sim N(0,\sigma_n^2)$ та додавався до нормалізованих зображень $I \in [0,1]$: $I_{noisy(x,y)} = clip\big(I_{orig(x,y)} + n(x,y), 0, 1\big)$. Параметр $\sigma_n = 30$ відповідає критичному рівню згідно з обмеженнями формалізації задачі, а $\sigma_n = 50$ моделює екстремальні умови $low - light\ photography$ (еквівалент ISO > 6400).

Результати експерименту представлено в таблиці 3.

Таблиця 3

Точність розпізнавання залежно від рівня гаусівського шуму

σ_n	DeepFace	FaceNet	ArcFace	AFRW	AFRW-X(orig)	AFRW-X(mod)
0	81,5 %	88,4 %	93,2 %	89,4 %	89,3 %	**94,3 %**
10	78,3 %	85,9 %	91,5 %	86,7 %	87,6 %	**93,1 %**
20	72,8 %	81,7 %	88,3 %	82,5 %	84,7 %	**90,8 %**
30	65,2 %	76,3 %	85,8 %	76,9 %	80,5 %	**87,4 %**
40	55,7 %	69,5 %	81,2 %	69,3 %	74,8 %	**82,6 %**
50	44,9 %	60,8 %	74,6 %	59,8 %	67,3 %	**75,3 %**
ΔTAR_{30}	**–16,3**	**–12,1**	**–7,4**	**–12,5**	**–8,8**	**–6,9**

Результати експерименту 2 (табл. 2) підтверджують суттєву перевагу запропонованого методу AFRW-X (modified) в умовах адитивного гаусівського шуму, оскільки при нульовому

шумі ($\sigma = 0$) він демонструє найвищу точність 94,3 %, перевершуючи ArcFace (93,2 %) та AFRW-X(orig) (89,3 %); при значному рівні шуму ($\sigma = 30$) запропонований метод зберігає точність 87,4 %, що вище за ArcFace (85,8 %) та значно краще за AFRW-X(orig) (80,5 %); ключовим показником є відносне падіння точності ΔTAR_{30}, яке для AFRW-X (modified) становить лише –6,9 %, що робить його єдиним методом, який задовольнив цільове обмеження робастності $\Delta \leq 10$ %, на відміну від ArcFace (–7,4 %) та DeepFace (–16,3 %); навіть в екстремальних умовах шуму $\sigma = 50$ модифікований метод зберігає відносно кращу працездатність (75,3 %), підтверджуючи ефективність інтегрованих модулів фільтрації.

Експеримент 3. Вплив варіації ракурсу на точність розпізнавання.

Мета експерименту – оцінка інваріантності досліджуваних методів до зміни просторової орієнтації обличчя (*yaw rotation*) для перевірки робастності до нефронтальних ракурсів, типових для OSINT-зображень.

Варіація ракурсу моделювалася шляхом синтезу віртуальних видів на основі однокадрової 3D-реконструкції обличчя з використанням методу 3DDFA-V2 (3D Dense Face Alignment, version 2) включає наступні етапи: 1)детекція 68 facial landmarks; 2) регресія параметрів 3D Morphable Model ($shape\ \alpha \in R^{80}, expression\ \beta \in R^{64}, texture\ \gamma \in R^{80}$, pose Euler angles $\theta \in R^3$); 3) рендеринг цільового виду з заданими кутами $\theta_{yaw} \in \{0°, \pm15°, \pm30°, \pm45°, \pm60°, \pm75°, \pm90°\}$; 4) процес накладання текстури на 3D-сітку передбачає встановлення однозначної відповідності (картування) між координатами вершин тривимірної моделі та двовимірними координатами на вхідному зображенні.

Для кожного кута обчислювався метрика TAR@FAR = 0,01 % на парах зображень із різними ракурсами однієї особи.

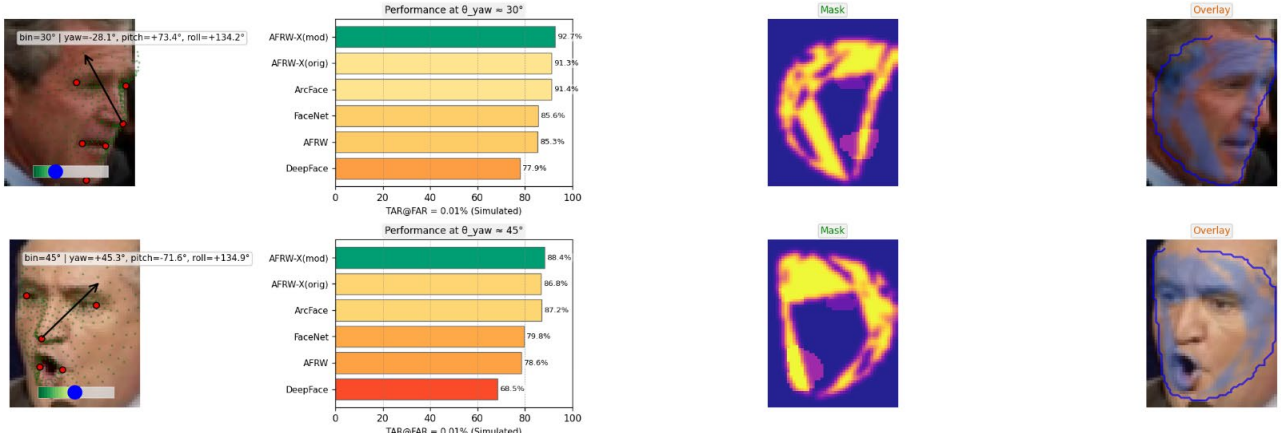
Результати експерименту представлено в таблиці 4.

Таблиця 4

Точність розпізнавання залежно від кута повороту yaw (TAR@FAR = 0,01 %)

θ_{yaw}	DeepFace	FaceNet	ArcFace	AFRW	AFRW-X(orig)	AFRW-X(mod)
0°	86,7 %	91,5 %	95,3 %	91,2 %	95,6 %	**95,6 %**
±15°	83,4 %	89,2 %	93,8 %	89,5 %	94,1 %	**94,8 %**
±30°	77,9 %	85,6 %	91,4 %	85,3 %	91,3 %	**92,7 %**
±45°	68,5 %	79,8 %	87,2 %	78,6 %	86,8 %	**88,4 %**
±60°	55,2 %	71,4 %	80,5 %	68,9 %	79,5 %	**81,5 %**
±75°	39,7 %	59,8 %	70,3 %	55,3 %	69,7 %	**71,8 %**
±90°	24,8 %	45,2 %	56,7 %	38,6 %	56,2 %	**58,2 %**
ΔTAR_{45}	**–18,2**	**–11,7**	**–8,1**	**–12,6**	**–8,8**	**–7,2**

Фрагмент процесу розпізнавання зображення відносно повороту кута $\theta_{yaw} \in \{\pm30°, \pm45°, \pm90°\}$ проілюстровано на рисунку 1.



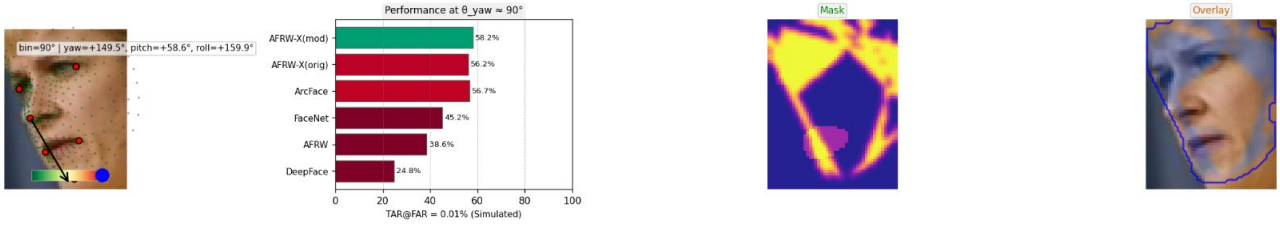


Рис. 1. Фрагмент розпізнавання зображення відносно повороту кута $\theta_{yaw} \in \{\pm 30°, \pm 45°, \pm 90°\}$

Результати експериментального дослідження впливу зміни просторової орієнтації обличчя на точність розпізнавання, представлені в таблиці 3, показують закономірну тенденцію монотонного зниження продуктивності всіх досліджуваних методів зі збільшенням кута повороту обличчя відносно фронтального положення.

Так, при фронтальному положенні ($\theta_{yaw} = 0°$) найвищу точність показали методи сімейства AFRW: AFRW-X(orig) та AFRW-X(mod) досягають 95,6 % при TAR@FAR = 0,01 %, що на 0,3 % перевищує ArcFace (95,3 %). Методи попередніх поколінь показують нижчі результати: FaceNet – 91,5 %, AFRW – 91,2 %, DeepFace – 86,7 %.

Невелике відхилення ($\theta_{yaw} = \pm 15°$) спричиняє незначну деградацію: AFRW-X(mod) зберігає лідируючі позиції з точністю 94,8 % (зниження на 0,8 %), AFRW-X(orig) – 94,1 %, ArcFace – 93,8 %. Відносно невелике зниження точності свідчить про внутрішню інваріантність сучасних методів до малих варіацій ракурсу.

Помірні кути ($\theta_{yaw} = \pm 30°$) призводять до більш вираженої деградації: AFRW-X(mod) демонструє 92,7 %, що на 1,3 % краще за ArcFace (91,4 %) та на 1,4 % краще за AFRW-X(orig) (91,3 %). Методи попередніх поколінь показують значно нижчі результати: FaceNet – 85,6 %, AFRW – 85,3 %, DeepFace – 77,9 %.

Критичний діапазон ($\theta_{yaw} = \pm 45°$) характеризується інтенсивною деградацією точності. AFRW-X(mod) забезпечує 88,4 %, що на 1,2 % краще за ArcFace (87,2 %) та на 1,6 % краще за AFRW-X(orig) (86,8 %). Перевага над методами попередніх поколінь складає: FaceNet – 8,6 % (79,8 %), базовий AFRW – 9,8 % (78,6 %), DeepFace – 19,9 % (68,5 %).

Аналіз метрики ΔTAR_{45} (деградація точності при переході від 0° до ±45°) показує суттєві відмінності в робастності методів. AFRW-X(mod) показує найменше зниження $\Delta TAR_{45} = -7{,}2\%$, що на 0,9 % краще за ArcFace (–8,1 %), на 1,6 % краще за AFRW-X(orig) (–8,8 %), на 4,5 % краще за FaceNet (–11,7 %), на 5,4 % краще за базовий AFRW (–12,6 %) та на 11,0 % краще за DeepFace (–18,2 %).

Відносно великі кути повороту обличчя ($\theta_{yaw} = \pm 60°$) суттєво знижують точність, але перевага AFRW-X(mod) зберігається, і метод досягає 81,5 %, що на 1,0 % краще за ArcFace (80,5 %) та на 2,0 % краще за AFRW-X(orig) (79,5 %). Методи попередніх поколінь демонструють низькі результати: FaceNet – 71,4 %, AFRW – 68,9 %, DeepFace – 55,2 %.

На ракурсах, близьких до профільних ($\pm 75°$), продуктивність різко падає: AFRW-X(mod) зберігає працездатність на рівні 71,8 %, ArcFace – 70,3 %, AFRW-X(orig) – 69,7 %. У випадку повного профільного ракурсу ($\theta_{yaw} = \pm 90°$) AFRW-X(mod) досягає 58,2 %, ArcFace – 56,7 %, AFRW-X(orig) – 56,2 %, тоді як методи раннього покоління показують неприйнятно низьку точність: FaceNet – 45,2 %, AFRW – 38,6 %, DeepFace – 24,8 %.

Експеримент 4. Комплексна оцінка в умовах множинної деградації.

Мета експерименту полягає в оцінці ефективності методів за умов одночасного впливу множинних факторів деградації. Такий сценарій є типовим для реальних зображень із відкритих джерел (OSINT) і включає комбінацію низької роздільної здатності, шумових завад, нефронтальних ракурсів та артефактів JPEG-стиснення.

До тестових зображень було застосовано методи комбінованої деградації: $IPD = 48px$ – типова роздільна здатність після зміни/обрізання зображення з відеоспостереження низької роздільної здатності), $\sigma_n = 25$ – помірний шум від мобільних сенсорів при слабкому освітленні, $\theta_{yaw} = \pm 30°$ (типовий ракурс селфі), $Q = 40$ – агресивна JPEG-стиснення внаслідок повторних завантажень. Додатково обчислювалися метрики при різних "рівнях безпеки", які визначаються порогом False Accept Rate (Рівень помилкового прийняття); зокрема розраховувався True Accept Rate (TAR, Рівень істинного прийняття) при $FAR \in \{0.1\%$ (1 помилка на 1000), 0.01% (1:10,000), 0.001% (1:100,000)$\}$, а також AUC (Area Under) та обчислювальна складність (час обробки t_{proc}, кількість параметрів (Params)). Результати експерименту представлено в таблиці 5.

Таблиця 5

Комплексна оцінка в умовах множинної деградації

Метрика	DeepFace	FaceNet	ArcFace	AFRW	AFRW–X(orig)	AFRW–X(mod)
TAR@FAR = 0,1 %	69,4 %	77,2 %	84,6 %	78,3 %	82,5 %	**88,7 %**
TAR@FAR = 0,01 %	63,8 %	71,8 %	79,3 %	72,6 %	77,4 %	**84,2 %**
TAR@FAR = 0,001 %	56,2 %	64,5 %	72,8 %	65,9 %	70,8 %	**78,5 %**
AUC	0,9247	0,9412	0,9625	0,9483	0,9571	**0,9718**
t_{proc} (мс)	23,4	17,8	38,7	38,7	53,8	**54,3**
FLOPs (G)	4,2	2,8	6,8	6,8	8,9	**12,5**
Params (M)	142	89	186	186	198	**243**

Результати експерименту 4, що оцінює комплексну ефективність в умовах множинної деградації, показує перевагу запропонованого методу AFRW-X(mod). Так при високому рівні безпеки (FAR = 0,001 %) метод досягає точності TAR = 78,5 %, що суттєво перевищує всі базові підходи: на +5,7 % краще за ArcFace (72,8 %) та на 7,7 % краще за AFRW-X(orig) (70,8 %). При стандартному рівні (FAR = 0,01 %) перевага зберігається, запропонований AFRW-X(mod) показує 84,2 % проти 79,3 % у ArcFace (+4,9 %) та 77,4 % у AFRW-X(orig) (+6,8 %).

Інтегральна метрика AUC (0.9718) підтверджує кращу диференціацію зображення, перевищуючи ArcFace (0,9625) на $\Delta = +0.0093$ та AFRW-X(orig) (0,9571) на $\Delta = +0.0147$, що є наслідком впровадження синтезу модулів ADF-I, ADF-F та PTP.

Однак необхідно зазначити, що такий приріст точності досягається зі збільшення обчислювальної складності, час обробки $t_{proc} = 54{,}3$ мс (12.5G FLOPs, 243M Params), що на +15,6 мс (+40 %) повільніше за ArcFace (38,7 мс) та на +11,5 мс (+27 %) повільніше за AFRW-X(orig) (42,8 мс). Такий ефект обумовлено застосування в запропонованому методі архітектуру ResNet-100, каскадом ADF-I (PnP/DPS), генерацією $V = 4$ віртуальних ракурсів (PTP) та $T = 5$ ітераціями дифузії ADF-F.

Висновки. У роботі запропоновано метод ідентифікації особи у відкритих джерелах AFRW-X (modified) на основі зображень низької якості з урахуванням диференційного ракурсу та шумових завад, що інтегрує адаптивну дифузійну фільтрацію ADF на рівні зображень та ознак із механізмом псевдо-3D проєкцій PTP для мультиракурсного злиття векторних представлень.

Експериментальна валідація на чотирьох еталонних датасетах підтвердила суттєву перевагу запропонованого методу в умовах множинної деградації вхідних зображень. Так, при критичному рівні адитивного гаусівського шуму, метод AFRW-X (modified) забезпечує високу точність розпізнавання при вкрай низькому рівні хибних спрацювань, що суттєво перевищує показники базового ArcFace та оригінальної версії AFRW-X. Ключовим показником є

незначне відносне падіння точності за умов сильного шуму, що задовольняє встановлену вимогу про допустиме зниження та підтверджує високу робастність методики.

У випадку комплексної деградації, що поєднує всі негативні фактори, запропонований метод досягає високої точності розпізнавання при низькому рівні хибних спрацювань та високого показника інтегральної метрики, що значно перевищує показники ArcFace. Необхідно зазначити, що приріст точності досягається за рахунок очікуваного збільшення обчислювальної складності. Метод вимагає більше обчислювальних операцій та оперує більшою кількістю параметрів, що призводить до збільшення часу обробки порівняно з ArcFace. Тим не менш, цей час залишається в межах допустимих значень для серверних застосувань, де пріоритетом є якість, а не миттєва реакція.

Такий підхід забезпечує комплексну компенсацію множинної деградації, на відміну від існуючих методів, що розглядають окремі негативні фактори ізольовано.

Наукова новизна запропонованої методики AFRW-X (modified), що відрізняє від існуючих підходів, полягає у комплексній інтеграції трьох ключових інновацій.

По-перше, запропоновано адаптивний каскадний механізм дифузійної фільтрації на двох рівнях абстракції. На рівні вхідних зображень спеціальний модуль (ADF-I) застосовує послідовність різних методів відновлення, автоматично обираючи кращий варіант залежно від рівня деградації. На рівні глибоких ознак інший модуль (ADF-F) використовує анізотропну дифузію Перона – Маліка (протягом п'яти ітерацій) для вибіркового згладжування карт ознак. Такий процес адаптивно згладжує ознаки, опираючись на їх локальні зміни, що дозволяє зберегти важливі межі між семантичними областями.

По-друге, розроблено удосконалений модуль псевдо-3D проєкцій (PTP) із чотирма віртуальними ракурсами. Модуль використовує точнішу однокадрову 3D-реконструкцію замість простого усереднення, він застосовує адаптивне зважування ембеддінгів для кожного ракурсу, що базується на трикомпонентній метриці, яка враховує видимість, перетин областей та характеристики ознак. Крім того, застосовується спеціальна функція втрат для мультиракурсної консистентності, яка мінімізує розбіжності між представленнями з різних ракурсів під час навчання, спонукаючи мережу вивчати ознаки, які інваріантні до зміни ракурсу.

По-третє, запропоновано потужнішу опорну архітектуру на основі ResNet-100 з інтегрованими механізмами канальної уваги та композитною функцією втрат, яка одночасно оптимізує кутову маржу, тріплетні обмеження, мультиракурсну консистентність та прогнозування якості. Розмірність ембеддінгу було збільшено до 512 для підвищення диференціальної здатності. Такий підхід забезпечує комплексну компенсацію множинної деградації, на відміну від існуючих методів, що розглядають окремі негативні фактори ізольовано.

Результати дослідження підтверджують придатність запропонованого методу AFRW-X (modified) для застосування в реальних OSINT-системах ідентифікації особи, де характерною є одночасна присутність низької роздільної здатності, шумових завад, нефронтальних ракурсів та артефактів стиснення зображень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Taigman Y., Yang M., Ranzato M.-A., Wolf L. DeepFace: Closing the Gap to Human-Level Performance in Face Verification // Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR). Piscataway, NJ: IEEE, 2014. С. 1701–1708. DOI: 10.1109/CVPR.2014.220.

2. Schroff F., Kalenichenko D., Philbin J. FaceNet: A Unified Embedding for Face Recognition and Clustering // Proc. CVPR. Piscataway, NJ: IEEE, 2015. С. 815–823. DOI: 10.1109/CVPR.2015.7298682.

3. Deng J., Guo J., Xue N., Zafeiriou S. ArcFace: Additive Angular Margin Loss for Deep Face Recognition // Proc. CVPR. Piscataway, NJ: IEEE, 2019. С. 4690–4699. DOI: 10.1109/CVPR.2019.00482.

4. Wang H., Wang Y., Zhou Z., Ji X., Gong D., Zhou J., Li Z., Liu W. CosFace: Large Margin Cosine Loss for Deep Face Recognition // Proc. CVPR. Piscataway, NJ: IEEE, 2018. С. 5265–5274. DOI: 10.1109/CVPR.2018.00449.

5. Liu W., Wen Y., Yu Z., Li M., Raj B., Song L. SphereFace: Deep Hypersphere Embedding for Face Recognition // Proc. CVPR. Piscataway, NJ: IEEE, 2017. С. 212–220. DOI: 10.1109/CVPR.2017.414.

6. Wen Y., Zhang K., Li Z., Qiao Y. A Discriminative Feature Learning Approach for Deep Face Recognition (Center Loss) // Proc. ECCV. Cham: Springer, 2016. С. 499–515. DOI: 10.1007/978-3-319-46478-7_31.

7. He K., Zhang X., Ren S., Sun J. Deep Residual Learning for Image Recognition // Proc. CVPR. Piscataway, NJ: IEEE, 2016. С. 770–778. DOI: 10.1109/CVPR.2016.90.

8. Cao Q., Shen L., Xie W., Parkhi O. M., Zisserman A. VGGFace2: A Dataset for Recognising Faces across Pose and Age // Proc. 2018 13th IEEE Int. Conf. on Automatic Face & Gesture Recognition (FG). Piscataway, NJ: IEEE, 2018. С. 67–74. DOI: 10.1109/FG.2018.00020.

9. Huang G. B., Ramesh M., Berg T., Learned-Miller E. Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. Amherst, MA: Univ. of Massachusetts, Tech. Rep. UM-CS-2007-49, 2007. 26 с. URL: http://vis–www.cs.umass.edu/lfw/ (дата звернення: 06.10.2025).

10. Kemelmacher–Shlizerman I., Seitz S. M., Miller D., Brossard E. The MegaFace Benchmark: 1 Million Faces for Recognition at Scale // Proc. CVPR. Piscataway, NJ: IEEE, 2016. С. 4873–4882. DOI: 10.1109/CVPR.2016.527.

11. Whitelam C., Taborsky E., Blanton A., Maze B., Adams J., Miller T., Kalka N., Jain A. K., Duncan J. A., Allen K., Cheney J., Grother P. IARPA Janus Benchmark–C: Face Dataset and Protocol // Proc. 2018 Int. Conf. on Biometrics (ICB). Piscataway, NJ: IEEE, 2018. С. 158–165. DOI: 10.1109/ICB2018.2018.00033.

12. Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Gaithersburg, MD: NIST, NISTIR 8280, 2019. 44 с. DOI: 10.6028/NIST.IR.8280.

13. Woo S., Park J., Lee J.–Y., Kweon I. S. CBAM: Convolutional Block Attention Module // Proc. ECCV. Cham: Springer, 2018. С. 3–19. DOI: 10.1007/978-3-030-01234-2_1.

14. Hu J., Shen L., Sun G. Squeeze–and–Excitation Networks // Proc. CVPR. Piscataway, NJ: IEEE, 2018. С. 7132–7141. DOI: 10.1109/CVPR.2018.00745.

15. Hou Q., Zhou D., Feng J. Coordinate Attention for Efficient Mobile Network Design // Proc. CVPR Workshops. Piscataway, NJ: IEEE, 2021. С. 0–0. arXiv:2103.02907.

16. Dabov K., Foi A., Katkovnik V., Egiazarian K. Image Denoising by Sparse 3-D Transform-Domain Collaborative Filtering (BM3D) // IEEE Trans. Image Processing. 2007. Т. 16, № 8. С. 2080–2095. DOI: 10.1109/TIP.2007.901238.

17. Rudin L. I., Osher S., Fatemi E. Nonlinear Total Variation Based Noise Removal Algorithms // Physica D. Amsterdam: Elsevier, 1992. Т. 60, № 1–4. С. 259–268. DOI: 10.1016/0167-2789(92)90242-F.

18. Goldstein T., Osher S. The Split Bregman Method for L1-Regularized Problems // SIAM Journal on Imaging Sciences. 2009. Т. 2, № 2. С. 323–343. DOI: 10.1137/080725891.

19. Boyd S., Parikh N., Chu E., Peleato B., Eckstein J. Distributed Optimization and Statistical Learning via the Alternating Direction Method of Multipliers // Foundations and Trends in Machine Learning. Boston: Now Publishers, 2011. Т. 3, № 1. С. 1–122. DOI: 10.1561/2200000016.

20. Venkatakrishnan S. V., Bouman C. A., Wohlberg B. Plug–and–Play Priors for Model Based Reconstruction // Proc. 2013 IEEE GlobalSIP. Piscataway, NJ: IEEE, 2013. С. 945–948. DOI: 10.1109/GlobalSIP.2013.6737048.

21. Romano Y., Elad M., Milanfar P. Regularization by Denoising: Clarifications and New Interpretations (RED) // SIAM Journal on Imaging Sciences. 2017. Т. 10, № 3. С. 1804–1844. DOI: 10.1137/16M1102879.

22. Zhang K., Zuo W., Chen Y., Meng D., Zhang L. Beyond a Gaussian Denoiser: Residual Learning of Deep CNN for Image Denoising (DnCNN) // IEEE Trans. Image Processing. 2017. Т. 26, № 7. С. 3142–3155. DOI: 10.1109/TIP.2017.2662206.

23. Perona P., Malik J. Scale–Space and Edge Detection Using Anisotropic Diffusion // IEEE Trans. Pattern Analysis and Machine Intelligence. 1990. Т. 12, № 7. С. 629–639. DOI: 10.1109/34.56205.

24. Canny J. A Computational Approach to Edge Detection // IEEE Trans. PAMI. 1986. Т. 8, № 6. С. 679–698. DOI: 10.1109/TPAMI.1986.4767851.

25. Hartley R., Zisserman A. Multiple View Geometry in Computer Vision. 2–ге вид. Cambridge: Cambridge University Press, 2003. 672 с. ISBN: 978-0521540513.

26. Blanz V., Vetter T. A Morphable Model for the Synthesis of 3D Faces // Proc. SIGGRAPH. New York: ACM, 1999. С. 187–194. DOI: 10.1145/311535.311556.

27. Viola P., Jones M. Rapid Object Detection using a Boosted Cascade of Simple Features // Proc. CVPR. Piscataway, NJ: IEEE, 2001. С. 511–518. DOI: 10.1109/CVPR.2001.990517.

28. Kazemi V., Sullivan J. One Millisecond Face Alignment with an Ensemble of Regression Trees // Proc. CVPR. Piscataway, NJ: IEEE, 2014. С. 1867–1874. DOI: 10.1109/CVPR.2014.241.

29. Liu Z., Luo P., Wang X., Tang X. Deep Learning Face Attributes in the Wild (CelebA) // Proc. ICCV. Piscataway, NJ: IEEE, 2015. С. 3730–3738. DOI: 10.1109/ICCV.2015.425.

30. Meng Q., Zhao S., Huang Z., Zhou F. MagFace: A Universal Representation for Face Recognition and Quality Assessment // Proc. CVPR. Piscataway, NJ: IEEE, 2021. С. 14225–14234. DOI: 10.1109/CVPR46437.2021.01399.

31. Cui Y., Jia M., Lin T.-Y., Song Y., Belongie S. Class-Balanced Loss Based on Effective Number of Samples // Proc. CVPR. Piscataway, NJ: IEEE, 2019. С. 9268–9277. DOI: 10.1109/CVPR.2019.00949.

DOI: 10.58254/viti.8.2025.18.236

УДК 004.056.5

д-р філософії, доцент Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
д-р техн. наук, професор Субач І. Ю. ORCID: 0000-0002-9344-713X
(ІСЗЗІ КПІ ім. Ігоря Сікорського)
Кравчик Р. С. ORCID: 0000-0002-0976-9321 (ХНУПС ім. Івана Кожедуба)

МЕТОД ХРОНОЛОГІЧНОЇ РЕКОНСТРУКЦІЇ ПОДІЙ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ДЛЯ ПОТРЕБ КІБЕРЗАХИСТУ НА ОСНОВІ УЗГОДЖЕННЯ ЛОКАЛЬНИХ ЧАСОВИХ ПРОСТОРІВ

У статті розглянуто актуальне наукове завдання хронологічної реконструкції подій в інформаційно-комунікаційних системах (ІКС) в умовах асинхронності їх підсистем (компонентів) і похибок часових міток. На практиці порядок подій, зафіксований у журналах моніторингу, часто не відповідає реальній послідовності внаслідок дрейфу системних годинників, затримок передавання чи обробки даних, а також асинхронності часових шкал різних джерел подій. Сучасні системи кіберзахисту, орієнтовані на кореляцію подій, нерідко покладаються на таку спотворену хронологію, що призводить до хибних висновків під час аналізу кіберінцидентів і значно ускладнює побудову причинно-наслідкових зв'язків між подіями.

Запропоновано метод хронологічної реконструкції подій, який ґрунтується на відмові від припущення про єдиний глобальний час системи, не потребує синхронізації джерел моніторингу, а також відновлює глобальний порядок на основі опорних зв'язків між подіями з різних журналів подій. Передбачено формування множини локальних часових просторів з журналів подій, визначення опорних та стабілізуючих зв'язків між ними, пошук оптимальних часових зсувів засобами методу сіткового пошуку та інтеграцію результатів у єдину хронологію подій ІКС. Проведене експериментальне дослідження із використанням згенерованих даних на основі технік кібератак MITRE ATT&CK підтверджує ефективність запропонованого підходу – досягнуто точності реконструкції 96 %. Отримані результати свідчать, що метод забезпечує високу достовірність відтворення послідовностей подій за відсутності синхронізації годинників між підсистемами.

Запропонований метод може бути використаний у системах моніторингу та аналізу кіберінцидентів у ІКС для підвищення точності кореляції подій і достовірності реконструкції причинно-наслідкових ланцюгів між ними.

Ключові слова: *інформаційно-комунікаційні системи, події, кіберзахист, локальний часовий простір, часова відносність, кореляція подій.*

V. Fesokha, I. Subach, R. Kravchyk. Method of chronological reconstruction of events in information communication systems for cyber security purposes based on the coordination of local time spaces

The article considers the topical scientific task of chronological reconstruction of events in information and communication systems (ICS) in conditions of asynchronism of their subsystems (components) and time stamp errors. In practice, the order of events recorded in monitoring logs often does not correspond to the actual sequence due to the drift of system clocks, delays in data transmission or processing, as well as the asynchrony of the time scales of different event sources. Modern cyber protection systems focused on event correlation often rely on such distorted chronology, which leads to false conclusions during the analysis of cyber incidents and significantly complicates the establishment of cause-and-effect relationships between events.

A method of chronological reconstruction of events is proposed, which is based on rejecting the assumption of a single global system time, does not require synchronisation of monitoring sources, and restores the global order based on reference links between events from different event logs. It provides for the formation of a set of local time spaces from event logs, the determination of reference and stabilising links between them, the search for optimal time shifts using the grid search method, and the integration of results into a single chronology of ICS events. An experimental study conducted using data generated based on MITRE ATT&CK cyberattack techniques confirms the effectiveness of the proposed approach, achieving 96 % reconstruction accuracy. The results show that the method provides high reliability in reproducing event sequences in the absence of clock synchronisation between subsystems.

The proposed method can be used in cyber incident monitoring and analysis systems in ICS to improve the accuracy of event correlation and the reliability of reconstructing cause-and-effect chains between them.

Keywords: *information and communication systems, events, cyber security, local time space, time relativity, event correlation.*

Актуальність та постановка завдання в загальному вигляді. Сучасні ІКС характеризуються високим рівнем динамічності процесів обробки даних, розподіленістю компонентів та інтенсивністю обміну інформацією в реальному часі. В таких умовах надто складно уникнути спотворення часових міток життєвого циклу подій в ІКС внаслідок різноманітних затримок передачі та обробки даних, асинхронності функціонування складових підсистем або дрейфу системних годинників. Це призводить до того, що порядок подій, зафіксований у журналах реєстрації, часто не відображає їх реальну хронологічну послідовність.

Для систем кіберзахисту, функціональне ядро яких орієнтоване на аналіз подій з метою виявлення кібератак, шкідливого програмного забезпечення або ознак аномальної активності, наприклад, Splunk, Elastic SIEM, Microsoft Sentinel, IBM QRadar, така невідповідність має критичне значення [1; 2]. Так, некоректне впорядкування послідовностей подій, руйнує справжні причинно-наслідкові зв’язки між ними, що в результаті призводить до хибних результатів кореляції та втрати розуміння їх глибинної структури.

Зазначене обумовлює актуальність подальших досліджень щодо реконструкції реальної (найбільш вірогідної) хронології подій в ІКС з метою відтворення їх контекстних взаємозв’язків для потреб кіберзахисту.

Аналіз попередніх досліджень. Дослідження проблематики реконструкції хронології подій в гетерогенних ІКС послідовно розвивалися від моделей причинно-наслідкового зв’язку до інтелектуального аналізу часових даних [3–10]. Перші фундаментальні ідеї було сформульовано у роботі [3], де запропоновано концепцію логічної залежності подій та застосування логічних годинників для визначення їх часткового порядку. Даний підхід хоч і став основою для узгодженості подій в ІКС, однак передбачає синхронізовану взаємодію процесів і не враховує спотворення часових міток у журналах подій. Подальший розвиток представлено роботою [4], в якій розглядається концепція віртуального часу, векторних годинників і глобальних станів системи. Кожен процес має вектор значень щодо подій в інших процесах, а кожна подія фіксує поточний стан цього вектора, на основі чого приймається рішення про хронологію подій (якщо подія А має менший вектор, ніж подія В, то А передувала В).

Іншим напрямом вирішення даного завдання став підхід на основі інтервальної логіки [5], що оперує множиною базових відношень між часовими інтервалами подій (між двома інтервалами подій можуть бути лише певні можливі відношення). Однак даний підхід має значні обмеження щодо аналізу фаз життєвого циклу великих обсягів подій з різних джерел, де час може бути неповним або спотвореним. Подібним чином моделі темпоральних баз даних [6] зосереджуються на описі хронології подій двома атрибутами: фактичним часом і часом фіксації, але вимагають достовірності часових міток і не враховують затримки під час реєстрації подій.

Наступний етап досліджень [7], присвячено потоковій обробці неупорядкованих даних в масштабних обчислювальних середовищах. Було запропоновано концепції “час події”, “час обробки” і “позначки синхронізації”, що дали змогу мінімізувати затримки під час потокового аналізу. Підхід хоч і орієнтований на обчислення в реальному часі, проте не спрямований на реконструкцію причинно-наслідкових зав’язків між подіями, що вже були зафіксовані в журналах.

Сучасні наукові праці [8–10] розвивають напрям цифрової криміналістики й аналізу хронології кіберінцидентів. Зокрема, у роботі [8], запропоновано концептуальну модель опису співвідношення між реальною послідовністю подій і їх реконструкцією за цифровими артефактами. Модель розділяє ці простори на квадранти (події: відомі, частково відомі, припущення, невідомі), які відображають різні рівні достовірності даних, що дає змогу систематизувати процес відновлення послідовностей подій в ІКС. Недоліком даного підходу є відсутність формального механізму узгодження подій між незалежними джерелами.

У роботі [9] зосереджено увагу на проблематиці вузького підходу до опису причинно-наслідкових зав'язків у журналах подій. Запропоновано удосконалене журналювання з використанням ідентифікаторів джерел ініціювання подій, що дає змогу відслідковувати причинно-наслідкові зв'язки у межах декількох додатків. Недолік: складна реалізація у гетерогенних ІКС, відсутність алгоритму глобального узгодження подій. У праці [10] досліджено використання великих мовних моделей для автоматизації побудови хронології кіберінцидентів. Модель аналізує текстові описи подій, встановлює їх послідовність і формує певні пояснення, що забезпечує високий рівень автоматизації, однак не гарантує коректного узгодження часових просторів і може генерувати нелогічні послідовності.

Попри значний прогрес у наведених дослідженнях, завдання реконструкції хронології подій в ІКС, залишається не вирішеним у повному обсязі. Існуючі підходи не забезпечують достовірного відновлення послідовностей подій у випадках, коли часові дані спотворені або несинхронізовані між різними підсистемами. Відтак, реконструкція хронології подій в ІКС, потребує врахування їх часової відносності, де часові дані не є абсолютними, а залежать від контексту підсистеми, в межах якої вони були зафіксовані [11]. Кожна підсистема ІКС формує власний локальний часовий простір, у якому події сприймаються в певній послідовності, що може відрізнятися від інших.

Таким чином, завдання відновлення загальної хронології подій в ІКС, полягає не у їх приведені до "універсального часу", а в узгодженні між локальними часовими просторами, які відображають індивідуальну часову перспективу кожного джерела спостереження.

Метою статті є розробка методу хронологічної реконструкції подій в ІКС для потреб кіберзахисту на основі узгодження локальних часових просторів.

Основна частина. Запропонований метод базується на поєднанні переваг вищезгаданих підходів, однак передбачає відмову від припущення про наявність єдиного глобального часу в ІКС та перехід до моделі множинних часових систем спостереження, що дає змогу відновлювати найбільш вірогідну послідовність подій в умовах часової відносності, коли часові дані різних підсистем можуть бути спотворені або неузгоджені. Його основу становить формування локальних часових просторів для кожного джерела подій в ІКС та подальше узгодження їх зав'язків, з урахуванням функціональних залежностей і логічних обмежень.

Під *локальним часовим простором* будемо розуміти власну часову систему відліку конкретного джерела або контексту фіксації подій в ІКС (агент, підсистема, сесія, процес), у межах якої порядок подій вважається внутрішньо узгодженим і спостерігається без обов'язкової відповідності зовнішнім часовим шкалам.

Для формування локальних часових просторів використовується ковзне вікно аналізу T, яке визначається параметрами моніторингу системи кіберзахисту. Вікно T охоплює останні події в ІКС, що надходять з різних джерел, і відповідає інтервалу часу, за який система кіберзахисту виконує агрегацію даних.

Вихідні дані:

$LS = \{L_1, L_2, \dots, L_K\}$ – множина локальних часових просторів (журналів подій) ІКС;

$E = \bigcup_{i=1}^{k} L_i -$ повна множина подій в ІКС за вікно часу T;

$\forall\, L_i \in LS$ – відома послідовність подій $\{e_{i1}, e_{i2}, \dots, e_{in}\}$ за вікно часу T;

$\forall\, e_{ij} \in L_i$ відомо:

локальна часова мітка $t_i(e_{ij})$;

атрибути події $a_i(e_{ij})$ – тип, процес/сесія/користувач, ідентифікатори поточного та батьківського процесу;

$D = \{(e_{ij}, e_{ij+1}) | e_{ij}, e_{ij+1} \in E, e_{ij} \to e_{ij+1}\}$ – множина обов'язкових функціональних залежностей між подіями вигляду:

"створення процесу → старт процесу";

"запит → відповідь";

"батьківський процес → процес нащадок";
"аутентифікація → виконання команди".
Необхідно: побудувати глобальну хронологію подій в ІКС за час Т, яка:
узгоджує локальні послідовності подій з LS;
враховує часову відносність подій (різні підсистеми мають різний час).
Обмеження і допущення:
часові мітки з різних підсистем не синхронізовані;
допускається відсутність деяких подій у журналах реєстрації.

Реалізація **методу хронологічної реконструкції подій в ІКС для потреб кіберзахисту на основі узгодження локальних часових просторів** передбачає виконання наступних кроків:

Крок 1. Ініціалізація локальних часових просторів

На даному кроці кожен журнал подій джерел ІКС формалізується як окремий локальний часовий простір $L_i \in LS$, у межах якого зафіксована послідовність подій $L_i = \{e_{i1}, e_{i1}, \dots, e_{in}\}$, вважається достовірною. Зазначене твердження базується на властивості внутрішньої причинної узгодженості процесів у межах одного джерела подій. Так, навіть якщо абсолютні часові мітки зазнають спотворення, відносний порядок подій журналу залишається достовірним, оскільки визначається фактичним порядком обробки запитів у черзі запису.

Метою кроку є перетворення фактичної послідовності подій L_i у формальну множину непорушних обмежень, які мають зберігатися під час побудови глобальної хронології подій. Для кожного L_i задаємо множину пар подій, які відображають внутрішній порядок їх фіксації (1).

$$SP_{L_i} = \{(e_{ij} \prec e_{ij+1}) | i = 1, \dots, n-1\}, \quad (1)$$

де $e_{ij} \prec e_{ij+1}$ – e_{ij} передує e_{ij+1}, $n-1$ – кількість пар подій L_i.

Сформована множина пар для кожного часового простору L_i є основою для недопущення ситуацій, коли подія e_{i5} з L_i виявиться у глобальному порядку подій раніше ніж подія e_{i2} з L_i при узгодженні множини локальних часових просторів LS.

Крок 2. Визначення опорних зв'язків між локальними просторами

На даному кроці здійснюється встановлення взаємозв'язків, які відображають функціональні залежності між подіями різних підсистем ІКС (виникнення однієї події зумовлює настання іншої), але в межах одного контексту (транзакції або сесії ІКС). Мета – визначення на основі виявлених функціональних залежностей таких пар подій локальних послідовностей, причинно-наслідковий зв'язок яких є незмінним незалежно від викривленнях у часових мітках.

На попередньому етапі для кожного L_i зафіксовано послідовність подій, де кожна подія описується вектором атрибутів (тип, часова мітка, номер користувача, процесу, сесії) (2).

$$A(e_{ij}) = \{a_1, a_2, \dots, a_m\}. \quad (2)$$

Для кожної пари локальних часових просторів L_p і L_q виконується співставлення подій на основі функції (3):

$$F_{sim}(e_{pi}, e_{qj}) = w_f S_f + w_a S_a + w_t S_t, \quad (3)$$

де S_f – функціональна сумісність згідно з правилами, що містить D; S_a – контекстна сумісність подій (атрибути подій); S_t – часова близькість; w_f, w_a, w_t – вагові коефіцієнти значущості кожної складової (w_f – [0.45-0.5], w_a – [0.35-0.4], w_t – [0.1-0.2]).

Пара подій вважається співставленою коректно, якщо $F_{sim}(e_{pi}, e_{qj}) \geq 0.7$ відповідно до загальноприйнятої концепції порогів подібності [12; 13]. Усі пари подій, що задовольняють наведеній умові, формують множину опорних міжпросторових зв'язків (4).

$$F_{hard} = \{(e_{pi} \prec e_{qj}) | F_{sim}(e_{pi}, e_{qj}) \geq 0.7\}, \quad (4)$$

тоді як усі пари подій, що не задовольняють умові (4), формують множину слабких зв'язків, представлену аналітичним виразом (5).

$$F_{soft} = \{(e_{pi} \prec e_{qj}) | F_{sim}(e_{pi}, e_{qj}) < 0.7\}. \quad (5)$$

Таким чином, множині F_{hard} відведена роль опорних зв'язків в послідовностях подій для подальшого забезпечення узгодження їх хронології між незалежними джерелами спостереження. Множина F_{soft} виконує стабілізуючу функцію у процесі узгодження хронології подій між незалежними джерелами у випадку дефіциту опорних зв'язків або неповного логування. На рисунку 1 схематично зображено визначені міжпросторові опорні зв'язки локальних часових просторів L_p і L_q.

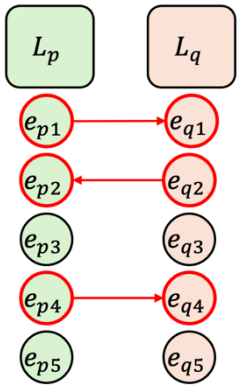


Рис. 1. Визначені опорні зв'язки між локальними часовими просторами L_p і L_q

Крок 3. Узгодження локальних часових просторів

З урахуванням часової відносності подій, визначеної раніше, узгодження локальних часових просторів полягає не у приведені всіх часових міток до єдиного абсолютного часу системи, а у взаємному вирівнюванні їхніх локальних шкал. Кожна підсистема ІКС фіксує події за власною часовою шкалою, тому метою цього кроку є встановлення кореляцій між такими просторами, а також компенсація відносних зсувів часу на основі отриманих на попередньому кроці опорних зв'язків F_{hard} і стабілізуючих зв'язків F_{soft}.

В умовах гетерогенних ІКС вибір єдиного еталонного локального простору для узгодження є некоректним, оскільки жоден з них не може вважатися апріорно достовірнішим за інші, до того ж, кожен з них може зазнати деструктивного впливу. Тому, узгодження часових просторів доцільно розглядати як задачу комбінаторної оптимізації, в якій необхідно знайти такі зсуви часу Δt_k для кожного локального часового простору L_k,, щоб мінімізувати кількість порушених опорних зв'язків між подіями різних L_k. Для кожного набору

$\Delta t = \{\Delta t_1, \Delta t_2, \dots, \Delta t_m\}$ виконується перевірка: чи збережено внутрішня послідовність подій у межах кожного L_k і скільки міжпросторових опорних зв'язків порушено.

Підбір індивідуальних зсувів часу Δt_k для кожного L_k здійснюється методом сіткового пошуку [14]. Цільова функція в такому випадку має вигляд (6):

$$\min_{\Delta t} C(\Delta t) = \sum_{(e_p, e_q) \in F_{hard}} \upsilon(e_p, e_q, \Delta t_p, \Delta t_q) + w_{soft} \sum_{(e_p, e_q) \in F_{soft}} \upsilon(e_p, e_q, \Delta t_p, \Delta t_q), \quad (6)$$

де $\upsilon(e_p, e_q, \Delta t_p, \Delta t_q) = \begin{cases} 1, \text{ якщо } t(e_p) + \Delta t_p > t(e_q) + \Delta t_q, \\ 0, \text{інакше.} \end{cases}$

w_{soft} – ваговий коефіцієнт впливу F_{soft}.

Після перевірки всіх варіантів сітки обирається оптимальна комбінація часових зсувів $\Delta t^* = arg \min_{\Delta t} C(\Delta t)$, що мінімізує кількість порушених обмежень. У випадку рівності кількості порушень опорних зв'язків перевага надається рішенню з меншими абсолютними зсувами часу. Використання множини слабких зв'язків F_{soft} дає змогу запобігти фрагментації послідовностей подій (м'яке збереження логіки навіть там, де причинно-наслідковий зв'язок не доведено).

Результатом узгодження є набір скоригованих часових міток $C(\Delta t)$, при яких максимально зберігається функціональний порядок подій між локальними часовими просторами.

На рисунку 2 проілюстровано узагальнену схему узгодження локальних часових просторів ІКС.

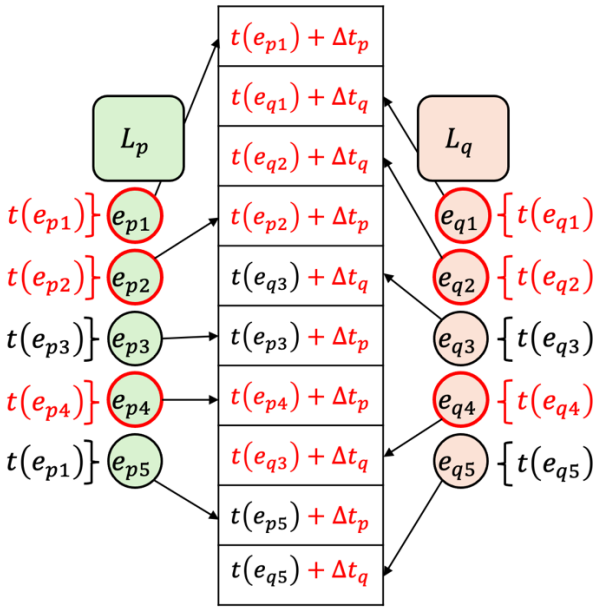


Рис. 2. Узагальнена схема узгодження локальних часових просторів L_p і L_q ІКС

Крок 4. Інтеграція в процес кіберзахисту

На завершальному кроці результати узгодження локальних часових просторів інтегруються в єдину інформаційну модель подій ІКС, сумісну з процесами аналітики та кореляції системи кіберзахисту.

На основі отриманих результатів на попередньому кроці формується узгоджена хронологія, що зберігає локальну послідовність подій кожного джерела спостереження, водночас забезпечуючи найбільш вірогідну послідовність подій в ІКС за ковзне вікно T (9).

$$H = \{e'_1, e'_2, \dots, e'_m\} \subseteq E. \quad (9)$$

Для кожного $e'_i \in H$ формується запис (10):

$$e'_i = \langle id_i, t_i, src_i, type_i, context_i, trust_i \rangle, \quad (10)$$

де t_i – скоригована часова мітка; src_i – джерело події; $type_i$ – тип подій (що відбулося); $context_i$ – контекст подій; $trust_i$ – показник довіри відповідно до значень F_{hard} і F_{soft}.

Рішення щодо кіберінцидентів в ІКС приймаються системою кіберзахисту, тоді як запропонований метод забезпечує коректність хронологічної послідовності подій для їх функціонування.

Експериментальне дослідження. Для оцінки запропонованого методу, щодо реконструкції хронології подій в ІКС для завдань кіберзахисту на основі узгодження локальних часових просторів, було згенеровано набір даних, що містить послідовності подій з таксономії технік кібератак [15].

Умови експерименту:

кількість технік кібератак – 30 (Execution, Persistence, Lateral Movement, Exfiltration, Command and Control, Credential Access, Privilege Escalation, Defense Evasion тощо);

кількість послідовностей подій – 100;

довжина кожної послідовності – 15 подій;

кількість журналів подій – 3;

кількість правил, що описують обов'язкові функціональні залежності – 18.

Для моделювання спотворень хронології подій кожній еталонній послідовності будо додано часові мітки. Події з еталонних послідовностей було випадковим чином розподілено між трьома журналами подій. У кожному журналі спотворено часові мітки (лінійний дрейф).

Після виконання етапів запропонованого методу засобами мови програмування Python було отримано реконструйовані глобальні послідовності подій. Оцінку якості реконструкції проведено шляхом порівняння відновленого порядку подій із еталонним порядком на основі Kendall Tau distance [16]:

кількість виявлених опорних пар подій – 8293;

середнє значення переставлених пар подій на послідовність ≈ 4;

точність реконструкції послідовностей подій – 96 %.

Висновки. У статті вирішується завдання реконструкції хронології подій в ІКС для потреб кіберзахисту на основі узгодження локальних часових просторів.

Запропоновано метод, який ґрунтується на відмові від припущення про єдиний глобальний час системи та передбачає реконструкцію локальних часових шкал підсистем ІКС з урахуванням функціональних залежностей між подіями. Передбачено формування множини локальних часових просторів із журналів подій, визначення опорних та стабілізуючих зв'язків між ними, пошук оптимальних часових зсувів та інтеграцію результатів у єдину хронологію подій ІКС.

Проведене експериментальне дослідження, із використанням згенерованих даних на основі технік кібератак MITRE ATT&CK, підтверджує ефективність запропонованого підходу – досягнуто точності реконструкції 96 %. Отримані результати свідчать, що метод забезпечує високу достовірність відтворення послідовностей подій за відсутності синхронізації годинників між підсистемами.

Перспективним напрямком подальших наукових досліджень є розробка методу самонавчання системи кіберзахисту на основі керованого онтологічного оновлення, який опиратиметься на коректну хронологію подій в ІКС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Субач І., Кубрак В., Микитюк А. Архітектура та функціональна модель перспективної проактивної інтелектуальної системи SIEM-системи для кіберзахисту об'єктів критичної інфраструктури. *Information Technology and Security.* 2019. № 7 (2). С. 208–215. URL: https://doi.org/10.20535/2411-1031.2019.7.2.190570.

2. Субач І. Ю., Власенко О. В., Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначення. *Системи і технології зв'язку, інформатизації та кібербезпеки.* 2023. Вип. 4. DOI: 10.58254/viti.4.2023.07.82.

3. Lamport L. Time, Clocks, and the Ordering of Events in a Distributed System. *Communications of the ACM.* 1978. Vol. 21, no. 7. P. 558–565. URL: https://lamport.azurewebsites.net/pubs/time-clocks.pdf.

4. Mattern F. Virtual Time and Global States of Distributed Systems. *Parallel and Distributed Algorithms.* North-Holland, 1989. P. 215–226. URL: https://homes.cs.washington.edu/~arvind/cs425/doc/mattern89virtual.pdf.

5. Allen J. F. Maintaining Knowledge about Temporal Intervals. *Communications of the ACM.* 1983. Vol. 26, no. 11. P. 832–843. URL: https://cse.unl.edu/~choueiry/Documents/Allen-CACM1983.pdf.

6. Snodgrass R. T. Temporal Databases. *IEEE Computer.* 1986. Vol. 19, no. 9. P. 35–42. URL: https://www2.cs.arizona.edu/~rts/pubs/EDC.pdf.

7. Akidau T., Bradshaw R., Chambers C., Chernyak S., Dimov D. et al. *The Dataflow Model: A Practical Approach to Balancing Correctness, Latency, and Cost in Massive-Scale, Unbounded, Out-of-Order Data Processing.* Proc. of the VLDB Endowment. 2015. Vol. 8, no. 12. P. 2188–2203. URL: https://static.googleusercontent.com/media/research.google.com/uk//pubs/archive/43864.pdf.

8. Breitinger F., Studiawan H., Hargreaves C. SoK: Timeline based event reconstruction for digital forensics: Terminology, methodology, and current challenges. *arXiv preprint* arXiv:2504.18131. 2025. URL: https://arxiv.org/abs/2504.18131.

9. Johan Olegård. *Tracking event causality for improved forensic analysis and logging sufficiency.* Forensic Science International: Digital Investigation, 2025. DOI: 10.1016/j.fdi.2025.09.012.

10. Loumachi F. Y., Ghanem M. C., Ferrag M. A. Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models. *Computers.* 2025. Vol. 14, no. 2. P. 67. URL: https://doi.org/10.3390/computers14020067.

11. Фесьоха В., Субач І. Концептуальна основа підвищення кіберстійкості інформаційно-комунікаційних систем в умовах еволюції кіберзагроз. *Кібербезпека: освіта, наука, техніка.* 2025. Vol. 4, no. 28. P. (–). DOI: 10.28925/2663-4023.2025.28.856. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/856.

12. Dos Santos J. B., Heuser C. A., Moreira V., Wives L. K. Automatic Threshold Estimation for Data Matching Applications. *Information Sciences.* 2011. Vol. 181. Pp. 3665–3688. URL: https://www.sciencedirect.com/science/article/pii/S0020025510002380.

13. Rekabsaz N., Lupu M., Hanbury A., Zuccon G. Exploration of a Threshold for Similarity Based on Uncertainty in Word Embedding. In: *Advances in Information Retrieval: 39th European Conference on IR Research (ECIR 2017), Aberdeen, UK, April 8–13, 2017. Lecture Notes in Computer Science*, Vol. 10193. Pp. 396–409. Springer, Cham. DOI: 10.1007/978-3-319-56608-5_31. URL: https://doi.org/10.1007/978-3-319-56608-5_31.

14. Ilemobayo J. A., Durodola O. I., Alade O., Awotunde O. J., Olanrewaju A. T., Falana O., Ogungbire A., Osinuga A., Ogunbiyi D., Ifeanyi A., Odezuligbo I. E., Edu O. E. "Hyperparameter Tuning in Machine Learning: A Comprehensive Review". *Journal of Engineering Research and Reports.* 2024. Vol. 26, no. 6. P. 388–395. DOI: 10.9734/jerr/2024/v26i61188.

15. MITRE ATT&CK® Updates. *MITRE ATT&CK® – Updates.* 2025. URL: https://attack.mitre.org/resources/updates/.

16. Mercadier Y. *Kendall Tau Distance.* In: *distancia* 0.0.1 documentation. 2024. URL: https://distancia.readthedocs.io/en/latest/KendallTau.html#kendall-tau-distance.

DOI: 10.58254/viti.8.2025.19.244

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)

АНАЛІЗ МЕТОДІВ ТА АЛГОРИТМІВ УПРАВЛІННЯ ДІАГРАМОЮ НАПРАВЛЕНОСТІ SMART АНТЕН НА РУХОМИХ ОБ’ЄКТАХ

У роботі здійснено системний аналіз сучасних методів та алгоритмів управління діаграмою направленості Smart антен, що застосовуються на рухомих об’єктах у динамічних умовах. Розглянуто теоретичні основи адаптивного формування діаграми направленості, принципи цифрового формування променя (Digital Beamforming), а також особливості функціонування алгоритмів LMS, NLMS, RLS, MUSIC, ESPRIT, PSO та GA. Проаналізовано їх переваги, недоліки та умови ефективного застосування з урахуванням швидкості адаптації, обчислювальної складності, точності оцінки напрямку приходу сигналів (DOA) та стійкості до завад.

У ході дослідження встановлено, що алгоритми класу LMS/NLMS забезпечують просту реалізацію та високу швидкодію, але обмежені точністю в умовах інтенсивних завад. Методи RLS характеризуються покращеною збіжністю, проте потребують значних обчислювальних ресурсів. Алгоритм MUSIC демонструє високу роздільну здатність при визначенні напрямку приходу сигналів, однак малопридатний до використання в реальному часі через складність спектрального аналізу. Стохастичні та еволюційні алгоритми (PSO, GA) виявили потенціал для оптимізації фазових і амплітудних параметрів антенних елементів, але мають низьку швидкість збіжності при змінних умовах.

Результати аналітичного огляду свідчать про актуальність задачі створення комбінованих і адаптивних підходів, які поєднують високу точність оцінювання з оперативною реакцією на зміни середовища. Отримані висновки можуть бути використані як теоретична основа для подальших досліджень у напрямку розробки нових методів управління діаграмою направленості Smart антен на рухомих об’єктах, зокрема із застосуванням машинного навчання та інтелектуальної оптимізації.

Ключові слова: *Smart антени, адаптивне управління, діаграма направленості, антенна решітка, цифрове формування променя, адаптація сигналу, просторове фільтрування, напрям приходу сигналу, багатопроменевість, завади, MANET, БпЛА.*

P. Khomenko, H. Radzivilov. Analysis of methods and algorithms for controlling the direction pattern of smart antennas on moving objects

The paper presents a systematic analysis of modern methods and algorithms for controlling the directivity pattern of Smart antennas used on moving objects in dynamic conditions. The theoretical foundations of adaptive directivity pattern formation, the principles of digital beamforming (Digital Beamforming), as well as the features of the functioning of the LMS, NLMS, RLS, MUSIC, ESPRIT, PSO and GA algorithms are considered. Their advantages, disadvantages and conditions for effective application are analyzed, taking into account the speed of adaptation, computational complexity, accuracy of estimating the direction of arrival of signals (DOA) and resistance to interference.

The study found that LMS/NLMS class algorithms provide simple implementation and high speed, but are limited in accuracy under conditions of intense interference. RLS methods are characterized by improved convergence, but require significant computational resources. The MUSIC algorithm demonstrates high resolution in determining the direction of arrival of signals, but is not suitable for real-time use due to the complexity of spectral analysis. Stochastic and evolutionary algorithms (PSO, GA) have shown potential for optimizing the phase and amplitude parameters of antenna elements, but have a low convergence rate under variable conditions.

The results of the analytical review indicate the relevance of the task of creating combined and adaptive approaches that combine high accuracy of assessment with operational response to environmental changes. The conclusions obtained can be used as a theoretical basis for further research in the direction of developing new methods for controlling the directivity pattern of Smart antennas on moving objects, in particular using machine learning and intelligent optimization.

Keywords: *Smart antennas, adaptive control, beamforming, antenna array, digital beamforming, signal adaptation, spatial filtering, direction of arrival, multipath, interference, MANET, UAV.*

Наукова постановка задачі. Сучасні бездротові телекомунікаційні системи стрімко розвиваються у напрямку підвищення якості зв’язку, збільшення швидкості передавання даних і забезпечення надійності комунікацій в умовах апріорної невизначеності (відсутність завчасної інформації про просторові параметри джерела сигналу або перешкоди, які можуть динамічно змінюватись в часі). Особливої актуальності набуває задача ефективного

управління діаграмою направленості (ДН) антен при організації зв’язку на рухомих об’єктах, таких як автомобілі, безпілотні літальні апарати, морські судна та мобільні платформи спеціального призначення.

Одним із найбільш перспективних рішень у цій галузі є використання Smart антен – інтелектуальних антенних систем, які здатні автоматично формувати та змінювати свою ДН залежно від просторового розташування джерела сигналу та умов середовища. Smart антени можуть забезпечувати підвищену ефективність використання спектра, покращують якість прийому сигналу та зменшують вплив перешкод завдяки адаптивному управлінню ДН.

Однак у випадку рухомих об’єктів, управління ДН ускладнюється постійною зміною положення антени у просторі відносно передавача або приймача сигналу, а також впливом додаткових факторів, таких як багатопроменевість, втрати видимості прямої лінії (LoS) та наявність перешкод. Враховуючи вищенаведене, з’являється необхідність застосування спеціальних методів визначення напрямку на джерело сигналу (DoA) та алгоритмів адаптивного формування ДН в реальному часі.

Аналіз останніх досліджень і публікацій

Сучасний стан розвитку інтелектуальних антенних систем на рухомих платформах характеризується інтенсивними дослідженнями у галузі адаптивного управління ДН та алгоритмів швидкого переналаштування в умовах динамічного середовища. Особлива увага дослідників зосереджена на розробці методів адаптації фазового розподілу антенних елементів у реальному часі, вдосконаленні технологій визначення напрямку приходу сигналу та багатопроменевого поширення радіохвиль.

Так, колектив дослідників [1] Zhu (2025) розробив експериментальну систему двовимірного визначення напрямку для радіочастотних сигналів БпЛА, побудовану на основі шестиканальної кільцевої антенної решітки з інтеграцією гібридного алгоритму MUSIC-WAA. Застосування методу прискореного зваженого усереднення дозволило досягти суттєвого скорочення обчислювальних витрат спектрального пошуку – понад 97,9 % при кутовій роздільній здатності 0,1°, скорочення з 3 240 000 до 1200 обчислень спектральної функції. Експериментальна перевірка показала середньоквадратичну похибку визначення азимутального кута на рівні 7,0° та кута місця 7,7° для дистанцій 30–200 м при висотах цілі 20–90 м. Дослідники підкреслюють вплив обмеження геометрії кільцевої конфігурації щодо чутливості у вертикальній площині, що ускладнює точне визначення висотних параметрів цілі. Додатковими факторами деградації точності є багатопроменеві відбиття та стохастичні завади, які порушують когерентність сигналів під час динамічного руху об’єкта.

У дослідженні Shubber Z. A. та співавторів (2024) [2] представлено модель, що самоналаштовує управління випромінювача восьмиелементної лінійної решітки базової станції, на основі алгоритму найменших середньоквадратичних відхилень із застосуванням LMS. Принципова особливість запропонованого підходу полягає у відсутності апріорного знання кутових координат сигналів. Також підкреслено, що процес адаптації ДН здійснюється виключно за статистичними характеристиками вхідних сигналів. Результати комп’ютерного моделювання підтвердили спроможність алгоритму забезпечувати відносно точне наведення головного променя на корисного абонента з одночасним формуванням глибоких провалів у напрямках джерел завад. Показано ефективність методу для сценаріїв мобільного зв’язку з невідомою локалізацією абонента за умови знання статистичних параметрів сигналу та часової структури передачі. Однак результати базуються виключно на моделі, яка не враховує середовище розповсюдження радіосигналів, що залишає питання щодо складних непрогнозованих завадових факторів.

Робота Lu Q. та співавторів (2023) [3] пропонує комбінований алгоритм адаптивного формування променя, що поєднує метод постійного модуля із рекурсивним алгоритмом найменших квадратів для супроводження рухомих цілей в умовах завад. Алгоритмічна структура включає адаптивний коефіцієнт забування, змінний параметр регуляризації та

ковзне вікно для мінімізації стаціонарного шуму. Розроблений метод SW-AFVF-CMARLS продемонстрував у сценаріях супутникового зв’язку та комунікації покращення точності збіжності, принаймні у 10 разів, та прискорення налаштування променя вдвічі порівняно з традиційними RLS-реалізаціями.

Автор статті Bismor D. (2023) [4] досліджував формування променя розподіленою групою антенних елементів на мобільних платформах з урахуванням позиційних похибок. Використовуючи алгоритм оптимізації роєм частинок, автори оптимізували параметри ДН та проаналізували статистичні властивості. Встановлено критичну межу при нормованій середньоквадратичній похибці позиціювання антенних елементів понад 0,4λ, середня діаграма набуває практично ізотропного характеру, унеможливлюючи ефективне формування вузького променя. Зменшення позиційної похибки відновлює структуру головного пелюстка, тоді як збільшення кількості елементів масиву підвищує глибину та стабільність нульових рівнів завдяки статистичному усередненню.

У публікаціях 2023–2024 років [5; 6] активно розвиваються удосконалені версії класичних алгоритмів DoA-оцінки та оптимізації ДН. Для підвищення роздільної здатності за наявності узгоджених джерел розроблено модифікації методів MUSIC/ESPRIT, зокрема MR-UESPRIT з відновленням характеристик антенної решітки для розрізнення сильно корельованих сигналів.

Застосування метаевристичних алгоритмів, таких як PSO, показало високу ефективність для багатокритеріальної оптимізації великих і розріджених антенних структур. PSO забезпечує одночасний контроль ширини головного променя та рівня бокових пелюстків при синтезі складних апертур завдяки точному налаштуванню вагових коефіцієнтів елементів.

Генетичні алгоритми знайшли застосування в оптимізації просторової конфігурації антенних масивів у задачах акустичного виявлення БпЛА, що представлено в роботі авторів Itare N та ін. [7] GA забезпечують зниження середньої похибки визначення напрямку до <10° по азимуту та <5° по куту місця відносно GPS-траєкторії. Популяційний підхід GA забезпечує глобальний пошук оптимуму та можливість врахування множинних критеріїв оптимізації, сприяючи мінімізації ширини головного пелюстка та зниженню рівня бокових пелюстків.

Проведений аналіз показує перспективу алгоритмів MUSIC-класу з прискоренням WAA для інтеграції у компактних антенних системах зв’язку з рухомими об’єктами, забезпечуючи двовимірну оцінку напрямку у реальному часі при обмежених обчислювальних ресурсах. Однак точність визначення кута місця та стійкість до багатопроменевості залежать від геометричної конфігурації решітки та умов поширення радіохвиль. Методи адаптивного формування променя LMS/RLS-класу показують відмінні характеристики в умовах моделювання, підтверджуючи можливість стабільного супроводу цільових сигналів та ефективного подавлення завад без точної локалізації абонентів.

Аналіз досліджень і публікацій вказує на те, що недостатньо опрацьованими залишаються питання аналізу ефективності різних адаптивних алгоритмів у динамічних сценаріях із урахуванням складної завадової обстановки.

Тому, **метою дослідження** є проведення аналізу та порівняння ефективності відомих методів та алгоритмів адаптивного управління ДН Smart антен в динамічних середовищах, що в подальшому дозволить знайти нові підходи до управління ДН.

Виклад основного матеріалу

Для проведення аналізу оцінки ефективності існуючих адаптивних алгоритмів управління ДН, що застосовуються у Smart антенах на рухомих об’єктах, у роботі застосовується комплексний підхід за наступними критеріями оцінювання [8; 9]:

час адаптації, тобто здатність алгоритму забезпечити швидке перелаштування ДН Smart антени у відповідь на зміну положення рухомого об’єкта в просторі для підтримання стабільного зв’язку в динамічних умовах функціонування;

точність наведення, спроможність досліджуваних алгоритмів забезпечити формування ДН у напрямку цільового джерела сигналу з мінімальними відхиленнями від оптимальної траєкторії наведення);

обчислювальні ресурси (визначення вимог до обчислювальної потужності та ресурсів системи, необхідних для функціонування конкретного алгоритму в режимі реального часу);

придатність до роботи в реальному часі, що визначає здатність роботи алгоритму в умовах динамічного середовища.

В результаті аналізу наукових досліджень визначено, що для формування та управління ДН Smart антен на рухомих об'єктах, як правило застосовуються адаптивні алгоритми, які наведено нижче:

1. NLMS (NormalLeast Mean Squares).
2. RLS (Recursive Least Squares).
3. Левенберга – Марквардта (Levenberg-Marquardt Algorithm).
4. PSO (Particle Swarm Optimization/ метод чисельної оптимізації).
5. Генетичні алгоритми (ГА).
6. MUSIC-WAA (Multiple Signal Classification – Weighted Average Algorithm).

Вибір саме цих алгоритмів обумовлений необхідністю комплексного охоплення методів із різною складністю, структурою та підходами до оптимізації.

Для аналізу вищенаведених алгоритмів необхідно детально розглянути їх механізми відносно рішення задачі адаптивного управління ДН.

NLMS-алгоритм (Normal Least Mean Squares) [10] є основним представником класу стохастичних градієнтних алгоритмів адаптивної фільтрації, що базується на теорії Вінерівської фільтрації із застосуванням методу найменших квадратів для мінімізації середньоквадратичної похибки. На відміну від детерміністичних методів оптимізації, LMS використовує стохастичну оцінку градієнта цільової функції, що забезпечує простоту реалізації та стійкість в умовах нестаціонарного сигнального середовища. Також необхідно зазначити, що LMS є одним із фундаментальних алгоритмів, який застосовується для адаптивного управління ДН Smart антен. Кожна ітерація LMS-алгоритму включає три основні етапи послідовної обробки:

Етап 1. На першому етапі алгоритму відбувається процес обчислення вихідного сигналу фільтра $y(n)$ на основі лінійної комбінації зважених вхідних відліків :

$$y(n) = \sum_{i=0}^{N-1} w_i(n)x(n-i) = w^T(n)x(n)b, \quad (1)$$

де $w_i(n) - i$-й ваговий коефіцієнт адаптивного фільтра в момент часу n, визначає амплітудно-фазове зважування відповідного елемента антенної решітки; $x(n-i)$ – затримка на i тактів вхідної вибірки сигналу; N – порядок фільтра (кількість вагових коефіцієнтів); $y(n)$ – вихідний сигнал адаптивного фільтра сформованої ДН.

Етап 2. На другому етапі розраховується значення миттєвої похибки між еталонним та вихідним сигналами:

$$e(n) = d(n) - y(n), \quad (2)$$

де $e(n)$ – сигнал похибки в момент часу n, що характеризує відхилення від оптимального Вінерівського рішення; $d(n)$ – еталонний сигнал в момент часу n, який може представляти відомий сигнал корисного джерела або результат попередньої обробки.

Етап 3. На третьому етапі відбувається корекція вектора вагових коефіцієнтів фільтра на основі градієнтного спуску:

$$w(n+1) = w(n) + 2\mu e(n)x(n), \quad (3)$$

де μ – параметр збіжності (розмір кроку) LMS-алгоритму, $0 < \mu < \frac{1}{\lambda_{max}}$, λ_{max} – максимальне власне значення кореляційної матриці, яка визначає швидкість адаптації та стійкість алгоритму; $w(n+1)$ – вектор вагових коефіцієнтів на наступній ітерації; $w(n)$ – поточний вектор вагових коефіцієнтів; $x(n) = [x(n), x(n-1), \dots, x(n-N+1)]^T$ – вектор вхідних даних, що містить поточну та попередні $N-1$ вибірок.

Властивості збіжності та стійкості LMS-алгоритму визначаються вибором параметра μ. Для забезпечення збіжності в середньому квадратичному необхідно дотримуватись умови:

$$0 < \mu < \frac{2}{3 \cdot tr[R]}, \tag{4}$$

де $tr[R]$ – слід кореляційної матриці вхідного сигналу.

Часові константи збіжності для i-го вагового коефіцієнта визначаються як:

$$\tau_i = \frac{1}{2\mu\lambda_i}, \tag{5}$$

де λ_i – i-те власне значення кореляційної матриці для статистичної оцінки нерівномірності збіжності різних мод сигналу.

Залишкова похибка після збіжності алгоритму становить:

$$\xi_{min} = \sigma_d^2 \left(1 - \sum_{i=0}^{N-1} \frac{\sigma_{di}^2}{\sigma_d^2 \lambda_i}\right) + \mu \sum_{i=0}^{N-1} \frac{\sigma_{di}^2}{\lambda_i}, \tag{6}$$

де σ_d^2 – потужність еталонного сигналу; σ_{di}^2 – потужність кросс-кореляції між еталонним сигналом та i-ю модою вхідного сигналу.

Основною перевагою LMS-алгоритму є його обчислювальна простота $O(N)$ операцій на ітерацію та стійкість до зміни параметрів сигнального середовища, проте, швидкість збіжності алгоритму обмежена розкидом власних значень кореляційної матриці вхідного сигналу та вибором компромісного значення параметра μ між швидкістю адаптації та залишковою похибкою в усталеному режимі.

Алгоритм RLS (Recursive Least Squares) [11] є реалізацією рекурсивної процедури методу найменших квадратів та одним з фундаментальних підходів в теорії адаптивної фільтрації. Ключова перевага алгоритму RLS, порівняно з методами на основі стохастичного градієнта, таким як LMS (Least Mean Squares), полягає у значно вищій швидкості збіжності. Ця властивість зумовлена тим, що на кожній ітерації алгоритм оновлює оцінку оберненої кореляційної матриці вхідного сигналу. Такий підхід дозволяє отримати більш точне наближення до оптимального вектора вагових коефіцієнтів фільтра. Кожна ітерація RLS-алгоритму включає чотири основних кроки:

1. На першому кроці відбувається формування ДН та обчислення вихідного сигналу антенної решітки:

$$y(n) = \overrightarrow{w^H}(n)\vec{x}(n) = \sum_{i=1}^{N} w_i^*(n) x_i(n), \tag{7}$$

де $w_i(n) = a_i(n) \cdot e^{j\Delta\psi_i(n)}$ – комплексний ваговий коефіцієнт *i*-го елемента КАР, що визначає амплітуду $a_i(n)$ та фазовий зсув $\Delta\psi_i(n)$; $\vec{x}(n)$ – вектор сигналів, прийнятих *N* елементами антенної решітки в момент часу *n*.

2. На другому кроці розраховується похибка адаптації для корекції напрямку наведення ДН:

$$e(n) = d(n) - y(n), \tag{8}$$

де $e(n)$ – сигнал похибки, що характеризує відхилення від оптимальної траєкторії наведення на цільове джерело сигналу $\phi_{s(t)}$; $d(n)$ – еталонний сигнал.

3. На третьому кроці обчислюється вектор коефіцієнта підсилення для адаптивного управління ДН:

$$\vec{k}(n) = \frac{\vec{P}(n-1)\vec{x}(n)}{\lambda + \overrightarrow{x^H}(n)\vec{P}(n-1)\vec{x}(n)}, \tag{9}$$

де $\vec{k}(n)$ – вектор коефіцієнта підсилення, що забезпечує оптимальну швидкість адаптації в умовах нестаціонарної сигнально-завадової обстановки; λ – фактор забування ($0.95 \leq \lambda \leq 1$), що визначає час адаптації алгоритму до зміни положення рухомого об'єкта.

4. На четвертому кроці відбувається адаптивне оновлення вагових коефіцієнтів та оберненої кореляційної матриці:

$$\vec{w}(n+1) = \vec{w}(n) + \vec{k}(n)e^*(n), \tag{10}$$

$$\vec{P}(n) = \frac{1}{\lambda}\left[\vec{P}(n-1) - \vec{k}(n)\overrightarrow{x^H}(n)\vec{P}(n-1)\right], \tag{11}$$

де $\vec{P}(n) \in C^{N\times N}$ – обернена кореляційна матриця, що забезпечує максимізацію відношення сигнал/(завада та шум) $SINR = \frac{P_s}{(P_i+P_n)}$ та формування нулів ДН в напрямках завад $\phi_i(t)$.

Основною перевагою RLS-алгоритму є його швидка збіжність, яка досягається завдяки значно більшій обчислювальній складності порівняно з LMS-алгоритмом.

Алгоритм Левенберга – Марквардта (Levenberg-Marquardt Algorithm) [12] (LMA) належить до методів нелінійної оптимізації типу найменших квадратів і поєднує переваги підходів Ґаусса – Ньютона та градієнтного спуску. У задачах адаптивного управління параметрами Smart антен, тобто вектором збуджень елементів (амплітудами й фазами), LMA забезпечує швидке та чисельно стійке наближення до оптимального значення. На відміну від класичних градієнтних методів, алгоритм характеризується квадратичною швидкістю збіжності до оптимуму завдяки апроксимації матриці Ґессе якобіаном у вигляді $J^\top J$. Сукупність цих властивостей робить LMA одним із часто застосованих інструментів оптимізації ДН Smart антен у динамічних середовищах. Кожна ітерація алгоритму охоплює п'ять базових кроків.

На першому кроці відбувається обчислення вектора похибок між еталонною та поточною ДН:

$$e(wk) = dtarget - y(w_k), \tag{12}$$

де $e(wk)$ – вектор похибок на k-й ітерації; $dtarget$ – еталонна ДН; $y(w_k) = A(\theta, \phi)w_k$ – поточна ДН, сформована за допомогою вагових коефіцієнтів w_k.

На другому кроці розраховується матриця якобіана для лінеаризації нелінійної залежності:

$$J_{ij} = \frac{\partial e_i}{\partial w_j} = -\frac{\partial y_i(w)}{\partial w_j}\Big|_{\boldsymbol{w=w_k}}, \tag{13}$$

де J – матриця якобіана розміром $M \times N$, що характеризує чутливість кожної компоненти похибки до зміни вагових коефіцієнтів; M – кількість точок оптимізації ДН; N – кількість елементів антенної решітки.

На третьому кроці обчислюється модифікована матриця Гессе з коефіцієнтом згасання, для забезпечення стійкості алгоритму:

$$H_{LM} = J^{TJ} + \lambda_k I, \tag{14}$$

де H_{LM} – модифікована матриця Ґессе; λ_k – коефіцієнт згасання $\lambda_k > 0$ для балансуванням вибору між методом Гаусса-Ньютона та градієнтним спуском; I – одинична матриця.

На четвертому кроці відбувається обчислення кроку оновлення вагових коефіцієнтів:

$$\Delta w_k = -(J^{TJ} + \lambda_k I)^{-1} J^{Te}(w_k), \tag{15}$$

де Δw_k – вектор приросту вагових коефіцієнтів для мінімізації цільової функції $F(w) = \frac{1}{2}|e(w)|^2$ з урахуванням коефіцієнта регуляризації.

На п'ятому кроці здійснюється адаптивне оновлення вагових коефіцієнтів та коефіцієнта згасання:

$$w_{k+1} = w_k + \Delta w_k, \tag{16}$$

$$\lambda_{k+1} = \begin{Bmatrix} \frac{\lambda_k}{\beta}, \text{якщо } F(w_{k+1}) < F(w_k); \\ \text{інакше } \lambda_k \cdot \beta, \end{Bmatrix}, \tag{17}$$

де β – коефіцієнт масштабування параметра демпфування для процесу автоматичного регулювання швидкості збіжності та стабільності алгоритму залежно від локальних властивостей цільової функції.

Основною перевагою LMA-алгоритму є його швидка збіжність та стійкість до поганої обумовленості матриці якобіана, однак це досягається за рахунок необхідності обчислення на кожній ітерації інверсії матриці $(J^{TJ} + \lambda_k I)$, що значно збільшує обчислювальну складність порівняно з простими градієнтними методами.

Алгоритм оптимізації роєм частинок (PSO) [13]. Оптимізація роєм частинок (PSO) є метаевристичним алгоритмом, який відтворює механізми колективної поведінки біологічних популяцій для глобальної оптимізації параметрів Smart антен. На противагу традиційним градієнтним методам, PSO оперує сукупністю потенційних рішень і використовує стохастичні оновлення параметрів, що в свою чергу, мінімізує «застрягання» в локальних екстремумах. Унаслідок цього, PSO широко розглядають як дієвий підхід до багатокритеріальної оптимізації ДН Smart антен у складній електромагнітній ситуації.

Принцип колективної взаємодії частинок у PSO базується на концепції розподіленого інтелекту, де кожна частинка i характеризується позицією xi *та швидкістю* vi *у просторі параметрів Smart антен. Позиція частинки відповідає вектору вагових коефіцієнтів антенних елементів* $wi = [wi1, wi2, \dots, wiN]^T$, а швидкість визначає напрямок та інтенсивність пошуку оптимальних параметрів ДН.

Важливим в алгоритмі PSO є механізм пам'яті та соціального навчання, який реалізується за рахунок збереження кращої індивідуальної позиції кожної частинки $p_{i^{best}}$ і глобальної позиції всього рою g^{best}. Перша – виконує роль індивідуальної когнітивної опори, стимулюючи експлуатацію локально знайдених високоякісних рішень, тоді як друга – роль соціальної опори, спрямованої на розширене дослідження простору параметрів і групування

траєкторій частинок у бік найкращої на поточний момент конфігурації. У сукупності вищенаведене забезпечує баланс між локальним вдосконаленням та глобальним пошуком і прискорює наближення рою до оптимальної конфігурації Smart антен.

Динаміка руху частинок описується системою рівнянь зі зворотнім зв'язком, що моделюють когнітивні та соціальні компоненти поведінки:

$$v_i^{(t+1)} = w \cdot v_i^{(t)} + c_1 \cdot r_1 \cdot \left(p_i^{best} - x_i^{(t)}\right) + c_2 \cdot r_2 \cdot \left(g^{best} - x_i^{(t)}\right), \quad (18)$$

$$x_i^{(t+1)} = x_i^{(t)} + v_i^{(t+1)}, \quad (19)$$

де w – коефіцієнт інерції контролю впливу попередньої швидкості частинок на поточний рух; c_1, c_2 – коефіцієнти прискорення когнітивної та соціальної компонент; r_1, r_2 – випадкові числа, які рівномірно розподілені на інтервалі $[0,1]$.

Стратегія адаптивного балансування між глобальним та локальним пошуком здійснюється шляхом динамічного регулювання параметрів алгоритму. Лінійне зменшення коефіцієнта інерції $w(t) = w_{max} - \frac{w_{max} - w_{min}}{t_{max}} \cdot t$ забезпечує інтенсивний пошуку статистичних закономірностей на початкових ітераціях та на завершальних стадіях оптимізації.

Функція оцінки якості для кожної частинки визначається як багатокритеріальна цільова функція:

$$f(x_i) = \alpha \cdot SLL(x_i) + \beta \cdot BW(x_i) + \gamma \cdot \eta(x_i), \quad (20)$$

де $SLL(x_i)$ – рівень бічних пелюсток ДН; $BW(x_i)$ – ширина головного променя; $\eta(x_i)$ – коефіцієнт використання антени; α, β, γ – вагові коефіцієнти важливості критеріїв.

Механізм оновлення вибору оптимальних рішень будується на основі процесу порівняння поточного значення цільової функції з історичними даними та глобальною статистикою рою. Це забезпечує збереження еліти рішень та направлену еволюцію популяції до оптимального налаштування параметрів Smart антен.

Основною перевагою PSO-алгоритму є його здатність до глобального пошуку оптимуму без потреби в обчисленні градієнтів та простота програмної реалізації, проте ефективність алгоритму суттєво залежить від правильного налаштування параметрів w, c_1, c_2 та розміру популяції для конкретної задачі оптимізації Smart антен.

Генетичний алгоритм (ГА) [14] належить до класу еволюційних обчислювальних методів, які ґрунтуються на принципах природної селекції та генетичної спадковості. Одним із ключових напрямів застосування ГА є задачі глобальної оптимізації, зокрема оптимізація параметрів Smart антен. Сутність методу полягає у формуванні та еволюційному вдосконаленні популяції потенційних рішень за допомогою операторів схрещування, мутації та селекції. Такий підхід дає змогу здійснювати пошук оптимальної конфігурації ДН антен у багатовимірному просторі параметрів.

Крім того, ГА вважається одним із найбільш ефективних алгоритмів для розв'язання комбінаторних задач оптимізації, зокрема за напрямком управління ДН антен, де параметри управління мають дискретний характер. Завдяки здатності до глобального пошуку, ГА забезпечує знаходження близьких до оптимальних рішень, навіть у складних нелінійних та багатокритеріальних задачах. Нижче розглянуто основні функції ГА.

Концепція кодування хромосом, передбачає представлення кожного індивіда популяції у вигляді хромосоми Ci, *що містить закодовані параметри вагових коефіцієнтів антенних елементів. Наприклад, для Smart антен з* N *елементами хромосома може бути представлена у двійковому коді як* $Ci = [bi1\ bi2 \dots b_{iL}]$, де $L = N \times m$ – загальна довжина хромосоми, m –

кількість біт для кодування одного вагового коефіцієнта. Декодування здійснюється за формулою:

$$w_{ij} = w_{min} + \frac{w_{max} - w_{min}}{2^m - 1} \cdot \sum_{k=0}^{m-1} b_{i(jm+k)} \cdot 2^k, \quad (21)$$

де w_{min}, w_{max} – границі допустимих значень вагових коефіцієнтів.

Механізм природної селекції в генетичному алгоритмі реалізується за рахунок функції пристосованості (fitness function), суть якої полягає у процесі оцінки якості кожної хромосоми відповідно до критеріїв оптимізації ДН:

$$F(C_i) = \frac{1}{1 + f(w_i)}, \quad (22)$$

де $f(w_i)$ – цільова функція, що може включати рівень бічних пелюстків SLL, коефіцієнт направленості D, ширину головного променя та інші характеристики Smart антен.

Оператор схрещування (кросовер) забезпечує обмін генетичною інформацією між батьківськими хромосомами для створення нащадків. Одноточковий кросовер, з імовірністю $p_c \in [0.6, 0.9]$, реалізується наступним чином:

$$Cchild1 = \left[Cparent1[1:k], Cparent2[k+1:L]\right] Cchild2 = \left[Cparent2[1:k], Cparent1[k+1:L]\right], \quad (23)$$

де k – випадково вибрана точка розрізу хромосоми.

Оператор мутації вносить випадкові зміни в генетичний код для підтримання різноманітності популяції та запобігання передчасної конвергенції до локальних оптимумів. Бітова мутація, з імовірністю $p_m \in [0.001, 0.1]$, змінює значення окремих генів:

$$b'_{ij} = \begin{cases} \overline{b_{ij}}, \text{якщо } rand\ (), < p_m \\ b_{ij}, \text{ інакше} \end{cases}, \quad (24)$$

де $\overline{b_{ij}}$ – інверсне значення біта.

Стратегія формування нового покоління базується на принципах елітизму та турнірної селекції. Елітна стратегія забезпечує збереження найкращих індивідів поточного покоління:

$$P_{elite} = C_i : F(Ci) \geq Fthreshold, \quad (25)$$

де $F_{threshold}$ – поріг пристосованості для відбору еліти.

Критерії припинення еволюції можуть включати досягнення максимальної кількості поколінь G_{max}, стагнацію найкращого рішення протягом G_{stag} поколінь або досягнення заданого рівня пристосованості F_{target}.

Адаптивне управління параметрами GA реалізується через динамічне регулювання ймовірностей кросоверу та мутації залежно від різноманітності популяції:

$$p_c(t) = p_{c,max} - \frac{p_{c,max} - p_{c,min}}{G_{max}} \cdot t, \quad (26)$$

$$p_m(t) = p_{m,min} + \frac{p_{m,max} - p_{m,min}}{G_{max}} \cdot t \quad (27)$$

Багатокритеріальна оптимізація Smart антен може бути реалізована за допомогою алгоритму NSGA-II (Non-dominated Sjrting Genetic Algoritm) [15], що дозволяє одночасно оптимізувати кілька субоптимальних цілей, таких як мінімізація рівня бічних пелюстків та максимізація коефіцієнта підсилення антени.

Основною перевагою генетичного алгоритму є його здатність здійснювати глобальний пошук оптимального розв'язку у багатомодальних функціях, що дає змогу уникнути передчасної збіжності до локальних екстремумів. На відміну від градієнтних методів, ГА не потребує аналітичної або чисельної інформації про похідні цільової функції, що робить його ефективним інструментом для задач, де функція є недиференційованою, шумною або має складну топологію. Додатковою сильною стороною алгоритму є можливість паралельної обробки популяції, що підвищує ефективність пошуку у багатовимірному просторі параметрів.

Разом із тим, застосування ГА супроводжується низкою обмежень. Зокрема, досягнення високої якості результатів вимагає виконання великої кількості обчислень функції пристосованості. Крім того, ефективність алгоритму істотно залежить від належного вибору його параметрів, таких як: розміру популяції, ймовірностей схрещування та мутації, а також критеріїв зупинки.

Алгоритм MUSIC-WAA (Multiple Signal Classification – Weighted Average Algorithm) [16] є представником класу удосконалених спектральних методів високої роздільної здатності, що базується на основі механізму адаптивного зваженого усереднення, для підвищення точності оцінювання напрямків приходу сигналів у багатоелементних антенних решітках. На відміну від класичного MUSIC, який потребує повного спектрального сканування, MUSIC-WAA оптимізує побудову псевдоспектра й зменшує обчислювальну складність більш ніж на 99,9 % за кутової роздільної здатності 0.1°. На основі вищевикладеного, підхід MUSIC-WAA розглядається як один із найбільш перспективних для реалізації систем радіопеленгації в реальному часі на основі рівномірних кільцевих антенних решіток. Алгоритм складається з 7 основних етапів, які наведено нижче.

Етап 1. Формування сигнальної моделі та початкових параметрів. Для розуміння процесів роботи алгоритму необхідно розглянути на прикладі математичної моделі системи Smart антен з M-елементною антенною решіткою, що приймає D некорельованих сигналів із напрямків $\theta_1, \theta_2, \dots, \theta_D$:

$$x(t) = A(\theta)s(t) + n(t), \tag{28}$$

де $x(t) \in C^{M\times 1}$ – вектор спостережень антенної решітки в момент часу t; $A(\theta) = [a(\theta_1), a(\theta_2), \dots, a(\theta_D)] \in C^{M\times D}$ – матриця керуючих векторів; $s(t) \in C^{D\times 1}$ – вектор комплексних амплітуд джерел випромінювання сигналу; $n(t) \in C^{M\times 1}$ – вектор адитивного білого гаусівського шуму з дисперсією σ_n^2.

Процес обчислення керуючого вектора для k-го джерела у випадку лінійної еквідистантної решітки визначається за рівнянням:

$$a(\theta_k) = \left[1, e^{-j\frac{2\pi d}{\lambda}sin\,\theta_k}, \dots, e^{-j(M-1)\frac{2\pi d}{\lambda}sin\,\theta_k}\right]^T, \tag{29}$$

де d – відстань між сусідніми елементами решітки; λ – довжина хвилі випромінювання.

Етап 2. На відміну від класичного MUSIC, що використовує рівномірне усереднення, алгоритм MUSIC-WAA впроваджує концепцію адаптивного зважування за рахунок обчислення вектора оптимальних вагових коефіцієнтів $w = [w_1, w_2, \dots, w_L]^T$ рівняння:

$$\hat{R}\text{xx}^{\text{classical}} = \frac{1}{\text{L}}\sum l = 1^{L} x(l)x^{H}(l), \tag{30}$$

$$\hat{R}\text{xx}^{\text{WAA}} = \sum l = 1^{L} w_l x(l)x^{H}(l) \tag{31}$$

де $\sum_{l=1}^{L} w_l = 1$ – вагові коефіцієнти, що задовольняють умовам нормалізації та невід'ємності $w_l \geq 0, \forall l$.

Етап 3. На третьому етапі відбувається пошук оптимальних вагових коефіцієнтів, які визначаються шляхом розв'язання задачі мінімізації відхилення від ідеального шумового підпростору:

$$w^* = arg\min_{w}\left\{tr\left[W\left(U_n^{(w)}\widehat{U_n^{(w)H}} - U_n^{ideal}U_n^{idealH}\right)^2\right]\right\}, \tag{32}$$

за умов: $\sum_{l=1}^{L} w_l = 1,\ w_l \geq 0, l = 1,2,\dots,L,$

де W – додатково-визначена вагова матриця; $\widehat{U_n^{(w)}}$ – оцінка матриці власних векторів шумового підпростору для зваженої кореляційної матриці.

Етап 4. На цьому етапі відбувається ітераційне обчислення оптимальних вагових коефіцієнтів на основі експоненційного зважування:

$$w_l^{(k+1)} = \frac{w_l^{(k)}\, exp\left(-\alpha\frac{\partial f\left(w^{(k)}\right)}{\partial w_l}\right)}{\sum_{i=1}^{L} w_i^{(k)}\, exp\left(-\alpha\frac{\partial f\left(w^{(k)}\right)}{\partial w_i}\right)}, \tag{33}$$

де $\alpha > 0$ – параметр регуляризації, що контролює швидкість збіжності ітераційного процесу; k – номер ітерації; $f(w)$ – цільова функція оптимізації.

Початкова ініціалізація здійснюється за законом рівномірного розподілу: $w_l^{(0)} = \frac{1}{L}, \forall l$.

Етап 5. Власна декомпозиція зваженої кореляційної матриці. Далі на етапі 5 виконується процес власного розкладу зваженої кореляційної матриці:

$$\widehat{R_{xx}^{WAA}} = \widehat{U_s}\widehat{\Lambda_s}\widehat{U_s^H} + \widehat{U_n}\widehat{\Lambda_n}\widehat{U_n^H}, \tag{34}$$

де $\widehat{U_s} \in C^{M\times D}$ – матриця власних векторів сигнального підпростору (відповідають D найбільшим власним значенням); $\widehat{U_n} \in C^{M\times(M-D)}$ – матриця власних векторів шумового підпростору.

Етап 6. Формування адаптивно-зваженого псевдоспектра. На шостому етапі відбувається процес обчислення псевдоспектра MUSIC-WAA з використанням адаптивних вагових коефіцієнтів для кожного власного вектора шумового підпростору:

$$P_{WAA}(\theta) = \frac{1}{\sum_{i=1}^{M-D}\beta_i\left|a^H(\theta)\widehat{u_n^{(i)}}\right|^2}, \tag{35}$$

де $\beta_i = \frac{\widehat{\lambda_s^{min}}}{\widehat{\lambda_n^{(i)}}+\gamma}$ – адаптивні вагові коефіцієнти власних векторів; $\widehat{\lambda_s^{min}}$ – мінімальне власне значення сигнального підпростору; $\widehat{\lambda_n^{(i)}}$ – i-те власне значення шумового підпростору; $\gamma > 0$ – параметр регуляризації для забезпечення чисельної стійкості.

Етап 7. На наступному етапі здійснюється процес визначення напрямку приходу сигналів, що визначаються як локальні максимуми псевдоспектра $P_{WAA}(\theta)$ за умови перевищення заданого порогу детекції:

$$\hat{\theta}\mathrm{k} = \arg\max \theta \in \Theta\, P_{WAA}(\theta), k = 1,2, \dots, D, \tag{36}$$

де Θ – область пошуку кутових напрямків.

Критерії збіжності алгоритму включають досягнення максимальної кількості ітерацій K_{max} або виконання умови стагнації:

$$\left|w^{(k+1)} - w^{(k)}\right|_2 < \epsilon\,, \tag{37}$$

де ϵ – заданий поріг збіжності.

Основною перевагою MUSIC-WAA є підвищена роздільна здатність та стійкість до кореляційних спотворень завдяки адаптивному зважуванню спостережень та оптимізації підпросторових проєкцій.

Отже, у результаті дослідження проведено узагальнення відомих методів управління ДН Smart антен, зокрема алгоритмів LMS/NLMS, RLS, Левенберга – Марквардта, MUSIC, GA та PSO. Встановлено, що стохастичні методи LMS/NLMS забезпечують прийнятну швидкодію при низьких обчислювальних витратах, рекурсивні методи RLS відзначаються високою точністю, проте мають підвищену складність, тоді як еволюційні підходи (GA, PSO) і MUSIC доцільно застосовувати у стаціонарних або слабкодинамічних умовах.

Висновки. Таким чином, проведене дослідження дозволило комплексно проаналізувати сучасні підходи до адаптивного управління ДН Smart антен, що функціонують на рухомих об'єктах у динамічному середовищі. Встановлено, що ефективність системи зв'язку значною мірою визначається здатністю алгоритму швидко та точно реагувати на зміну просторового положення антенних елементів, характеристик сигналу та завад. Здійснений аналіз засвідчив, що класичні методи, зокрема LMS/NLMS і RLS, забезпечують прийнятну швидкодію та точність в умовах обмежених ресурсів, проте їх продуктивність суттєво знижується при високій мобільності та багатопроменевості середовища.

Алгоритми на основі стохастичної оптимізації, такі як Particle Swarm Optimization (PSO) та Генетичні алгоритми (ГА), продемонстрували потенціал у глобальному пошуку оптимальних фазових і амплітудних параметрів, однак відзначаються підвищеною обчислювальною складністю та затримкою адаптації. Методи спектральної оцінки, MUSIC і MVDR, забезпечують високу просторову роздільну здатність і точність визначення напрямку приходу сигналів (DOA), проте їхня ефективність зменшується при наявності шумів, корельованих джерел і швидких змін положення антени.

Результати порівняльного аналізу підтвердили, що найкращим компромісом між швидкістю адаптації, стабільністю та точністю управління є алгоритми класу NLMS, які здатні динамічно оновлювати вагові коефіцієнти антен з мінімальними обчислювальними витратами. Водночас, їх застосування обмежується лінійністю моделі середовища, що не враховує нелінійні ефекти відбиттів, дифракції та багатопроменевості.

Тому, **напрямком подальших досліджень** є визначення оптимального алгоритму управління ДН в умовах динамічного середовища з урахуванням завадової обстановки, за допомогою стохастичної моделі випадкового переміщення типу Random Waypoint (RWP) та застосуванням мови програмування Python для імітаційного моделювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zhu J., Fan K., He Q., Ye J., Fan A. Two-Dimensional Real-Time Direction-Finding System for UAV RF Signals Based on Uniform Circular Array and MUSIC-WAA. *Drones.* 2025. №9 (4). P. 278. DOI: 10.3390/drones9040278. URL: https://www.mdpi.com/2504-446X/9/4/278 (date of access: 21.10.2025).

2. Shubber Z. A., Abbas N. H., Kadhim H. T. Innovative Approaches to Beamforming Antenna Array Using PU-NLMS Algorithms. *e-Prime – Advances in Electrical Engineering, Electronics and Energy.* 2024. P. 100855. DOI: 10.1016/j.prime.2024.100855.

3. Lu Q., He Y., Yu R., Huang H. A Fast and Robust Variable-Step-Size LMS for Wideband Interference Cancellation Systems. *Sensors.* 2023. № 23 (18). P. 7871. DOI: 10.3390/s23187871.

4. Bismor D., Ogonowski Z., Czyż K. Leaky Partial-Update LMS Algorithms in Application to Multichannel ANC. *Sensors.* 2023. № 23 (3). P. 1169. DOI: 10.3390/s23031169.

5. Schmidt R. Multiple Emitter Location and Signal Parameter Estimation. *IEEE Trans. Acoust., Speech, Signal Process.* 1986. № 34 (3). P. 276–280. DOI: 10.1109/TASSP.1986.1164317.

6. Roy R., Kailath T. ESPRIT–Estimation of Signal Parameters via Rotational Invariance Techniques. *IEEE Trans. Acoust., Speech, Signal Process.* 1989. № 37 (7). P. 984–995. DOI: 10.1109/29.32276.

7. Itare N., Thomas J.-H., Raoof K. Genetic Algorithm-Based Acoustic Array Optimization for Estimating UAV DOA Using Beamforming. Drones. 2025. Vol. 9, no. 2. P. 149. URL: https://doi.org/10.3390/drones9020149**.**

8. Vorobyov S. A. Principles of Minimum Variance Robust Adaptive Beamforming Design. *Signal Processing.* 2011. № 91 (12). P. 2748–2765. DOI: 10.1016/j.sigpro.2011.04.014.

9. Chen Y., Wiesel A., Eldar Y.C., Hero A. O. Shrinkage Algorithms for MMSE Covariance Estimation. *IEEE Trans. Signal Process.* 2010. № 58 (10). P. 5016–5029. DOI: 10.1109/TSP.2010.2053029.

10. Tan K., Litva J., Chetty P.R. Performance of a Circular Array with Phase-Mode Excitation. Defence R&D Canada–Ottawa, Tech. Note TN 2002-001. 2002. URL: https://apps.dtic.mil/sti/pdfs/ADA403393.pdf (date of access: 14.10.2025).

11. Wong K. T., Zoltowski M. D. Root-MUSIC-based 2-D DoA Estimator Using Uniform Circular Arrays with Mode-Space Pre-Processing. *IEE Proc. – Radar, Sonar and Navigation.* 2000. № 147 (4). P. 179–184. DOI: 10.1049/ip-rsn:20000576.

12. Van Trees H. L. Optimum Array Processing (Detection, Estimation, and Modulation Theory, Part IV). New York: Wiley, 2002. ISBN: 978-0-471-09390-4.

13. Haykin S. Adaptive Filter Theory. 5th ed. Upper Saddle River, NJ: Pearson, 2013. ISBN: 978-0-13-267145-3.

14. Günşen K., Karaaslan M. A Comprehensive Survey of Metaheuristic Optimization Methods for Antenna Array Synthesis. *International Journal of RF and Microwave Computer-Aided Engineering.* 2023. № 33 (8). P. e23688. DOI: 10.1002/mmce.23688.

15. Uzdiaev V. et al. Dual-Objective PSO for Microstrip Patch Antenna Arrays: SLL and Beamwidth Control. *IEEE Access.* 2024. № 12. DOI: 10.1109/ACCESS.2024.

16. Rout D. K. et al. FANET Routing Protocol Analysis for Multi-UAV-Based Systems: A Comprehensive Survey. *Drones.* 2023. № 7 (11). P. 700. DOI: 10.3390/drones7110700.

DOI: 10.58254/viti.8.2025.20.257

УДК 681.35

канд. техн. наук Хусаінов П. В. ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)
Терещенко Т. П. ORCID: 0000-0002-9659-7897 (ВІТІ ім. Героїв Крут)
Череушенко В. Б. ORCID:0009-0006-2839-3637 (ВІТІ ім. Героїв Крут)

ФОРМУВАННЯ АЛЬТЕРНАТИВНИХ СТРАТЕГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ SERVER-SIDE WEB APPLICATION ІЗ ВРАХУВАННЯМ ЗМЕНШЕННЯ НЕВИЗНАЧЕНОСТІ

Тестування на проникнення (penetration testing) є одним із дієвих активних методів зниження ризиків компрометації системи шляхом експлуатації вразливості її програмних компонентів. В Україні поняття "тестування на проникнення" визначено як пошук та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. На сучасному етапі розвитку практики пошуку та виявлення вразливості системи (об'єкта кіберзахисту) цей процес базується на участі фахівця з тестування на проникнення. Понад усе він відповідає за правильне виявлення (доведення існування) вразливості системи (об'єкта кіберзахисту) на основі використання сучасного міжнародного досвіду для здійснення такої діяльності.

До розгляду пропонується постановка наукового завдання на розробку методичного апарату для вибору стратегій дій процесу тестування на проникнення. На основі використання запропонованого методичного апарату сформульовано задачу пошуку та виявлення вразливості системи (об'єкта кіберзахисту) за мінімальний (прийнятний) час за умови прийнятної (мінімальної) величини витрат ресурсів та визначеної ймовірності правильного виявлення вразливості системи (об'єкта кіберзахисту).

Оприлюднюються основні положення розробленого методичного апарату для вирішення задач тестування на проникнення: семантична мережа структурно-казуальних відношень між задачами досягнення тактичних цілей (тактик); обґрунтування на основі застосування підходів The Cyber Kill Chain, The Unified Kill Chain, Ethical Hacking Methodology, таксономій ATT&CK, CAPEC, CVE, CWE; інтерпретація в контексті логіко-психологічної схеми прийняття рішень; орієнтований граф граф-схеми дій фахівця; модель формування множини альтернативних стратегій. Надається змістовний метод стратегії дій фахівця з тестування на проникнення Server-Side Web Application системи (об'єкта кіберзахисту, в процесі якого здійснюється досягнення тактичної цілі (тактики) Initial Access на основі вирішення задачі Exploit Public-Facing Application.

Ключові слова: *тестування на проникнення, вибір рішень, альтернативні стратегії дій.*

P. Khusainov, T. Tereshchenko, V. Chereushenko. Formulation of alternative strategies for testing Server-Side Web Application penetration, taking into account the reduction of uncertainty

Penetration testing is one of the most effective active methods of reducing the risk of system compromise by exploiting vulnerabilities in its software components. In Ukraine, the concept of "penetration testing" is defined as the search for and identification of potential vulnerabilities in information (automated), electronic communication, information and communication systems, and electronic communication networks. At the current stage of development of the practice of searching for and identifying system vulnerabilities (cyber protection objects), this process is based on the participation of a penetration testing specialist. Above all, he is responsible for the correct identification (proving the existence) of system vulnerabilities (cyber protection objects) based on the use of modern international experience for carrying out such activities.

We propose to consider setting a scientific task to develop a methodological framework for selecting strategies for the penetration testing process. Based on the use of the proposed methodological apparatus, the task of searching for and detecting vulnerabilities in a system (cyber protection object) in a minimum (acceptable) amount of time has been formulated, subject to acceptable (minimum) resource costs and a defined probability of correctly detecting vulnera The main provisions of the developed methodological apparatus for solving penetration testing tasks are published: a semantic network of structural-causal relationships between tasks for achieving tactical goals (tactics); justification based on the application of The Cyber Kill Chain, The Unified Kill Chain, Ethical Hacking Methodology, ATT&CK, CAPEC, CVE, CWE taxonomies; interpretation in the context of a logical-psychological decision-making scheme; an oriented graph of a specialist's action scheme; a model for forming a set of alternative strategies. A meaningful method of a specialist's strategy for testing the penetration of a Server-Side Web Application system (cyber protection object) is provided, in the process of which the tactical goal (tactics) of Initial Access is achieved based on solving the Exploit Public-Facing Application task.bilities in the system (cyber protection object).

Keywords: *penetration testing, decision selection, alternative action strategies.*

Постановка завдання. Тестування на проникнення уособлює комплекс заходів оцінки захищеності об'єкта кіберзахисту від кіберзагроз, спрямований на доведення або заперечення твердження про можливість компрометації системи (об'єкта кіберзахисту) із застосуванням способів та засобів здійснення кібератак [1; 2]. Досягнення цілі тестування на проникнення уособлює методичний базис для здійснення:

пошуку та виявлення потенційних вразливостей інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж на основі публічної пропозиції [3];

перевірки ефективності здійснення заходів кіберзахисту об'єкта критичної інфраструктури від зовнішнього втручання не рідше одного разу на рік [4];

підтвердження відновлення штатного функціонування систем/мереж аудиту та перегляду діяльності, пов'язаної із реагуванням на кіберінциденти/кібератаки з використанням сил та засобів Держспецзв'язку або інших сил кіберзахисту [5].

Доведення можливості компрометації системи (об'єкта кіберзахисту) свідчить про її вразливість. Вразливість системи (об'єкта кіберзахисту) – властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режим функціонування системи (об'єкта кіберзахисту), здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів. Дослідник потенційної вразливості (далі – Дослідник) – фізична або юридична особа, яка здійснює пошук потенційної вразливості системи. Застосування Дослідником тактик, методів (способів, технік) та засобів кібератак на відміну від діяльності зловмисника (хакера, суб'єкта кібератаки) здійснюється з дотриманням певного етичного кодексу правил, зокрема, відмови від нанесення реальної шкоди (через порушення режиму функціонування, знищення, шифрування інформації і т. ін.).

На підставі викладеного пропонується змістовна постановка наукової задачі на розробку науково-методичного апарату вибору стратегії дій Дослідника в процесі пошуку та виявлення вразливості системи (об'єкта кіберзахисту), яка повинна забезпечувати:

мінімальну або допустиму величину часових витрат;

допустиму або мінімальну величини витрат ресурсів;

гарантовану ймовірність правильного виявлення вразливості за визначений час;

мінімальний вплив невизначеності.

Причинами невизначеності (неповноти, недостатності, обмеженості, неточності) інформації для вибору рішення Дослідником у процесі пошуку та виявлення вразливості системи (об'єкта кіберзахисту) можуть бути: неможливість точного передбачення наслідків рішень; неможливість повторення або експериментальної перевірки рішення; особа, яка приймає рішення, не має можливості контролю всіх факторів; наявність множини альтернативних рішень та необхідність вибору одного з них; низька якість початкової інформації постановки задачі та вибору рішення. Аналіз результатів експериментальних випробувань показав, що стратегії діяльності Дослідника, які спрямовані на виявлення вразливості *Server-Side Web Application,* мають найменший вплив невизначеності.

Аналіз публікацій. Для ознайомлення з принципами будови, категоріями вразливості *Server-side Web Application* (об'єкта кіберзахисту) з оцінками *Common Weakness Scoring System* та *Common Vulnerability Scoring System*, а також і методикою застосування критеріїв зменшення невизначеності при виборі варіанту стратегії в процесі пошуку та виявлення вразливості системи (об'єкта кіберзахисту) за величною часових витрат необхідно звернутися до [6–8]. Науково-методичний апарат, використаний для створення моделі формування множини альтернативних стратегій діяльності Дослідника в процесі пошуку та виявлення вразливості системи (об'єкта кіберзахисту), деталізується в [9; 10].

Формулювання мети статті. Метою статті є викладення постановки та напрямку вирішення наукової задачі вибору стратегії дій Дослідника в процесі пошуку та виявлення

вразливості системи (об'єкта кіберзахисту) на основі множини альтернативних стратегій за показниками величини часових витрат, величини витрат ресурсів та ймовірності правильного виявлення вразливості за визначений час. Центральним елементом викладення є обґрунтування моделі формування множини альтернативних стратегій діяльності Дослідника на основі зваженого ймовірнісно-часового орієнованого графа.

Основна частина. Виявлення вразливості системи (об'єкта кіберзахисту) є результатом психологічної діяльності Дослідника та її головною ціллю. Поняття "ціль" уособлює очікуваний (ідеалізований, уявний) результат психологічної діяльності людини на певному інтервалі часу. Формулювання цілі (постановка задачі) є наслідком певного стимулу змінити поточну ситуацію у потрібному напрямку з урахуванням набутого досвіду. Постановка задачі характеризується використанням кількісних даних (параметрів) очікуваного результату на відміну від більш ідеалізованого (уявного) формулювання цілі. Під поняттям "ситуація" розглядається деякий узагальнений стан (актуальний опис поточного стану предметної області, визначений на певному часовому інтервалі), що змінюється за результатом вирішення задачі. Вирішення задачі у загальному вигляді є послідовністю дій щодо формування варіантів рішення, вибору та реалізації одного з них.

Вибір рішення є прерогативою людини і принципово не може мати формального подання. Особа, яка приймає рішення (Дослідник потенційної вразливості), керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб'єктивними уявленнями, судженнями, емоціями. Прямий чи опосередкований вплив на вибір особи, яка приймає рішення, може мати психологічні властивості, які не є вродженими і з розвитком особистості змінюються (формуються) залежно від конкретних суспільно-історичних умов: світогляду (система поглядів на суспільство та природу явищ); інтересів (спрямованість на певні предмети та явища); здібностей (індивідуальні особливості – умови успішного виконання якої-небудь однієї або кількох видів діяльності); темпераменту; характеру; уваги (спрямованість свідомості на певний предмет або діяльність: стійкість, перемикання, розподіл та об'єм).

Розрізняють два широких класи задач вибору рішень при неповній інформації про задачу та проблемну ситуацію. Перший клас задач відомий як "прийняття рішень в умовах ризику", другий – "прийняття рішень в умовах невизначеності". Неповнота інформації для вибору рішення 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. Можуть бути відома деяка кінцева кількість значень кожної величини, але без відповідних функцій розподілу ймовірностей.

Етап реалізації рішення полягає у виконанні операцій за планом обраної стратегії дій на етапі вибору рішення досягнення цілі (вирішення задачі). Реалізація рішення зазвичай здійснюється в умовах можливого прояву внутрішніх та зовнішніх дестабілізуючих факторів, що викликає певну невідповідність фактичного результату очікуваному. Визначення такої невідповідності, аналіз причин та вироблення рекомендацій щодо її усунення (зменшення) на наступному циклі управління уособлює етап оцінювання результату (вирішення задачі).

Сформулюємо наукову задачу пошуку та виявлення Дослідником потенційної вразливості (об'єкта кіберзахисту). *Необхідно* довести існування вразливості (об'єкта кіберзахисту) за найменшу $min\,T$ або граничну величину $T \le T_{\circ}$ сумарних часових витрат при обмеженні на витрату ресурсів $C \le C_{\circ}$ або їх мінімальну величину $min\,C$ за умови, що ймовірність правильного виявлення вразливості системи (об'єкта кіберзахисту) буде не менше певного граничного значення$P(T \le T_{\circ}) \ge P_{\circ}$.

Вирішення сформульованої наукової задачі полягає у виборі такого варіанта стратегії діяльності Дослідника (потенційної вразливості) в процесі пошуку та виявлення потенційної вразливості (об'єкта кіберзахисту) з множини альтернативних стратегій A, при якому буде

забезпечено $min\,T$при обмеженні $C \le C_{\circ}$ або $min\,C$ при обмеженнях $T \le T_{\circ}$ із забезпеченням $P(T \le T_{\circ}) \ge P_{\circ}$. Під поняттям "стратегія дій Дослідника" уособлюється один із можливих варіантів виконання Дослідником дій для забезпечення послідовності операцій рішення задач, спрямованих на досягнення головної цілі у формі доведення вразливості системи (об'єкта кіберзахисту) через досягнення сукупності тактичних цілей (тактик).

Потужність множини A визначається можливістю Дослідника здійснити застосування всієї сукупності комбінацій технік (методів, способів) кібератак для одержання результатів (вирішення задач) досягнення тактичних цілей (тактик) і доведення факту існування вразливості як головного результату процесу пошуку та виявлення вразливості системи (об'єкта кіберзахисту). Методичний базис предметної області (відношення між поняттями, що утворюють єдину основу для одноманітного розуміння рішення задачі), який обумовлює утворення множини альтернативних стратегій A діяльності Дослідника:

The Cyber Kill Chain – узагальнена послідовна схема кібератаки спрямована на нав'язування виконання шкідливого програмного засобу [11];

The Unified Kill Chain – узагальнена послідовна схема кібератаки за трьома циклічними фазами (*In, Through, Out*) її реалізації [12];

Ethical Hacking Methodology – схема кібератаки за методологією *Certified Ethical Hacker (CEH)* [13];

Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) – тактики (*tactics*), технік (*techniques*) кібератак на системи *Enterprise, Industrial Control System, Mobile* [14];

Common Attack Pattern Enumerations and Classifications (CAPEC) – система відношень понять абстрактного, стандартного та конкретно-технологічного рівня деталізації опису типових (шаблонних) механізмів технік (методів, способів) кібератак [15].

При ієрархічному представленні структурних відношень між поняттями утворюється деревоподібний граф, при мережевому представленні – граф типу "мережа". Структурні відношення понять застосовуються для визначення ієрархій або мереж понять, казуальні – причинно-наслідкові зв'язків (ланцюгів зв'язків), семантичні – для всіх інших можливих типів відношень. Семантична мережа є найбільш повною моделлю представлення знань про предметну область з використанням різнотипних відношень.

Діяльність людини характеризується деревом цілей. Дерево цілей є відображенням декомпозиції головної цілі в систему часткових цілей. Коренева вершина ієрархічного графа дерева цілей асоціюється з головною ціллю, вузлові вершини – з проміжними (частковими, тактичними) цілями, кінцеві (термінальні) вершини є відображенням первинних (елементарних) цілей. 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 (часткові, тактичні). Типовим фрагментом траєкторії діяльності є частково-впорядкована послідовність дій досягнення (головної, проміжної, первинної) цілі з деякої фіксованої початкової ситуації. Така частково-впорядкована послідовність дій розпочинається від перебування у відомому стані початкової ситуації, подібна казуальному сценарію та може розглядатися у контексті застосування стереотипних знань.

При використанні на семантичній мережі тільки структурних відношень вона перетворюється у мережу класифікації, при використанні тільки казуальних відношень – у сценарій. Сценарій – формалізований опис стандартної послідовності взаємозв'язаних фактів типової ситуації предметній області, послідовності дій або процедур досягнення цілей, тобто 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. 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. Сценарій класифікації призначений для структурованого відображення результатів узагальнення знань про предметну область. Для структуризації знань в 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 і 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 для одержання нових знань.

Успішним результатом доведення Дослідником існування вразливості є здійснення запуску на виконання демонстраційної шкідливої програми в обчислювальному середовищі будь-якого компонента (об'єкта кіберзахисту) з повноваженнями авторизованого користувача (рис. 1). Під поняттям "демонстраційна шкідлива програма" розглядається спеціальна форма реалізації в принципі широкого спектра функціональних можливостей абстрактної шкідливої програми без деструктивної частини її алгоритму (*payload*).

Казуальний сценарій пошуку та виявлення Дослідником потенційної вразливості системи (об'єкта кіберзахисту) розпочинається (рис. 1, П) з вирішення задач досягнення тактичної цілі (тактики) *Reconnaissance* (за методологією *ATT&CK*). Тактична ціль *Reconnaissance* полягає в одержанні (здобутті) Дослідником якомога повної інформації про систему (об'єкт кіберзахисту). Зокрема, визначається призначення, завдання, умови та штатний режим функціонування системи (об'єкта кіберзахисту), складові її інфраструктури (інтерфейси, структура мережного сегмента, сервіси, операційні системи і т.д.).

Успішним результатом досягнення тактичної цілі *Reconnaissance* є одержання (здобуття) Дослідником повної інформації для вирішення задач досягнення тактичної цілі (тактики) *Resource Development*, спрямованої на:

вибір методу (способу, техніки) запуску демонстраційної шкідливої програми шляхом вирішення задач досягнення тактичної цілі (тактики) *Initial Access*;

врахування можливості виконання демонстраційної шкідливої програми у складі вразливого компонента системи (об'єкта кіберзахисту) шляхом вирішення задач досягнення тактичної цілі (тактики) *Execution*;

забезпечення достатності умов для технічного ефекту доведення уразливості системи (об'єкта кіберзахисту) внаслідок виконання демонстраційної шкідливої програми шляхом вирішення задач досягнення тактичної цілі (тактики) *Penetration Testing Impact* (рис. 1, К).

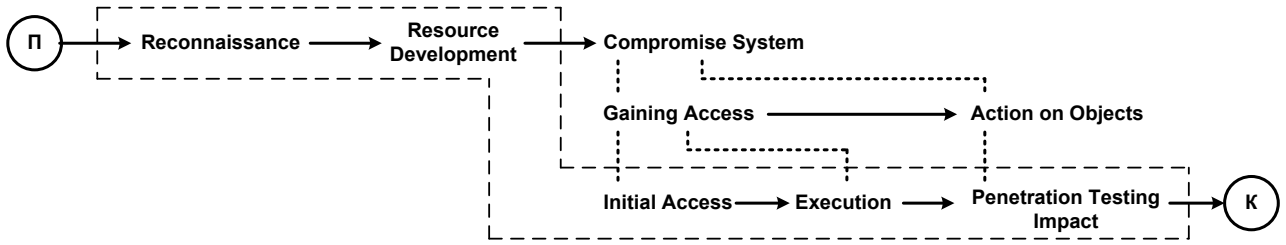


Рис. 1. Семантична мережа структурно-казуальних відношень цілеспрямованої діяльності Дослідника в процесі пошуку та виявлення вразливості системи (об'єкта кіберзахисту)

Для формування повного уявлення про предметну область семантична мережа структурно-казуальних відношень процесу пошуку та виявлення вразливості системи (об'єкта кіберзахисту) доповнена такими означеннями та співставленнями:

початок фази *Compromise System* за методологією *The Unified Kill Chain* та фази *Gaining Access*, відповідно, за методологією *CEH* співвідноситься з початком вирішення задач досягнення тактичної цілі (тактики) *Initial Access*;

початок фази *Action on Objects* за методологією *CEH* співвідноситься з початком вирішення задач досягнення тактичної цілі (тактики) *Penetration Testing Impact*.

Логіко-психологічна схема вирішення задачі за участю людини, яка приймає рішення (Дослідник потенційної вразливості), у загальному вигляді є послідовністю етапів інформаційної підготовки, вибору та реалізації рішення задачі. Етап інформаційної підготовки рішення уособлює сукупність операцій здобуття, обробки, аналізу інформації для ідентифікації ситуації вироблення множини альтернативних рішень.

Функціонально-динамічний підхід спрямований на дослідження комплексу психологічних механізмів вибору рішення людиною. Розумова діяльність людини розглядається як багаторівнева сукупність взаємозв’язаних процесів психофізичного, психологічного, гносеологічного та програмного характеру. Основні форми розумової діяльності: емпіричне, аксіоматичне, діалектичне. Емпіричне мислення базується на узагальненні попереднього досвіду, аксіоматичне – на застосуванні початкових знань про правила вирішення задачі. Діалектичне мислення є вищою формою психічних процесів людини, забезпечує позитивний прояв багатоваріантності, адаптації, самоорганізації, вибір рішення в умовах як повної, так і неповної інформації для вибору рішення.

Розглядаючи представлену семантичну мережу структурно-казуальних відношень предметної області як процес вирішення задачі пошуку та виявлення вразливості системи (об’єкта кіберзахисту) за участю людини (Дослідника), необхідно зазначити (рис. 2):

загальна тривалість вирішення задач досягнення тактичної цілі (тактики) *I.Reconnaissance* справедливо проінтерпретувати як етапи *інформаційної підготовки* і *вибору рішення*, вирішення комплексу взаємопов’язаних задач у процесі послідовного досягнення тактичних цілей (тактик) *II.Resource Development*, *III.Initial Access*, *IV.Execution*, *V.Penetration Testing Impact* як чотири послідовних фази етапу реалізації рішення доведення існування вразливості системи (об’єкта кіберзахисту);

можливість повернення до вирішення задач етапів інформаційної підготовки і вибору рішення (*I.Reconnaissance*) при недостатності (неповноті, невизначеності) інформації для якісної технічної підготовки реалізації рішення (рис. 2, *а*);

наявність принципової невизначеності другої (*III.Initial Access*) та третьої (*IV.Execution*) фаз етапу реалізації рішення обумовлює відповідного повернення та уточнення вирішення задач фази (*II.Resource Development*) технічної підготовки реалізації рішення (рис. 2, *б*).

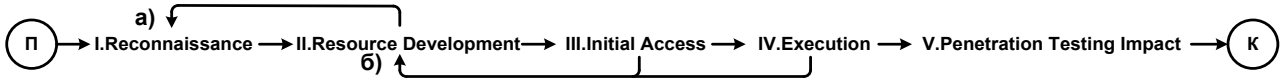


Рис. 2. Логіко-психологічна схема інформаційної підтримки вибору та реалізації рішень Дослідника в процесі пошуку та виявлення вразливості системи (об’єкта кіберзахисту)

Відповідно до визначеного напрямку вирішення наукової задачі сформуємо орієнтований граф граф-схеми алгоритму діяльності Дослідника. Вершини орієнтованого графа граф-схеми (рис. 2) уособлюють сукупність задач, спрямованих на досягнення тактичних цілей (тактик), відповідно, на етапах інформаційної підготовки, вибору та реалізації рішення (рис. 3) Дослідником (потенційної вразливості) у процесі пошуку та виявлення потенційної вразливості (об’єкта кіберзахисту).

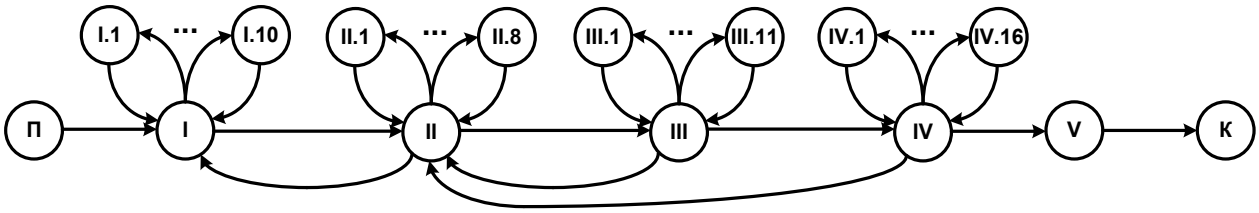


Рис. 3. Орієнтований граф граф-схеми алгоритму діяльності Дослідника в процесі пошуку та виявлення вразливості системи (об’єкта кіберзахисту)

Так, одержання (здобуття) необхідної Досліднику інформації з використанням специфічних засобів визначає десять категорій можливих методів (способів, технік) вирішення задач (рис. 3, I, I.1–I.10) досягнення Дослідником тактичної цілі (тактики) *Reconnaissance* (інформаційна підготовка і вибір рішень):

I.1. *Active Scanning* (сканування);

I.2. *Gather Victim Host Information* (ідентифікація хоста);

I.3. *Gather Victim Identity Information* (ідентифікація персоналій користувачів);

I.4. *Gather Victim Network Information* (ідентифікація мережної інфраструктури);

I.5. *Gather Victim Org Information* (ідентифікація організації);

I.6. *Phishing for Information* (фішинг);

I.7. *Search Closed Sources* (ідентифікація в приватних базах даних);

I.8. *Search Open Technical Databases* (ідентифікація в технічних базах даних);

I.9. *Search Open Websites/Domains* (ідентифікація зв’язаних вебресурсів/доменів);

I.10 *Search Victim-Owned Websites* (ідентифікація персоналій власників вебресурсів).

Відсутність необхідних засобів і/або незабезпечення необхідних умов визначає вісім категорій (рис. 3, II, II.1–II.8) можливих методів (способів, технік) вирішення задач досягнення Дослідником потенційної вразливості тактичної цілі (тактики) *Resource Development* (перша фаза етапу реалізації рішення, технічна підготовка):

II.1. *Acquire Access* (придбання легітимних повноважень);

II.2. *Acquire Infrastructure* (придбання легітимної інфраструктури);

II.3. *Compromise Accounts* (компрометація допоміжних легітимних облікових записів);

II.4. *Compromise Infrastructure* (попередня компрометація допоміжної інфраструктури);

II.5. *Develop Capabilities* (вибір, розробка засобів);

II.6. *Establish Accounts* (легітимізація облікових записів);

II.7. *Obtain Capabilities* (придбання засобів);

II.8. *Stage Capabilities* (розміщення засобів).

Впровадження одного з можливих методів (способу, техніки) запуску демонстраційної шкідливої програми має одинадцять категорій (рис. 3, III, III.1–III.11) вирішення такої задачі досягнення тактичної цілі *Initial Access* (друга фаза етапу реалізації рішення):

III.1. *Content Injection* (під час обробки *Specially Crafted Input* через канал клієнт-серверної комунікації);

III.2. *Drive-by Compromise* (під час обробки *Specially Crafted Input* при завантаженні з неконтрольованого джерела та використання за ініціативою користувача);

III.3. *Exploit Public-Facing Application* (під час обробки *Specially Crafted Input* в процесі клієнт-серверної комунікації з програмними засобами публічних інформаційних сервісів);

III.4. *External Remote Services* (під час обробки *Specially Crafted Input* в процесі клієнт-серверної комунікації з програмними засобами сервісів видаленої роботи);

III.5. *Hardware Additions* (під час обробки *Specially Crafted Input* в процесі підключення зовнішнього апаратного засобу за ініціативою користувача або технічного працівника);

III.6. *Phishing* (під час обробки *Specially Crafted Input* в процесі клієнт-серверної комунікації з програмними засобами оманних інформаційних сервісів та сервісів видаленої роботи за ініціативою користувача);

III.7. *Replication Through Removable Media* (під час обробки *Specially Crafted Input* в процесі підключення зовнішнього носія інформації за ініціативою користувача або технічного працівника);

III.8. *Supply Chain Compromise* (під час обробки *Specially Crafted Input* в процесі підключення апаратного засобу, і/або зовнішнього носія інформації, і/або використання програмного засобу, для якого не визначена безпека походження та надходження за ініціативою користувача або технічного працівника);

III.9. *Trusted Relationship* (під час обробки *Specially Crafted Input* в процесі клієнт-серверної комунікації з програмними засобами інформаційних сервісів та сервісів видаленої роботи, підключенні та використанні апаратного засобу, і/або зовнішнього носія інформації, і/або використання програмного засобу, для якого визначена неконтрольована категорія довіри, у тому числі за ініціативою користувача або технічного працівника);

III.10. *Valid Accounts* (шляхом використання повноважень авторизованого користувача через діючий обліковий запис для запуску на виконання програмних засобів);

III.11. *Wi-Fi Networks* (шляхом використання повноважень авторизованого комунікаційного пристрою бездротової локальної мережі).

Поняття "*Specially Crafted Input*" уособлює сукупність спеціально сформованих даних, які надаються для обробки алгоритму цільового програмного засобу (прикладного чи системного призначення) з метою прояву його вразливості (*vulnerability*) для нав'язування виконання негативного технічного ефекту (*negative technical impact*). Нав'язування негативного технічного впливу базується на можливості непередбаченого використання (експлуатації) певного дефекту (*weakness*) цільового програмного (програмно-апаратного) засобу, який за певних умов призводить до її вразливого стану (вразливості). Спробу експлуатації дефекту цільового програмного (програмно-апаратного) засобу з метою нав'язування йому вразливого стану для прояву негативного технічного ефекту прийнято називати атака (*attack*).

Дані *Specially Crafted Input* можуть бути заздалегідь підготовлені, розташовані у складі легітимного логічного об'єкта (файл даних, завантажувальний модуль, бібліотека, командний рядок, команда протоколу обміну даними, змінна, аргумент, структура, метод класу і т. ін.) та надані для обробки цільовим програмним (програмно-апаратним) засобом (прикладного чи системного призначення) з використанням певного носія інформації або у пам'яті апаратного пристрою. Іншою формою надання даних *Specially Crafted Input* для обробки є їх генерування в процесі комунікації з цільовим програмним (програмно-апаратного) засобом (прикладного чи системного призначення). Спеціальний програмний засіб, який здійснює генерування даних *Specially Crafted Input* в процесі комунікації прийнято називати експлойт (*exploit*).

Відомо понад 938 типових класів дефектів на етапах проєктування, реалізації, введення в експлуатацію, супроводження та завершення роботи програмних (програмно-апаратних) продуктів. Станом на 22.10.2025 обліковано 298 000 вразливостей за одинадцятьма категоріями: *Overflow* (перевищення ємності місць для розміщення даних) – 20 %; *Memory Corruption* (пошкодження пам'яті) – 20 %; *Sql Injection* (поява в запитах мовою *Structured Query Language* зовнішніх даних) – 9 %; *Cross-Site Scripting* (компрометація гіперпосилань) – 25 %; *Directory Traversal* (некоректна інтерпретація шляху у файловій системі) – 5 %; *File Inclusion* (нав'язування оброблення файлу з неконтрольованого джерела) – 1,5 %; *Cross-Site Request Forgery* (підміна суб'єкта доступу за запитом) – 6 %; *XML External Entity* (обробка зовнішніх об'єктів *eXtensible Markup Language*) – 1,5 %; *Server-side Request Forgery* (підміна суб'єкта доступу до довіреного сервісу) – 1,5%; *Open Redirect* (модифікація шляху доступу) – 1,5%; *Input Validation* (порушення фільтрації вхідних даних) – 9 %. Найбільш

характерні наслідки практичної експлуатації вразливості програмних (програмно-апаратних) продуктів та технологічних рішень (за останні 10 років обліковано 69833 кіберінциденти): *Code Execution* (виконання команд, програм із зовнішніх джерел) – 27 %; *Bypass* (подолання захисних механізмів) – 10 %; *Privilege Escalation* (розширення повноважень) – 14 %; *Denial of Service* (припинення функціонування) – 33 %; *Information Leak* (порушення конфіденційності інформації) – 16 %.

Близько 20 % категорій дефектів програм (196 із 940) таксономії *Common Weakness Enumeration (CWE)* та більше ніж 20 % вразливостей (63 324 з 298 000) таксономії *Common Vulnerabilities and Exposures (CVE)* відносяться до *Server-side Web Application* [16; 17].

Врахування придатності вразливого компонента (об'єкта кіберзхаисту) для виконання демонстраційної шкідливої програми визначає шістнадцять категорій (рис. 3, IV, IV.1–IV.16) можливого розширення обсягу технічної підготовки реалізації рішення шляхом необхідності додавання вирішення задач досягнення тактичної цілі (тактики) *Execution* (третя фаза етапу реалізації рішення):

IV.1. *Cloud Administration Command* (адміністрування хмарних сервісів);

IV.2. *Command and Scripting Interpreter* (командні інтерпретатори);

IV.3. *Container Administration Command* (адміністрування середовища контейнерізації);

IV.4. *Deploy Container* (розгортання контейнерної інфраструктури);

IV.5. *ESXi Administration Command* (адміністрування віртуальних машин);

IV.6. *Exploitation for Client Execution* (експлуатація вразливості клієнтських програм);

IV.7. *Input Injection* (використання інтерфейсу користувача);

IV.8. *Inter-Process Communication* (використання інтерфейсу взаємодії процесів);

IV.9. *Native API* (використання інтерфейсу системних викликів операційної системи);

IV.10. *Scheduled Task/Job* (адміністрування сервісів виконання за розкладом);

IV.11. *Serverless Execution* (використання інтерфейсу хмарних сервісів);

IV.12. *Shared Modules* (нав'язування виконання подільних бібліотек);

IV.13. *Software Deployment Tools* (адміністрування сервісів розгортання програм);

IV.14. *System Services* (використання сервісів виконання команд);

IV.15. *User Execution* (нав'язування користувачу виконання програм);

IV.16. *Windows Management Instrumentation* (експлуатація можливостей *WMI*).

Забезпечення достатності умов для технічного ефекту доведення уразливості системи (об'єкта кіберзахисту) внаслідок виконання демонстраційної шкідливої програми (*Penetration Testing Impact*) пропонується розглядати (рис. 3, V) у формі вирішення задачі досягнення тактичної цілі (тактики) *Command and Control* (за методологією *ATT&CK*), тобто утворення прихованого каналу обміну даними між командним інтерпретатором (з повноваженнями деякого авторизованого користувача) в обчислювальному середовищі вразливого компонента системи (об'єкта кіберзахисту) та терміналом автоматизованого робочого місця Дослідника.

Дуги орієнтованого графа граф-схеми алгоритму діяльності Дослідника в процесі пошуку та виявлення потенційної вразливості (об'єкта кіберзахисту) визначають напрямки переходів між вершинами (рис. 3), які:

уособлюють вирішення задач Дослідником у контексті досягнення відповідних тактичних цілей (тактик);

уособлюють етапи інформаційної підготовки і вибору та реалізації рішення Дослідника при наявності інформації необхідної якості для технічної підготовки реалізації рішення за напрямком завершення процесу або у зворотному напрямку у разі її неповноти.

Елементарними структурними елементами забезпечення зв'язності вершин є ланцюг, циклічний та паралельний контур. В якості прикладів ілюстрації таких елементарних структурних елементів можна розглянути, відповідно (рис. 3):

односпрямовану зв'язність вершин I, II та III (ланцюг);

циклічну зв'язність вершин I, I.1 або II, II.8 і т. д. (циклічний контур);

паралельну зв’язність вершин IV, II і III, II за умови паралельного об’єднання вершин III та IV (паралельний контур).

Перетворимо орієнтований граф граф-схеми у модель для формування множини альтернативних стратегій A діяльності Дослідника в процесі пошуку та виявлення потенційної вразливості (об’єкту кіберзахисту) шляхом означення її вершин показниками, де $i = \overline{1,n}$, $j = \overline{1,m}$, n – кількість задач, $m = 5$ – фази етапів інформаційної підготовки і вибору та реалізації рішення (рис. 2, 3):

середнього значення τ_{ij}та дисперсії $D(\tau_{ij})$величини часових витрат;

ймовірності одержання якісного результату вирішення задачі q_{ij} (у контексті досягнення відповідної тактичної цілі);

прогнозованою величиною необхідних ресурсів c_{ij}.

Дуги зв’язності вершин ізоморфні переходам між операціями вирішення задач Дослідником у процесі пошуку та виявлення потенційної вразливості (об’єкта кіберзахисту) і зважуються ймовірностями p_{lk} їх використання при побудові можливих шляхів просування граф-схемою, де $l,k = \overline{1,v}$, $l \neq k$, v– кількість вершин граф-схеми.

Формування множини альтернативних стратегій A здійснюється у два кроки. Перший крок реалізується шляхом імітаційного моделювання всіх можливих шляхів просування граф-схемою на основі оперування можливими значеннями ймовірностей q_{ij} та похідних від неї значень ймовірностей p_{lk} (в частині, яких стосується). Другий крок полягає у здійсненні перетворень елементарних структурних елементів (ланцюг, циклічний контур, паралельний контур) орієнтованого підграфа можливого шляху просування граф-схемою з обчисленням еквівалентних значень T, C та $P(T \leq T_{\circ})$для кожної альтернативної стратегії множини A. Науково-методичним апаратом побудови та перетворення орієнтованого графа граф-схеми процесу пошуку та виявлення Дослідником вразливості системи (об’єкта кіберзахисту) є:

структурно-алгоритмічний метод аналізу і синтезу діяльності;

функціонально-структурна теорія функціонування ергатичних систем;

ймовірнісно-часовий граф алгоритму діяльності оператора системи.

Рішенням буде вибір такої стратегії дій Дослідника (потенційного вразливості) в процесі пошуку та виявлення потенційної вразливості (об’єкта кіберзахисту) з таким еквівалентними значеннями T, C та $P(T \leq T_{\circ})$, які будуть задовольняти умовам сформульованої постановки наукової задачі. При наявності у зазначених показниках для множини альтернативних рішень ознак неоднозначності вибору використовуються критерії прийняття рішень в умовах невизначеності: мінімаксний (максимінний), Лапласа (Байеса-Лапласа), Севіджа, а також похідних від них Гурвіца, Ходжа-Лемана, Гермейера.

Адекватність запропонованого науково-методичного апарату вирішення поставленої задачі підтверджується результатами експериментальних випробувань класу стратегій діяльності Дослідника в процесі пошуку та виявлення вразливості *Server-side Web Application* (рис. 4) системи (кіберзахисту), які в якості обов’язкової фази реалізації рішення включають досягнення тактичної цілі (тактики) *Initial Access* на основі вирішення задачі *Exploit Public-Facing Application* (рис. 4, III.3). Достатня репрезентативність експериментальної бази підкреслюється охопленням більше ніж 63 324 категорій дефектів (проєктування, реалізації, налаштування) *Server-side Web Application* (більше 20 % записів *CVE*):

53 % – передавання на обробку небезпечних (некоректних) вхідних даних (об’єктів), надлишкова інформативність під час обробки некоректних (неправильних) запитів до системи керування базою даних;

30 % – некоректна зміна повноважень (недотримання принципу найменших привілеїв), маркерів доступу (функцій інтерфейсу прикладного програмування, посилань на об’єкти);

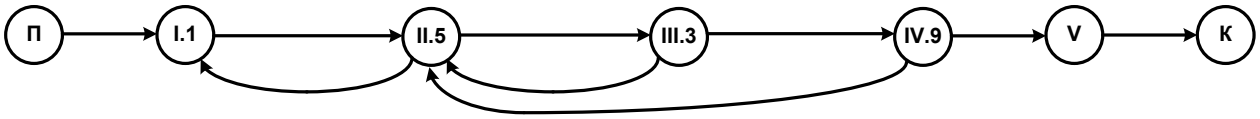


Рис. 4. Приклад орієнтованого графа граф-схеми діяльності Дослідника потенційної вразливості *Server-Side Web Application*

6 % – 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);

5 % – некоректна перевірка дійсності параметрів автентифікації, цифрових підписів програмних компонентів, запобігання надлишкової інформативності під час обробки некоректних криптографічних даних (ключів, векторів ініціалізації) при утворені менш стійких захищених каналів комунікації;

5 % – недотримання порядку *OWASP Software Assurance Maturity Model* під час розробки компонентів із застосуванням апробованих колекцій програмних компонентів).

Результати експериментальних випробувань в основному збігаються з положеннями та оцінками рейтингу *Top 10 Web Application Security Risks* під егідою *The Open Worldwide Application Security Project* [18].

Висновки. Необхідність ефективної організації пошуку та виявлення вразливості системи (об’єкта кіберзахисту) обумовило актуальну необхідність постановки наукового завдання на розробку науково-методичного апарату вибору стратегій діяльності Дослідника (потенційної вразливості) в умовах невизначеності. Основним напрямком вирішення наукового завдання є формування множини альтернативних рішень з оцінкою кожного з них за показниками часових, ресурсних витрат та ймовірністю правильного виявлення вразливості за визначений час. Надання Досліднику можливості вибору найкращої раціональної стратегії з автоматичним генеруванням послідовності операцій доведення існування вразливості є передумовою суттєвого покращення ефективності задач тестування на проникнення шляхом скорочення часового інтервалу етапу інформаційної підготовки.

Подальші дослідження здійснюються у напрямку розробки комплексу імітаційного моделювання множини альтернативних стратегій діяльності Дослідника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.10.2025).

2. NIST SP 800-115 Technical Guide to Information Security Testing and Assessment. URL: https://www.nist.gov/privacy-framework/nist-sp-800-115.

3. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: Постанова Каб. Міністрів України від 16.05.2023 № 497. URL: https://zakon.rada.gov.ua/laws/show/497-2023-п#Text (дата звернення: 28.10.2025).

4. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури: Постанова Каб. Міністрів України від 19.06.2019 № 518: станом на 7 верес. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 28.10.2025).

5. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі від 03.07.2023 № 570. URL: https://zakon.rada.gov.ua/rada/show/v0570519-23#Text.

6. 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: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2024. № 5. С. 204–214. DOI: 10.58254/viti.5.2024.

7. 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: збірник наукових праць // за заг. ред. Г. Д. Радзівілова. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2024. № 6. С. 264–274. DOI: 10.58254/viti.6.2024.

8. Хусаінов П. В., Черниш Ю. О., Терещенко Т. П. Зменшення невизначеності оцінки часу компрометації Server-Side Web Application об’єкта критичної інфраструктури // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2025. № 7. С. 232–242. DOI: 10.58254/viti.7.2025.21.232.

9. 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.

10. Герасимов Б. М., Камишин В. В. Організаційна ергономіка: методи і алгоритми дослідження та проєктування. К.: Інфосистем, 2009. 212 с.

11. The Cyber Kill Chain. URL: https://www.lockheedmartin.com/cyber/cyber-kill-chain.html.
12. The Unified Kill Chain. URL: https://www.unifiedkillchain.com.
13. Certified Ethical Hacker. URL: https://cert.eccouncil.org/certified-ethical-hacker.html.
14. Adversarial Tactics, Techniques & Common Knowledge. URL: https://attack.mitre.org.
15. Common Attack Pattern Enumerations and Classifications. URL: https://capec.mitre.org.
16. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org.
17. Common Weakness Enumeration. URL: https://cwe.mitre.org.
18. Open Worldwide Application Security Project. URL:https://owasp.org.

DOI: 10.58254/viti.8.2025.21.269

УДК 681.35

канд. техн. наук Хусаінов П. В. ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Штаненко С. С ORCID: 0000-0001-9776-4653 (ВІТІ ім. Героїв Крут)

ОБҐРУНТУВАННЯ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ФАХІВЦЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

До розгляду пропонується висвітлення основних положень науково-методичного апарату інформаційної підтримки фахівців із реагування на інциденти кібербезпеки, які виконують свої обов'язки у складі групи реагування на комп'ютерні надзвичайні події об'єкта критичної інфраструктури.

У першій змістовній частині статті оприлюднено: принципи будови об'єкта критичної інфраструктури з позиції системного аналізу; системні риси основних компонентів об'єкта критичної інформаційної інфраструктури у контексті реалізації управління; реалізація функціонування об'єкта критичної інфраструктури як процесу управління; констатація обов'язковості врахування наявності з'єднання внутрішньої комунікаційної системи з мережею Інтернет (публічний кіберпростір) для забезпечення трактів утворення каналів прямого (зворотного) зв'язку; особливості вироблення керуючих впливів на основі програмного, оптимального та адаптивного управління; особливості реалізації автоматичного та автоматизованого управління технологічним процесом; умови своєчасного вироблення органом управління об'єкта критичної інфраструктури правильних керуючих впливів; цикл управління технологічним процесом, ролі та функції компонентів його забезпечення; опис показника ефективності процесу управління.

Друга частина висвітлює такі аспекти дослідження: доцільність розгляду компонентів забезпечення циклу управління технологічним процесом як мережі масового обслуговування; зв'язок відмов основних компонентів об'єкта критичної інформаційної інфраструктури з погіршенням ефективності управління технологічним процесом; характеристика відмов із зазначенням можливості їх компенсації шляхом апріорного аналізу надійності; констатується непридатність зменшення апріорної невизначеності на етапі проєктування для компенсації відмов внаслідок несанкціонованого втручання у формі кібератак через публічний кіберпростір; необхідність реалізації інформаційної підтримки рішень фахівця з реагування на інциденти кібербезпеки на етапі експлуатації об'єкта критичної інфраструктури.

Ключові слова: *об'єкт критичної інфраструктури, процес управління, інформаційна підтримка рішень.*

P. Khusainov, S. Shtanenko. Justification of information support for specialists responding to cybersecurity incidents at critical infrastructure facilities

The following is proposed for consideration: highlighting the main provisions of the scientific and methodological apparatus for information support of cybersecurity incident response specialists who perform their duties as part of a computer emergency response team for critical infrastructure facilities.

The first substantive part of the article reveals: the principles of critical infrastructure facility design from the perspective of system analysis; the systemic features of the main components of critical information infrastructure facilities in the context of management implementation; the implementation of critical infrastructure facility operation as a management process; the statement of the necessity to take into account the connection of the internal communication system to the Internet (public cyberspace) to ensure the formation of direct (reverse) communication channels; features of the development of control influences based on programmatic, optimal, and adaptive management; features of the implementation of automatic and automated management of the technological process; conditions for the timely development of correct control influences by the management body of the critical infrastructure object; the cycle of technological process management, the roles and functions of its support components; description of the management process efficiency indicator.

The second part highlights the following aspects of the study: the feasibility of considering the components of the technological process management cycle as a mass service network; the relationship between the failure of key components of critical information infrastructure and the deterioration of technological process management efficiency; the characteristics of failures with an indication of the possibility of compensating for them through a priori reliability analysis; it is stated that reducing a priori uncertainty at the design stage is not suitable for compensating for failures due to unauthorized interference in the form of cyberattacks through public cyberspace; the need to implement information support for decisions made by specialists responding to cybersecurity incidents at the stage of critical infrastructure facility operation.

Keywords: *critical infrastructure facility, management process, information support for decisions.*

Постановка завдання. Останні зміни до Закону України “Про основні засади забезпечення кібербезпеки України” запровадили у нормативно-правове поле поняття “реагування на кіберінциденти” як структуровану сукупність дій, спрямованих на підготовку до кіберінцидентів, їх виявлення та аналіз, мінімізацію шкоди від кіберінциденту та запобігання їх повторенню у майбутньому. Забезпечення реагування на кіберінциденти (кібератаки, кіберзагрози) для об’єктів кіберзахисту, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об’єктів критичної інформаційної інфраструктури покладається на Національну систему реагування на кіберінциденти, кібератаки, кіберзагрози. Її організаційною основою є команди реагування на кіберінциденти, кібератаки, кіберзагрози або команди реагування на комп’ютерні надзвичайні події (Computer Security Incident Response Team, CSIRT). Введення у нормативно-правове поле означення “CSIRT” за термінологією The Forum of Incident Response and Security Teams (FIRST) спрямоване на гармонізацію (впровадження) нормативно-правового регулювання з урахуванням розподілу ролей, завдань, функцій та відповідальності публічного сектору, операторів, власників або розпорядників об’єктів критичної інформаційної інфраструктури, сумісності з відповідними стандартами Європейського Союзу та НАТО [1–4].

Об’єкт критичної інформаційної інфраструктури – інформаційна, електронна комунікаційна, інформаційно-комунікаційна або технологічна система, яка необхідна для стійкого та безперервного функціонування об’єкта критичної інфраструктури, істотно впливає на безперервність та стійкість процесу надання життєво важливих функцій та/або послуг та відсутній альтернативний об’єкт (спосіб) їх надання. До об’єктів критичної інфраструктури відносять об’єкти інфраструктури, системи (сукупність систем, їх частини), які забезпечують функції та/або послуги у сферах: урядування; енергозабезпечення; водопостачання, водовідведення; продовольчого забезпечення; охорони здоров’я; фармацевтичної промисловості; виготовлення вакцин, функціонування біолабораторій; розповсюдження інформації; електронних комунікацій; фінансів; транспорту; оборони, державної безпеки; правопорядку, правосуддя; цивільного захисту, порятунку; космічної діяльності; хімічної промисловості; дослідницької діяльності [5; 6].

Відповідно до чинного законодавства Державною службою спеціального зв’язку та захисту інформації України визначений рекомендаційний порядок реагування на кіберінциденти/кібератаки для суб’єктів Національної системи захисту критичної інфраструктури в контексті, що стосується забезпечення кіберзахисту об’єктів критичної інфраструктури. Безпосереднє виконання заходів порядку реагування на кіберінциденти/кібератаки (підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності) здійснюється фахівцями CSIRT операторів об’єктів критичної інфраструктури. Відповідні трудові функції фахівців CSIRT, а також необхідні для цього компетенції та результати навчання визначені у професійному стандарті “Фахівець з реагування на інциденти кібербезпеки” [7–9].

Сукупність факторів виникнення подій ненавмисного характеру та/або таких, що мають ознаки несанкціонованого втручання у функціонування об’єкта критичної інфраструктури (з відповідними можливими наслідками інциденту безпеки критичної інфраструктури) за допомогою засобів електронних комунікацій об’єкта критичної інформаційної інфраструктури у кіберпросторі, уособлює поняття “кіберінцидент/кібератака”. Реагування на кіберінциденти/кібератаки об’єкта критичної інформаційної інфраструктури спрямоване на недопущення (мінімізацію наслідків) порушення сталого, надійного та штатного режиму функціонування такого об’єкта та/або порушення безпеки критичної технологічної інформації в умовах кіберзагроз.

Аналіз останніх публікацій. Для ознайомлення з науково-методичним апаратом інформаційної підтримки рішень оператора технічної системи, зокрема фахівця з реагування

на інциденти інформаційної безпеки, необхідно звернутися до [10–12]. Призначення, цілі, задачі, принципи будови, структура, процеси діяльності та засоби CSIRT із розкриттям досвіду організації реагування на кіберінциденти/кібератаки, ролей, компетенції та необхідних умінь відповідної групи фахівців деталізується в [13; 14].

Формулювання мети статті. Метою статті є висвітлення напрямку дослідження наукових проблем забезпечення інформаційної підтримки прийняття рішень фахівців з реагування на інциденти кібербезпеки об'єктів критичної інформаційної інфраструктури.

Основна частина. Будь-яке порушення безперервності, стійкості, штатного режиму функціонування критичної інфраструктури чи окремого її об'єкта, реагування на яке потребує залучення додаткових сил і ресурсів, уособлює поняття "кризова ситуація". Негативний тренд розвитку кризової ситуації функціонування об'єкта критичної інфраструктури у часі може призвести до загрози для населення, суспільства, соціально-економічного стану, національної безпеки і оборони України. Якщо виникнення кризової ситуації стало наслідком незаконних дій, тоді такі дії називають несанкціонованим втручанням (у функціонування об'єкта критичної інфраструктури). Подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки несанкціонованого втручання у функціонування об'єкта критичної інфраструктури, прийнято називати "інцидент безпеки критичної інфраструктури".

Режим (умови та вимоги залежно від стану і динаміки розвитку ситуації) функціонування об'єкта критичної інфраструктури визначається її оператором. Оператор критичної інфраструктури є юридичною особою, що здійснює управління об'єктом критичної інфраструктури, відповідає за його поточне функціонування, захист та реагування на кризові ситуації. Захист критичної інфраструктури – всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації. Реагування на кризові ситуації визначається оператором критичної інфраструктури шляхом введення відповідного режиму для забезпечення стійкості об'єкта критичної інфраструктури за відповідних умов, обставин і чинників.

Функціонування об'єкта критичної інфраструктури (безперервне, стійке, штатне) повинно забезпечувати реалізацію важливих для національної безпеки функцій та/або послуг певного органу державної влади, місцевого самоврядування, установи, суб'єкта господарювання та організацій будь-якої форми власності. Спрямованість на досягнення цілі (цілей) національної безпеки (державний суверенітет; територіальна цілісність; демократичний конституційний лад; прогресивний демократичний розвиток; безпечні умови життєдіяльності і добробут її громадян) характеризує об'єкти критичної інфраструктури як цілеспрямовані системи.

Основною властивістю цілеспрямованої системи є її здатність до реалізації управління, тобто здійснення послідовності зміни стану об'єкта управління для досягнення цілі існування системи або одержання очікуваного результату на визначеному часовому інтервалі функціонування системи. Важливо зазначити, що тут поняття "система" застосовується для констатації використання системного підходу при розгляді об'єкта критичної інфраструктури безвідносно до його призначення, функцій та/або послуг.

Процес управління (послідовність переходів між станами об'єкта управління) має циклічний характер. Циклічність такого процесу забезпечується органом управління. Узагальнено цикл управління полягає у послідовному здійснені чотирьох складових етапів: формулювання цілі (постановка задачі); вибір рішення; реалізація рішення; оцінювання досягнення результату. Ціль – очікуваний (ідеалізований, уявний) результат психологічної діяльності людини (органу управління) на певному інтервалі часу. Формулювання цілі

виникає як певний стимул змінити поточну ситуацію (процесу управління) у потрібному напрямку з урахуванням набутого досвіду. Постановка задачі характеризується використанням кількісних даних (параметрів) очікуваного результату на відміну від більш ідеалізованого (уявного) формулювання цілі. При формулюванні цілі (постановці задачі) здійснюється: збирання даних про стан об’єкта управління та зовнішнього середовища; прогнозування можливих змін (цільової функції поточної ситуації процесу управління) та вироблення (на основі обраних критеріїв) альтернативних стратегій керуючих впливів на об’єкт управління у формі відповідної послідовності операцій. Операція – впорядкована та взаємопов’язана сукупність дій, спрямованих на досягнення цілі (вирішення задачі). Вибір за одним чи кількома критеріями однієї з можливих альтернативних стратегій уособлює етап вибору рішення. Етап реалізації рішення полягає у виконанні операцій за планом обраної стратегії (керуючих впливів) досягнення цілі (вирішення задачі). Реалізація рішення (керуючих впливів на об’єкт управління) зазвичай здійснюється в умовах можливого прояву внутрішніх і зовнішніх дестабілізуючих факторів, що викликає певну невідповідність фактичного результату очікуваному. Визначення такої невідповідності, аналіз причин та вироблення рекомендацій щодо її усунення (зменшення) на наступному циклі управління уособлює етап оцінювання досягнення результату (вирішення задачі).

Під поняттям “орган управління” будемо розглядати функціональний компонент об’єкта критичної інфраструктури, який здійснює формулювання цілі (постановку задачі), підготовку, вибір, реалізацію та оцінку результату рішення циклу управління технологічним процесом (об’єкт управління) основної послуги, яка надається оператором критичної інфраструктури у певному секторі/підсекторі (рис. 1). Дестабілізуючі фактори охоплюють сукупність явищ, які можуть мати негативний прояв для досягнення цілі (вирішення задачі) на певному часовому інтервалі функціонування об’єкта критичної інфраструктури. Прояв того чи іншого дестабілізуючого фактора на певному часовому інтервалі функціонування об’єкта критичної інфраструктури є випадковою подією реального світу. Випадкова подія (реального світу) – подія, яка при фіксованих умовах випробування (експерименту) може як відбутися, так і не відбутися зі стабілізацією частоти такого результату у ряді випробувань. Можливість настання випадкової події характеризується числовим значенням її ймовірності.

Рис. 1. Об’єкт критичної інфраструктури як предмет системного аналізу

Ймовірність випадкової події залежить від комплексу умов, в яких здійснюється випробування (експеримент). Пояснення невідповідності фактичного результату процесу управління очікуваному проявом випадковості дестабілізуючих факторів або їх скритої закономірності є вельми складною задачею. Ефективним засобом рішення складних, недостатньо чітко сформульованих проблем є системний аналіз. Предмет системного аналізу ґрунтується на загальносистемних характеристиках і взаємодії системи із зовнішнім середовищем. Основною концепцією системного аналізу є системний підхід, де система – цілісний комплекс взаємозв’язаних компонентів (орган управління; об’єкт критичної інформаційної інфраструктури; об’єкт управління, зовнішнє середовище), які взаємодіють:

шляхом передачі інформації керуючого впливу від органу до об’єкта управління через тракт каналу прямого зв’язку (рис. 1, *а, б*) та інформації про стан об’єкта до органу управління через тракт каналу зворотного зв’язку (рис. 1, *в, г*);

шляхом обміну інформацією про параметри обміну речовиною (енергією) об’єкта управління із зовнішнім середовищем у контексті реалізації технологічного процесу об’єкта критичної інфраструктури.

Сукупність зв’язаних один з одним об’єктів (елементів) системи, здатних приймати, зберігати, перероблювати та передавати інформацію, уособлює кібернетичний аспект системного підходу до дослідження складних систем. Передавання/приймання інформації передбачає наявність у компонентів складної системи передавача/приймача та каналу зв’язку між ними, здатного відображати стан передавача та стан приймача, для зберігання інформації – наявність фізичного середовища, яке здатне фіксувати, зберігати і відтворювати свій стан. Перероблення інформації полягає у виконанні певного алгоритму, вхідні дані якого ототожнюються зі станом фізичного середовища для запам’ятовування.

У цьому контексті об’єкт критичної інформаційної інфраструктури уособлює сукупність систем електронних комунікацій, які забезпечують тракти утворення каналів прямого та зворотного зв’язку між пристроєм зв’язку з об’єктом управління та обчислювальною машиною органу управління через комунікаційну систему (об’єкта критичної інформаційної інфраструктури) і/або мережу Інтернет (рис. 2). Під поняттям “тракт каналу прямого (зворотного) зв’язку об’єкта критичної інфраструктури” будемо розглядати послідовне з’єднання сукупності технічних засобів комунікаційної системи і/або мережі Інтернет для забезпечення електронних комунікацій між пристроєм зв’язку з об’єктом управління та обчислювальною машиною органу управління.

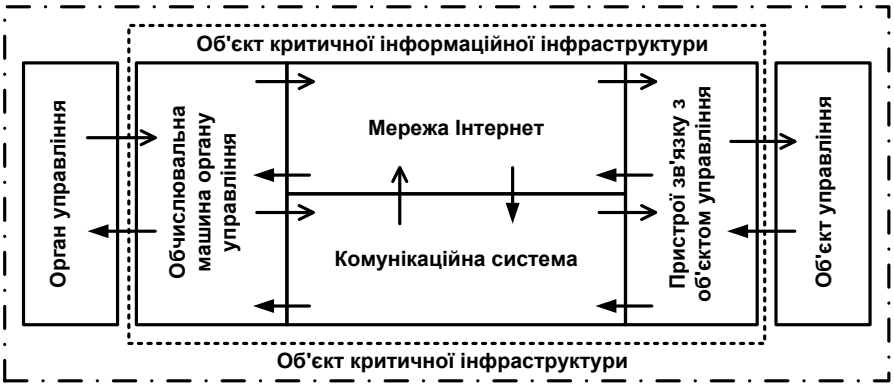


Рис. 2. Декомпозиція об’єкта критичної інформаційної інфраструктури

Компонент “комунікаційна система” уособлює складну систему передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв’язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв’язку, комп’ютери, інша комп’ютерна техніка, інформаційно-комунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних. Електронна комунікація (телекомунікація, електрозв’язок) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій. Мережа Інтернет (Інтернет) – глобальна електронна комунікаційна мережа, що призначена для передачі даних і складається з фізично та логічно взаємоз’єднаних окремих електронних комунікаційних мереж, взаємодія яких

базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стандартами [15; 16].

Усі методи управління зводяться до вироблення органом управління інформації керуючого впливу на підставі інформації від пристрою зв’язку з об’єктом управління. Пристрій зв’язку з об’єктом управління здійснює перетворення та передачу через канал зворотного зв’язку інформації про сукупність значень фізичних величин опису стану об’єкта управління, а також перетворення інформації керуючого впливу з каналу прямого зв’язку в операції надання необхідних значень регульованим фізичним величинам об’єкта управління. Обчислювальна машина органу управління здійснює одержання інформації від пристрою зв’язку з об’єктом управління, її перетворення у форму, придатну для вибору, забезпечення вибору керуючого впливу (органом управління) з множини можливих варіантів (програмного, оптимального управління чи авторегулювання) та відправлення інформації керуючого впливу через канал прямого зв’язку.

За змістовною природою об’єкта управління досягнення цілі функціонування об’єкта критичної інфраструктури може здійснюватися методами програмного, оптимального управління та авторегулювання. Програмне управління полягає у реалізації певної траєкторії (з множини сприятливих) послідовної зміни станів об’єкта управління, спрямованої на досягнення цілі (очікуваного результату постановки задачі) або якомога близького наближення до неї. Оптимальне управління спрямоване на забезпечення максимального чи мінімального значення деякої цільової функції, авторегулювання – на забезпечення заданого значення такої функції.

Поняття “цільова функція” уособлює функціональне відображення на кількісну величину ступеня наближення до цілі управління (постановки задачі) внаслідок керуючого впливу. Визначення ступеня наближення до цілі управління (постановки задачі) внаслідок керуючого впливу здійснюється шляхом оцінки корисності результату вирішення задачі. Залежність ступенів наближення вирішення задачі до цілі (постановки задачі) для всієї множини одержаних результатів називається функцією корисності. Математичне очікування множини дискретних або неперервних значень функції корисності є кількісною мірою ефективності, тобто показником ефективності (вирішення задачі).

Методичним базисом оцінки корисності результату вирішення задач є дослідження операцій, експертне оцінювання, імітаційне моделювання. За умови постановки задачі управління у контексті понятійного апарату розділів дослідження операцій кількісна велична цільової функції має найкраще обґрунтування, зокрема в частині, що стосується: розподілу ресурсів; масового обслуговування; пошуку; конкурентних ігор; складання розкладів; визначення маршрутів; постачання ресурсів; заміни обладнання і т. д. Експертне оцінювання полягає у залученні групи фахівців із необхідним рівнем знань та досвіду, імітаційне моделювання – у використанні результатів машинного експерименту.

Реалізація вибору керуючого впливу у формі алгоритму програмного компонента обчислювальної машини органу управління уособлює об’єкт критичної інфраструктури як автоматичну систему управління. Вибір керуючого впливу за участю людини у ролі органу управління є ключовою ознакою розгляду об’єкта критичної інфраструктури як автоматизованої системи управління. Різновид автоматичних та автоматизованих систем управління організаційними і/або технологічними процесами об’єктів критичної інфраструктури віднесений до класу систем управління технологічними процесами. Також слід зазначити, що переважна кількість таких систем належить до автоматизованого типу.

Участь людини-оператора в процесі управління технологічним процесом (об’єкта критичної інфраструктури) обумовлена необхідністю усунення невизначеності вибору рішення. Причинами невизначеності (неповноти, недостатності, обмеженості, неточності) інформації для вибору рішення можуть бути: неможливість точного передбачення наслідків; неможливість повторення або експериментальної перевірки; немає можливості контролю всіх

факторів; наявність множини альтернативних рішень. Вибір рішення є прерогативою людини і принципово не може мати формального подання. Особа, яка приймає рішення, керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб’єктивними уявленнями, судженнями, емоціями.

Людина-оператор (органу управління) – людина, яка бере участь в управлінні об’єктами і системами як складовий елемент ергатичної системи. Може виступати в ролі приймача, ретранслятора і перетворювача інформації, приймати рішення, вироблювати команди, здійснювати контроль роботи системи та бути виконавцем команд. Відрізняється багатоканальністю сприйняття, раціональним використанням інформації, здатністю до навчання, малою пропускною здатністю, обмеженою швидкістю та втомлюваністю.

Розглянемо кілька прикладів технологічних процесів критичної інфраструктури, управління якими передбачає застосування автоматизованого підходу при побудові відповідних систем:

управління системами передачі, енергопостачання, розподілом електричної енергії, експлуатації гідротехнічних споруд;

видобуток, передача (транзит), очищення, переробка, зберігання та постачання нафти, нафтопродуктів, газу;

експлуатація нафтопроводів та газотранспортної системи;

управління повітряним рухом, авіаперевезення (робота авіаційного транспорту);

перевезення пасажирів метрополітеном;

пасажирські, вантажні залізничні перевезення;

експлуатація та технічне обслуговування залізниці, забезпечення роботи вокзалів та вузлових станцій;

постачання теплової енергії, постачання гарячої води, централізоване питне водопостачання, централізоване водовідведення, управління побутовими відходами;

виробництво промислового газу, добрив або азотистих сполук, пестицидів, агрохімічних продуктів, вибухових, основних органічних, неорганічних речовин і т. д.

Умови (виконання функцій) своєчасного вироблення органом управління (об’єкта критичної інфраструктури) правильних керуючих впливів для об’єкта управління (рис. 3):

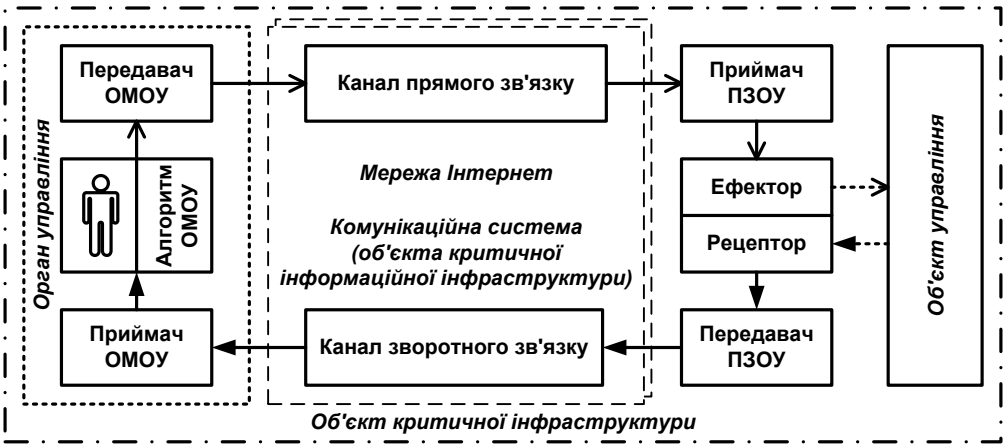


Рис. 3. Компоненти забезпечення циклу управління технологічним процесом

передача за визначений час інформації про стан об’єкта управління від пристрою зв’язку з об’єктом управління (ПЗОУ) через канал зворотного зв’язку якомога повної інформації про стан об’єкта управління;

своєчасний і правильний вибір людиною-оператором (автоматизована система управління) варіанту керуючого впливу з множини можливих варіантів сформованих

управляючим програмним алгоритмом обчислювальної машини органу управління (ОМОУ), який правильно функціонує або автоматичний вибір рішення самим таким алгоритмом без участі людини-оператора (автоматична система управління);

передача за визначений час інформації керуючого впливу від ОМОУ через канал прямого зв’язку;

правильне функціонування (справність, працездатність) програмно-апаратного компонента ефектора ПЗОУ (перетворення інформації з каналу прямого зв’язку в значення регульованих фізичних величин об’єкта управління за визначений час);

правильне функціонування (справність, працездатність) програмно-апаратного компонента рецептора ПЗОУ (перетворення значень фізичних величин опису стану об’єкта управління в інформацію для каналу зворотного зв’язку за визначений час).

Впорядкована сукупність операцій передавання (обробки, перетворення) інформації у контурі послідовного охоплення компонентів ОМОУ, каналу прямого зв’язку, ПЗОУ та каналу зворотного зв’язку утворюють цикл управління технологічним процесом (ЦУТП), що багатократно повторюється в процесі управління (об’єктом критичної інфраструктури). Тривалість ЦУТП дорівнює сумарній середній тривалості операцій передавання (обробки, перетворення) інформації в ОМОУ, ПЗОУ та каналів прямого (зворотного) зв’язку.

Ефективність ЦУТП є кількісним показником (мірою) математичного очікування множини значень фактичної тривалості циклів управління технологічним процесом при штатному режимі функціонування апаратних, програмних (програмно-апаратних) компонентів об’єкта критичної інформаційної інфраструктури, зокрема, ОМОУ, каналів прямого (зворотного) зв’язку та ПЗОУ. Математично очікувана тривалість ЦУТП не повинна перевищувати деякої максимально допустимої величини для об’єкта критичної інфраструктури як системи ієрархічного управління в реальному масштабі часу на етапі проєктування процесів оброблення інформації для забезпечення необхідного темпу змін станів технологічного процесу (об’єкта управління). Методичним базисом обґрунтування часових ЦУТП є теорія систем масового обслуговування (модель мережі масового обслуговування), при застосуванні якої ОМОУ, ПЗОУ та канали прямого (зворотного) зв’язку розглядаються як прилади обслуговування.

Раніше вже було зазначено, що режим функціонування об’єкта критичної інфраструктури визначається її оператором (юридична особа, що здійснює управління об’єктом критичної інфраструктури, відповідає за його поточне функціонування, захист та реагування на кризові ситуації) як процес забезпечення реалізації певних визначених для такого об’єкта функцій (послуг). Під поняттям “функція” (об’єкта) – властивість (об’єкта) відповідно до вимог нормативної та (чи) конструкторської (проєктної) документації (на етапі розробки вимог, проєктування, виробництва, використання і ремонту об’єкта), де об’єкт – самостійна одиниця з погляду надійності (технічні система, програмний засіб, людино-машинна система, споруда, машина, підсистема, апаратура, функційна одиниця, пристрій, елемент чи будь-яка їх частина). Надійність – властивість об’єкта зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання та транспортування. Методичним базисом застосування методів розрахунку надійності технічних систем, виробів, способів оптимізації і підвищення ефективності їх експлуатації є теорія надійності [17–19].

Параметри штатного режиму функціонування апаратних, програмних (програмно-апаратних) компонентів забезпечення циклу управління технологічним процесом (ОМОУ, канал прямого зв’язку, ПЗОУ, канал зворотного зв’язку) в заданих умовах визначаються як складова частина відповідності системи управління технологічним процесом (об’єкта критичної інфраструктури) проєктному цільовому призначенню. Подія, яка полягає у втраті об’єктом здатності виконувати потрібну функцію, тобто порушення працездатного стану

об’єкта, називається відмовою. Причини відмов (обставини під час проєктування, виробництва чи використання об’єкта, які призвели до відмови):

недосконаліть чи порушення встановлених правил і/або норм проєктування та конструювання (конструкційна відмова);

невідповідність виготовлення проєкту нормам виробництва (виробнича відмова);

поступові зміни значень одного чи декількох параметрів (поступова відмова);

внаслідок відмови чи несправності іншого об’єкта (залежна відмова);

однозначно пов’язана з необхідністю модифікації проєкту, виробництва, правил експлуатації, документації чи інших чинників, що враховуються (систематична відмова);

діяння під час використання об’єкта навантажень, що перевищують його встановлену спроможність (відмова через перевантаження);

неправильне чи необережне поводження (відмова через неправильне поводження);

неміцність самого об’єкта, коли діяння навантаження на об’єкт не перевищують встановлену спроможність об’єкта (відмова через неміцність);

процеси деградації в об’єкті при дотриманні всіх встановлених правил і/або норм його проєктування, виготовлення та експлуатації (деградовна відмова);

непередбачуване стихійне лихо (відмова внаслідок стихійного лиха).

Виникнення відмови є випадковою подією, що викликана проявом зазвичай складної комбінації типових класів обставин (викладені у поєднанні з причинами відмов) та випадкових об’єктивних і суб’єктивних (обумовлені ймовірністю помилкових рішень осіб, які приймають рішення при створенні та експлуатації об’єктів) факторів експлуатаційного, технологічного та організаційного характеру. Традиційними підходами (теорії надійності) до зменшення негативного впливу об’єктивних і суб’єктивних факторів прояву відмов компоненті технічних систем є резервування, оптимальне управління запасними елементами, термінами експлуатації, технічна діагностика, обслуговування тощо за результатами апріорного аналізу надійності. Апріорний аналіз надійності здійснюється шляхом вибору одного з можливих варіантів проєктування (створення) об’єкта (технічної системи) за умови наявності повної інформації про ймовірність відмов її компонентів, апостеріорний аналіз – на основі обробки статистичних даних випробування (експлуатації) за умови незалежності випадкових величин, що спостерігаються. На практиці спостерігається наявність невизначеності (неповнота, невірогідність) вихідної інформації про закони розподілу випадкових величин, що характеризують надійність окремих елементів, складових частин (компонентів) та об’єкта в цілому. Найбільш актуальні напрямки зменшення (усунення) “апріорної невизначеності” в задачах надійності досліджені авторським колективом під керівництвом Креденцера Б. П. шляхом комплексного застосування наукових результатів Стойкової Л. С., Каштанова В. О. В якості принципових положень наукового дослідження “апріорної невизначеності” вихідних даних апріорного аналізу надійності було зафіксовано:

надійність задається при проєктуванні (апріорний аналіз), уточняється на основі даних випробування (апостеріорний аналіз), враховується при виробництві та реалізується в процесі експлуатації об’єкта (технічної системи);

відсутність (недостатність) знання про складні залежності між складовими елементами (компонентами) об’єкта, об’єму достовірної вибірки експериментальних даних експлуатації аналога створюваного об’єкта (технічної системи) внаслідок його унікальності;

невідповідність (слабка адекватність) між розрахунковими результатами апріорного аналізу надійності одержаних на основі довідкових даних та фактичними даними досвіду експлуатації об’єкта (технічної системи) в реальних умовах.

Раніше вже було зазначено, що характерною експлуатаційною рисою переважної кількості об’єктів критичної інфраструктури є використання публічного (загальнодоступного, відкритого) кіберпростору для забезпечення обміну інформацією управління через тракти утворення каналів прямого (зворотного) зв’язку. Під поняттям “кіберпростір” уособлюється

середовище (віртуальний простір), утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем і забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Наявність з’єднання компонентів забезпечення ЦУТП об’єкта критичної інформаційної інфраструктури з кіберпростором обумовлює ймовірність спрямованих (навмисних) дій несанкціонованого втручання у формі кібератаки [20–22].

Розгляд інших подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) експлуатації об’єкта критичної інфраструктури за умови апріорної невизначеності уособлює всю широту поняття “кіберінцидент”. Порушення безперервності, стійкості, штатного режиму функціонування компонентів забезпечення ЦУТП виникненням відмов належить до класу кризових ситуацій (об’єкта критичної інфраструктури). При виникненні відмови (компонентів забезпечення ЦУТП) оператором критичної інфраструктури вводиться режим реагування на виникнення кризової ситуації із застосуванням заходів реагування.

Фахівець з реагування на інциденти кібербезпеки здійснює неперервний контроль за штатним режимом функціонування об’єкта критичної інформаційної інфраструктури та активно втручається в процес при виникненні кризових ситуацій. Вирішення наукових задач організації ефективної діяльності фахівців із реагування на кіберінциденти/кібератаки об’єктів критичної інформаційної інфраструктури здійснено на основі науково-методичного апарату створення систем інформаційної підтримки прийняття рішень Герасимова Б. М. та узагальнення результатів дисертаційних досліджень представників цієї наукової школи.

Висновки. Штатний режим функціонування об’єкта критичної інфраструктури в реальному масштабі часу може бути відображений ефективністю на основі оцінки тривалості циклу управління технологічним процесом, компоненти забезпечення якого розглядаються пристроями мережі масового обслуговування. Погіршення ефективності через відмову таких компонентів може бути компенсовано на етапі проєктування шляхом апріорного аналізу надійності із застосуванням наукових результатів усунення (зменшення) апріорної невизначеності. Цей апробований підхід є недієвим для визначення ймовірностей кібератак на етапі експлуатації конкретного об’єкта через неможливість одержання достовірної статистики і обумовлює необхідність реагування на кіберінциденти/кібератаки (на виникнення кризової ситуації) на основі апарату інформаційної підтримки прийняття рішень.

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. NIST Special Publication 800-61. Computer Security Incident Handling Guide.

3. Про затвердження Положення про організаційно-технічну модель кіберзахисту: постанова Каб. Міністрів України від 29.12.2021 № 1426 // Офіційний вісник України. 2022. № 4. С. 247. Ст. 219.

4. Computer Security Incident Response Team Services Framework, Service Role and Competencies. URL: https://www.first.org/standards/frameworks/.

5. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX // Офіційний вісник України. 2021. № 98. С. 23. Ст. 6341.

6. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури: постанова Каб. Міністрів України від 19.06.2019 № 518 // Офіційний вісник України. 2019. № 50. С. 53. Ст. 1697.

7. Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: постанова Каб. Міністрів України від 04.04.2023 № 299 // Офіційний вісник України. 2023. № 39. С. 54. Ст. 2061.

8. Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: наказ Адміністрації Державної служби спеціального

зв’язку та захисту інформації України від 03.07.2023 № 570 // URL: https://zakon.rada.gov.ua/rada/show/v0570519-23#Text.

9. Професійний стандарт “Фахівець з реагування на інциденти кібербезпеки”, затв. наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 23.01.2024 № 38 // URL: https://register.nqa.gov.ua/uploads/0/571-fahivec_z_reaguvanna_na_incidenti_kiberbezpeki_v_2.pdf.

10. Хусаінов П. В. Система інформаційної підтримки адміністратора безпеки: структура, задачі, оцінка ефективності // Збірник наукових праць ВІТІ НТУУ “КПІ”. Вип. 3. Київ: ВІТІ НТУУ “КПІ”, 2007. С. 146–155.

11. 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.

12. Герасимов Б. М., Камишин В. В. Організаційна ергономіка: методи і алгоритми дослідження та проектування. К.: Інфосистем, 2009. 212 с.

13. Ten Strategies of a World-Class Cybersecurity Operations Center. Carson Zimmerman. ISBN: 978-0-692-24310-7. URL: https://a.co/d/gyPR2WW.

14. The Modern Security Operations Center: The People, Process, and Technology for Operating SOC Services Joseph Muniz, Aamir Lakhani, Omar Santos, Moses Frost ISBN-10:0135619858, ISBN-13: 978-0135619858 Addison-Wesley Professional.

15. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. 1994. № 31. Ст. 286.

16. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX // Офіційний вісник України. 2021. № 6. С. 10. Ст. 306.

17. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. [Чинний від 1996-01-01]. URL: https://dbn.co.ua/load/normativy/dstu/dstu_2860_94_nadijnist_tekhniki_termini_ta_viznachennja/5-1-0-1209.

18. Основи теорії надійності та експлуатації радіоелектронних систем: навч. посіб. / В. І. Василишин, С. В. Женжера, О. В. Чечуй, А. П. Глушко. Х.: ХНУПС, 2018. 208 с.

19. Креденцер Б. П., Вишнівський В. В., Жердєв М. К., Могилевич Д. І., Стойкова Л. С. Оцінка надійності резервованих систем при обмеженій вихідній інформації / Під наук. редак. д-ра техн. наук, проф. Б. П. Креденцера. К.: Фенікс, 2013. 336 с.

20. Adversarial Tactics, Techniques & Common Knowledge. URL: https://attack.mitre.org.

21. Common Attack Pattern Enumerations and Classifications. URL: https://capec.mitre.org.

22. Common Weakness Enumeration. URL: https://cwe.mitre.org.

DOI: 10.58254/viti.8.2025.22.280

УДК 004.056.5

д-р техн. наук, професор Чевардін В. Є. ORCID 0000-0002-1070-4568 (ВІТІ ім. Героїв Крут)
Прийма О. О. ORCID 0009-0008-6991-1773 (ВІТІ ім. Героїв Крут)

РЕЗУЛЬТАТИ АНАЛІЗУ СТІЙКОСТІ ТА ОБЧИСЛЮВАЛЬНОЇ ШВИДКОДІЇ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ВЛАСТИВОСТЕЙ

У статті представлено результати комплексного дослідження криптографічних властивостей та обчислювальної ефективності детермінованих генераторів псевдовипадкових послідовностей (DRBG), стандартизованих NIST SP 800-90A Rev.1. Проведено порівняльний аналіз алгоритмів CTR_DRBG, HASH_DRBG, HMAC_DRBG та Dual_EC_DRBG з використанням різних криптографічних примітивів: блокового шифру AES-256, хеш-функцій SHA-256/SHA-512 та еліптичних кривих P-256/P-384.

Досліджено залежність продуктивності генераторів від типу базового криптографічного примітива шляхом вимірювання кількісних показників cycles per byte (cpb) на 64-бітній архітектурі. Верифіковано статистичні властивості згенерованих послідовностей за допомогою тестового набору NIST SP 800-22 Rev.1a. Встановлено, що CTR_DRBG на основі AES-256 та HMAC_DRBG із SHA-256 забезпечують оптимальне співвідношення між криптографічною стійкістю та швидкодією, демонструючи найвищу продуктивність серед досліджених реалізацій.

Показано, що Dual_EC_DRBG, побудований на операціях скалярного множення точок еліптичних кривих, характеризується найвищою обчислювальною складністю внаслідок арифметики у групі точок еліптичної кривої, проте демонструє граничну статистичну якість вихідних послідовностей. Обґрунтовано перспективність застосування еліптичних криптопримітивів у контексті побудови постквантово-стійких генераторів.

Результати дослідження формують методологічну основу для обґрунтованого вибору типу DRBG відповідно до вимог конкретного криптографічного застосування з урахуванням обмежень на обчислювальні ресурси та рівень безпеки. Отримані дані можуть бути використані для оптимізації протоколів генерації ключового матеріалу, розробки систем електронного підпису та автентифікації, а також проєктування криптографічних механізмів, сумісних із міжнародними стандартами безпеки.

Ключові слова: *детерміновані генератори псевдовипадкових бітів, DRBG, криптографічна стійкість, обчислювальна складність, еліптичні криві, блокові шифри, хеш-функції, статистичне тестування, постквантова криптографія.*

V. Chevardin, O. Pryma. Results of the Analysis of Cryptographic Resilience and Computational Performance of Pseudorandom Generators

The paper presents the results of a comprehensive study of the cryptographic properties and computational efficiency of deterministic random bit generators (DRBG) standardized in NIST SP 800-90A Rev.1. A comparative analysis of the CTR_DRBG, HASH_DRBG, HMAC_DRBG, and Dual_EC_DRBG algorithms was conducted using various cryptographic primitives, including the AES-256 block cipher, SHA-256/SHA-512 hash functions, and elliptic curves P-256 and P-384.

The dependence of generator performance on the type of underlying cryptographic primitive was investigated by measuring the quantitative indicator cycles per byte (cpb) on a 64-bit architecture. The statistical properties of the generated sequences were verified using the NIST SP 800-22 Rev.1a test suite. It was established that CTR_DRBG based on AES-256 and HMAC_DRBG using SHA-256 provide an optimal balance between cryptographic strength and computational speed, demonstrating the highest performance among the studied implementations.

Dual_EC_DRBG, based on scalar point multiplication over elliptic curves, exhibits the highest computational complexity due to the arithmetic of elliptic-curve point groups but achieves the highest statistical quality of output sequences. The study substantiates the prospects of using elliptic-curve cryptographic primitives for the design of post-quantum-resistant random bit generators.

The results form a methodological basis for the reasoned selection of DRBG types according to specific cryptographic application requirements, considering computational constraints and security levels. The findings can be used to optimize key-generation protocols, design electronic signature and authentication systems, and develop cryptographic mechanisms compliant with international security standards.

Keywords: *deterministic random bit generators, DRBG, cryptographic strength, computational complexity, elliptic curves, block ciphers, hash functions, statistical testing, post-quantum cryptography.*

Постановка проблеми та актуальність дослідження

Поява квантових комп'ютерів викликала реальну потребу в підвищенні стійкості існуючих криптопримітивів, які використовуються в системах електронно-цифрового підпису, системах та комплексах автентифікації та розмежування доступу, генерації загальних секретних ключів для шифрування та автентифікації даних. Паралельно була розпочата компанія щодо розробки нових криптопримітивів, які використовують інші математичні апарати для побудови криптографічних операцій. Особливу увагу вчені завжди приділяли розробці стійких алгоритмів генерації криптографічних ключів, що обґрунтовано їх значенням для протоколів та алгоритмів шифрування даних, інкапсуляції криптографічних ключів. За останнє десятиріччя було прийнято декілька національних стандартів NIST в якості базових та загально визначених алгоритмів генерації псевдовипадкових послідовностей для створення криптографічних ключів, а саме сімейства алгоритмів, які в якості криптопримітивів використовують блокові симетричні схеми шифрування, алгоритми гешування даних, перетворення точок еліптичної кривої над простими полями та їх розширення. Поява нових алгоритмів завжди викликає нові ризики щодо появи невідомих раніше уразливостей, які можуть бути виявлені з часом. Це, в свою чергу, уповільнює впровадження нових алгоритмів в існуючі інформаційні системи для криптографічного захисту інформації, тому власники інформаційних систем іноді схиляються до використання існуючих криптографічних систем з деякими удосконаленнями за рахунок збільшення параметрів криптографічної стійкості, за що платою є незначні зниження швидкодії алгоритмів, які компенсуються підвищенням потужності обчислювальних засобів.

Таким чином, підвищення швидкодії криптографічних генераторів псевдовипадкових послідовностей (ГПВП), оцінка їх псевдовипадкових властивостей та криптографічної стійкості є актуальним науковим напрямом важливим для забезпечення стійкості існуючих криптосистем до нових загроз викликаних появою та збільшенням потужності квантових комп'ютерів. У цієї роботі наведено порівняння основних класів генераторів із короткими характеристиками та оцінками стійкості та обчислювальної швидкодії.

Аналіз останніх публікацій та наукових результатів

Сьогодні існує багато розроблених як генераторів випадкових послідовностей (random bit generator – RBG) так і генераторів псевдовипадкових послідовностей (deterministic random bit generator – DRBG), які створені для використання в різноманітних протоколах, але як правило, мають схожий математичний апарат для побудови криптографічних систем шифрування, гешування та інших криптопримітивів. Останніми результатами, досягнутими в цьому напрямку є використання стандартизованих криптографічних алгоритмів для побудови криптографічно стійких генераторів DRBG. Розглянемо існуючі класи ГПВП, рекомендовані різними джерелами та стандартами, які були досліджені за останнє десятиріччя.

У роботі [1] розроблено нові моделі безпеки для генераторів псевдовипадкових чисел із вхідною ентропією. Основним результатом є побудова seedless-генераторів, що не потребують початкового випадкового зерна (ентропійного значення seed), але залишаються стійкими до компрометації внутрішнього стану генератора та впливу на джерела ентропії. Криптографічна стійкість ГПВП досягається за рахунок використання криптографічних хеш-функцій SHA-2, SHA-3 та HMAC, що забезпечують за думкою автора як обчислювальну, так і теоретичну стійкість.

У роботі [2] формалізовано визначення сім'ї 12-раундових функцій Keccak, відомих як TurboSHAKE, для використання в постквантових криптографічних схемах. Показано, що скорочення кількості раундів не погіршує стійкість алгоритму, а забезпечує вищу продуктивність і сумісність із існуючими реалізаціями Keccak/XOF, що стало можливим завдяки оптимізації структури примітива, запозиченого з Kangaroo Twelve.

У роботі [3] запропоновано нову конструкцію детермінованого генератора псевдовипадкових бітів (XDRBG), що ґрунтується на використанні будь-якої функції з

розширюваним виходом (XOF). Основним результатом є доведення формальної стійкості в ідеальній моделі XOF із щільними межами стійкості та демонстрацією квантової стійкості. Безпечність досягнуто завдяки універсальній конструкції, що поєднує алгоритми SHAKE128, SHAKE256 і ASCON-XOF та забезпечує як високу швидкодію, так і стійкість до компрометації внутрішнього стану генератору ПВП.

У роботі [4] наведено результати аналізу стійкості генератора DRBG, що базується на перестановках, запропонованого Coretti та іншими авторами на конференції CRYPTO 2019. Зокрема, авторами було доведено, що конструкція генераторів цього класу, заснована на "губковій" (sponge) схемі. Цей алгоритм отримав назву Sponge-DRBG. У роботі показано, що ця конструкція є стійкою до криптографічних атак. Авторам вдалося покращити теоретичну межу безпеки DRBG, що базується на перестановках, із рівня $O(min\{2^{c/3}, 2^{\lambda/2}\})$ до $O(min\{2^{c/2}, 2^{\lambda/2}\})$, тобто до максимально можливої (так званої *birthday-bound*) границі стійкості. Завдяки аналізу губкової структури (sponge construction) запропоновано новий генератор POSDRBG з підвищеною швидкістю генерації (output rate = 1) без втрати безпеки. Підвищення досягнуто за рахунок оптимізації параметрів ємності (c) та мінімальної ентропії (λ).

У роботі [5] запропоновано новий тип генератора псевдовипадкових бітів, побудований на асиметричних числових системах (ANS), які традиційно використовуються у стисненні даних. Автори показали статистичну схожість вихідних послідовностей з істинно випадковими для великих параметрів R на основі NIST STS тестів. Також автори показали, що після застосування Keccak-перетворень і ротаційних операцій вихідні дані також успішно проходять тести NIST STS. На думку авторів, отримані результати засвідчили формальну криптографічну стійкість при великих R та евристичну стійкість при менших значеннях, включно із заявленою квантовою стійкістю конструкції.

Таким чином, аналіз останніх робіт підтверджує основні напрями вдосконалення існуючих схем генерації ПВП, а саме це оцінка та підвищення криптографічної стійкості генераторів DRBG за рахунок використання більш стійких криптоперетворень як до існуючих методів криптоаналізу, так і для методів квантового криптоаналізу. Також, дослідження сучасних і перспективних алгоритмів генерації ПВП, пов'язано з швидкими оцінками потенційних властивостей вихідних послідовностей генераторів ПВП із використанням методик оцінки статистичної безпеки NIST STS. Далі у статті представлено власні дослідження існуючих та перспективних схем генерації ПВП з оцінкою криптографічної та статистичної безпеки.

Дослідження та оцінка параметрів стійкості та статистичної властивостей

Лінійні ГПВП (LCG, MCG)

Прості у реалізації та швидкі в роботі, проте вони не забезпечують криптографічної стійкості, що робить їх непридатними для захисту інформації. Основне призначення таких генераторів – це симуляції, статистичне моделювання та інші задачі, де не потрібна криптографічна захищеність.

Прикладами лінійних генераторів є LCG, MCG, XORShift, Mersenne Twister, PCG та WELL512a, серед яких найкращі показники швидкодії демонструє PCG зі значенням 1.5-4 cpb. Водночас криптографічна стійкість PCG залишається досить низькою та оцінюється приблизно на рівні $2^{30} - 2^{40}$, що підтверджує непридатність цього класу генераторів для криптографічних застосувань.

ГПВП на основі регістрів зсуву (LFSR/NLFSR)

Генератори цього типу формуються на основі регістрів зсуву з лінійними (LFSR) або нелінійними (NLFSR) зворотними зв'язками між бітами регістра. Завдяки високій обчислювальній ефективності та можливості апаратної реалізації, вони знайшли широке застосування у потокових шифрах, що забезпечують захист даних у режимі реального часу.

До найпоширеніших представників цього класу належать LFSR, NLFSR, Combined LFSR, Geffe, Shrinking та Stop-and-Go генератори. Серед них базовий LFSR характеризується найвищою швидкодією – приблизно 1–3 cycles per byte (cpb). Криптографічна стійкість генераторів, побудованих на основі регістрів зсуву, зазвичай оцінюється в межах $2^{50} - 2^{70}$, що робить їх прийнятними для окремих прикладних завдань, хоча вони поступаються сучасним криптографічним стандартам за рівнем безпеки.

Комбіновані ГПВП

Створюються шляхом поєднання кількох різних алгоритмів або методів генерації, що дозволяє значно підвищити як криптографічну стійкість, так і період послідовності порівняно з простими генераторами. Такий підхід компенсує недоліки окремих алгоритмів і забезпечує кращі статистичні властивості вихідної послідовності.

До найвідоміших представників комбінованих генераторів належать Xoshiro256**, Xoroshiro, WELL1024 та Hybrid Taus, серед яких найкращі показники швидкодії демонструє Xoshiro256** зі значенням 1–3 cpb. Криптографічна стійкість комбінованих генераторів оцінюється приблизно на рівні $2^{60} - 2^{80}$, що робить їх придатними для широкого спектра застосувань, включаючи наукові обчислення та деякі криптографічні задачі середнього рівня безпеки.

Криптографічні ГПВП (DRBG)

DRBG є фундаментальним компонентом сучасних систем криптографічного захисту інформації. Призначення DRBG полягає у формуванні бітових послідовностей, статистичні властивості яких наближені до істинно випадкових, але отримані детермінованим способом із використанням криптографічних перетворень. Забезпечення якісної псевдовипадковості є ключовою передумовою надійності криптографічних протоколів, систем шифрування, автентифікації, цифрових підписів та керування сесіями [6].

На відміну від класичних генераторів псевдовипадкових чисел, криптографічні DRBG мають підвищені вимоги до стійкості до передбачуваності, стійкості до відтворення попередніх станів генератору та стійкості до криптоаналітичних атак на алгоритм генерації внутрішнього стану генератору. Ці три показника визначають властивість таких алгоритмів, що навіть за умови розкриття частини внутрішнього стану або попередніх вихідних даних зловмисник не може обчислити наступні елементи послідовності [7].

Сучасні реалізації криптографічних DRBG ґрунтуються на використанні криптографічних примітивів із доведеною односторонністю, зокрема блочних шифрів, хеш-функцій, потокових шифрів та інших криптопримітивів. Це дозволяє пов'язати рівень криптографічної стійкості генератора із криптографічною стійкістю базового алгоритму. Найпоширенішими прикладами таких реалізацій є CTR-DRBG, HMAC-DRBG, SHAKE256 та Fortuna, які застосовують різні механізми оновлення початкового стану (reseed) та генерації внутрішнього стану DRBG.

Одним із найбільш ефективних та стандартизованих DRBG є CTR-DRBG (Counter-mode Deterministic Random Bit Generator), описаний у документі NIST SP 800-90A Rev. 1 [8]. Принцип його роботи базується на алгоритмі блочного шифрування у режимі лічильника (Counter Mode), що забезпечує високий рівень розсіювання, відсутність внутрішньої кореляції між блоками, криптографічну стійкість і непередбачуваність вихідних даних.

Прикладами генераторів ПВП на основі блокових, потокових схем шифрування та шгеш-функцій є: ChaCha20, AES-CTR-DRBG, HMAC-DRBG, SHAKE256, Fortuna, з яких за показниками швидкодії кращим є ChaCha20, а саме значення швидкодії для нього складає 3–12 cpb, при цьому значення його криптографічної стійкості складає $\geq 2^{128}$.

Квантові генератори (QRNG)

QRNG формують випадковість із фізичних квантових процесів, таких як фотонна емісія, квантові флуктуації вакууму або розпад радіоактивних ізотопів. Вважається, що сьогодні це найвищий рівень непередбачуваності, але використання цих генераторів для потокового

шифрування або для генерації спільних криптографічних ключів є складною задачею, що обмежує їх сферу застосування в криптографічних алгоритмах.

Прикладами генераторів ПВП на основі фізичних квантових процесів є генератори: ID Quantique QRNG, Toshiba QRNG, Quantis, Quside QRNG, з яких за показниками швидкодії кращим є ID Quantique QRNG, а саме значення швидкодії для нього складає 10–100 cpb, при цьому, значення його криптографічної стійкості неможливо оцінити класично. Завдяки квантовій природі випадковості, QRNG забезпечують теоретично абсолютну непередбачуваність, проте їхнє практичне впровадження стримується високою вартістю обладнання, складністю інтеграції та обмеженою швидкістю генерації порівняно з програмними рішеннями.

Принципи побудови DRBG

Формування криптографічно стійких псевдовипадкових послідовностей базується на моделі детермінованої генерації, у якій випадковість вихідних даних забезпечується не фізичними джерелами ентропії (наприклад шуми діодів, зміни повітряної турбулентності та інші джерела ентропії), а криптографічною складністю відновлення внутрішнього стану генератора [9].

Згідно з визначенням [8], криптографічно стійкий DRBG можна подати у вигляді відображення $G: \{0,1\}^s \to \{0,1\}^n$, яке, отримавши початковий стан генератора (seed), сформований на основі ентропійних вхідних даних (entropy input), породжує послідовність довжиною $n \gg s$ біт, статистичні властивості якої не відрізняються від властивостей істинно випадкової послідовності.

Архітектура DRBG включає три основні фази [8]:

● Ініціалізація генератора (Instantiate) – це процес встановлення початкового внутрішнього стану генератора псевдовипадкових чисел. Результатом ініціалізації є встановлення параметрів внутрішнього стану, який визначається впорядкованою парою $S = (K, V)$, де K – симетричний ключ блочного шифру, а V – внутрішній лічильник, що керує послідовністю блоків.

● Оновлення стану генератора (Reseed) – це процес періодичного відновлення внутрішнього стану генератора з метою підвищення ентропії та запобігання втраті криптографічної стійкості. Під час оновлення до поточного стану вводяться нові ентропійні дані, а також, за потреби, додаткові параметри. У результаті формується нова пара (K, V), що замінює попередні значення ключа та лічильника. Процедура гарантує неможливість відтворення попередніх вихідних даних навіть за умови часткової компрометації стану.

● Генерація вихідних даних (Generate) – це процес формування вихідних бітів шляхом криптографічного перетворення поточного стану генератора. Для CTR_DRBG це відбувається через блочне шифрування лічильника V під ключем Key у режимі лічильника (CTR) $Output_i = E_K(V + i)$. Після завершення генерації виконується оновлення параметрів K та V, що запобігає повторному використанню стану та підтримує криптографічну стійкість генератора.

Криптографічно стійкий DRBG повинен задовольняти властивостям безпеки [8]:

● Стійкість до передбачення (prediction resistance) – компрометація поточного внутрішнього стану не повинна давати змоги передбачити майбутні вихідні біти.

● Стійкість до відновлення попередніх виходів (backtracking resistance) – компрометація поточного стану не дозволяє відновити дані, згенеровані раніше.

● Стійкість до продовження компрометації стану (state compromise extension resistance) – властивість, за якої компрометація внутрішнього стану генератора не впливає на подальші вихідні дані: після виконання оновлення стану генератора нові вихідні послідовності залишаються криптографічно незалежними від попередніх.

Оцінка показників обчислювальної швидкодії та криптографічної стійкості криптопримітивів реалізованих в структурах DRBG

Реалізації CTR-DRBG відрізняються вибором симетричного блочного шифру, який визначає як рівень стійкості, так і експлуатаційні характеристики (швидкодію, можливість паралельної обробки тощо). У цьому розділі систематизовано властивості реалізацій на основі DES, 3DES та AES у контексті вимог NIST SP 800-90A Rev.1 [8] і супутніх рекомендацій [14; 15].

Введемо показники для оцінки обчислювальної швидкодії та криптографічної стійкості DRBG:

- Cycles per byte (cpb) – це одиниця виміру складності, яка показує, скільки тактів процесор в середньому витрачає на обробку одного байта даних. Для більш кращого сприйняття переваги в швидкодії алгоритму та порівняльного аналізу продуктивності алгоритмів будемо використовувати обернену величину (1/cpb).
- Cycles per block – це одиниця виміру складності, яка показує, скільки тактів процесор в середньому витрачає на обробку одного блоку даних.
- Криптографічна стійкість (security strength) – ймовірність визначення закону формування ПВП (тобто прогнозування будь-яких бітів ПВП без знання секретного параметра seed) за рахунок визначення секретних параметрів генератора або зламу шифру. Криптографічну стійкість прийнято поєднувати також з обсягом обчислювальних витрат, які необхідно витратити для зламу криптографічного перетворення, на основі якого побудований генератор ПВП. Згідно з [8], необхідний об'єм роботи для відтворення закону формування ПВП з довжиною вхідного seed 112, 128, 192, 256 біт складе $2^{112}, 2^{192}, 2^{256}$ операцій відповідно. Є доведена та обчислювальна криптостійкість.

Під час порівняння криптографічних алгоритмів часто використовують їх здатність до розпаралелювання, тобто можливість одночасного опрацювання декількох блоків даних алгоритму як окремих потоків даних, що дає можливість отримувати перевагу над іншими алгоритмами в швидкодії.

У таблиці 1 наведено порівняння продуктивності CTR-DRBG із різними блочними шифрами. Показник cycles per byte (cpb) використовується як умовна міра швидкодії на архітектурі x86-64.

Таблиця 1

Порівняння CTR-DRBG на різних алгоритмах шифрування

Алгоритм	Блок (біт)	Раунди	Cycles / byte (cpb)	Cycles / block	Оцінка швидкодії (1/cpb)	Криптостійкість (2^exp)
AES -128	128	10	12–15	~1500–1900	0.08–0.066	$\approx 2^{128}$
AES-192	128	12	15–18	~1900–2300	0.066–0.055	$\approx 2^{192}$
AES-256	128	14	18–22	~2300–2800	0.055–0.045	$\approx 2^{256}$
AES-NI	128	10	1.0–1.5	~150–200	≈ 1	$\approx 2^{128}$
DES	64	16	70–90	~560–720	0.014–0.011	$\approx 2^{56}$
TDES	64	48	200–250	~1600–2000	0.005–0.004	$\approx 2^{112}$
EC P-256	240	2 операції	~5000–6000	$\sim 1.2 \times 10^6$	~0.00017–0.0002	$\approx 2^{128}$
EC P-384	368	2 операції	~10 000–12 000	$\sim 2.8 \times 10^6$	~0.00008–0.0001	$\approx 2^{192}$

Примітка. Для Dual_EC_DRBG кожна ітерація виконує дві еліптичні операції множення точки над базовими точками P та Q.

Як видно з таблиці 1, AES залишається найбільш ефективним варіантом для побудови CTR-DRBG. У сучасних процесорах підтримка інструкцій AES-NI знижує час генерації до 1–1.5 циклів на байт, що робить CTR-DRBG одним із найшвидших генераторів в своєму класі, який забезпечує криптографічну стійкість визначену стандартом NIST. Але слід зауважити, що з теоретичної точки зору цей клас не володіє доказовою стійкістю, а має лише обчислювальну стійкість. Доведення криптографічної стійкості генераторів CTR-DRBG базується на зведені задачі зламу DRBG до задачі зламу блокового ширу, який в свою чергу оцінюється тестуванням статистичних властивостей, а ні математичним доведенням границь розподілу. В довгострокової перспективі це означає, що у разі зниження стійкості цього шифру або появі нового методу криптоаналізу під загрозу підпадають всі побудовані на його основі криптоалгоритми. Для усунення цього недоліку виникає потреба в розробці нового криптопримітиву, як це було в ситуації з алгоритмом DES. В алгоритмі AES, на відміну від DES, розробники вже намагалися деякі перетворення зробити доказово стійкими.

У зв'язку з цим, в NIST SP 800-90A була зроблена спроба отримати доказово стійку схему генерації ПВП на основі перетворень в групі точок еліптичної кривої, для якої, нажаль, з часом були знайдені недоліки [12]. Враховуючи, що процес знаходження уразливостей в математичних конструкціях є повільним, іноді це займає роки, на практиці для оперативної оцінки уразливостей алгоритмів DRBG використовують одну з методик тестування статистичних властивостей (статистичної безпеки): DIEHARD, CRYPT-S, RIPE, NIST STS. Як правило, перевага віддається стандартизованій методиці NIST STS [13-14].

Оцінка статистичних властивостей DRBG пакетом NIST Statistical Test Suite v2.1.2

Оцінювання статистичних властивостей псевдовипадкових послідовностей, згенерованих генераторами DRBG, виконано за допомогою пакета NIST Statistical Test Suite v2.1.2, який реалізує 15 базових статистичних тестів, визначених стандартом NIST SP 800-22. Для кожного алгоритму було згенеровано 100 незалежних бінарних послідовностей довжиною 1 000 000 біт. Перевірку проводили при рівні значущості $\alpha = 0.01$. Відповідно до вимог NIST, мінімальний рівень проходження тестів становить не менше 96 % для основних тестів і від 49 % до 69 % для тестів Random Excursions та Random Excursions Variant, залежно від кількості доступних траєкторій. Кожна згенерована послідовність оцінювалася за критерієм p-value, що дозволяє визначити статистичну відповідність розподілу бітів гіпотезі справжньої випадковості. Проходження тесту фіксувалося за умови p-value $\geq \alpha$, що свідчить про відсутність статистично значущих відхилень від рівномірного розподілу.

На діаграмах (рис. 1–10) по горизонтальній осі подано індекси тестів (Test Index), а по вертикальній – кількість послідовностей, що успішно пройшли тестування (Proportion of Passing Sequences).

Експериментальні дослідження проводилися на апаратній платформі Apple MacBook Pro (16-inch, 2021) з такими параметрами:

- процесор: Apple M1 Pro;
- оперативна пам'ять: 16 ГБ;
- операційна система: macOS Tahoe версії 26.1.

Сумарний та середній час генерації для кожного генератора наведено в таблиці 2.

Таблиця 2

Час генерації псевдовипадкових послідовностей для різних реалізацій DRBG-алгоритмів

Генератор	Загальний час генерації 100 послідовностей	Середній час генерації 1 послідовності
CTR_DRBG (DES)	13.837 с	0.138 с
CTR_DRBG (TDES)	40.304 с	0.403 с
CTR_DRBG (AES-256)	5.227 с	0.052 с
HASH_DRBG (SHA-1)	0.596 с	0.006 с

Генератор	Загальний час генерації 100 послідовностей	Середній час генерації 1 послідовності
HASH_DRBG (SHA-256)	0.384 с	0.004 с
HASH_DRBG (SHA-512)	0.227 с	0.002 с
HMAC_DRBG (SHA-1)	2.827 с	0.028 с
HMAC_DRBG (SHA-256)	1.712 с	0.017 с
HMAC_DRBG (SHA-512)	0.932 с	0.009 с
Dual_EC_DRBG (P-256)	20 хв 36 с	12.37 с
Dual_EC_DRBG (P-384)	35 хв 2 с	21.02 с

Отримані результати свідчать, що Dual_EC_DRBG характеризується найбільшою обчислювальною складністю через еліптичні операції, тоді як HASH_DRBG на основі SHA512 демонструє найвищу швидкодію. CTR-DRBG (AES256) та HMAC-DRBG (SHA256) забезпечують оптимальний баланс між продуктивністю та криптографічною стійкістю, що робить їх доцільними для практичного застосування у сучасних безпекових системах.

Для оцінки продуктивності генерації псевдовипадкових послідовностей було проведено порівняльний аналіз різних реалізацій алгоритмів DRBG. Вимірювання виконувалися на 64-бітній архітектурі з використанням метрики cycles per byte (cpb), що дозволило кількісно оцінити обчислювальні витрати кожного алгоритму. У таблиці 3 наведено показники швидкодії. Дані дозволяють порівняти ефективність симетричних (CTR_DRBG, HASH_DRBG, HMAC_DRBG) та еліптичних (Dual_EC_DRBG) підходів.

Таблиця 3

Оцінка продуктивності генераторів псевдовипадкових послідовностей (DRBG)

Генератор	Cycles / byte (cpb)	Оцінка швидкодії (1/cpb)
CTR_DRBG (DES)	70–90	0.014–0.011
CTR_DRBG (TDES)	200–250	0.005–0.004
CTR_DRBG (AES-256)	18–22	0.055–0.045
HASH_DRBG (SHA-1)	~22–28	~0.045–0.036
HASH_DRBG (SHA-256)	~12–16	~0.083–0.063
HASH_DRBG (SHA-512)	~9–11	~0.11–0.09
HMAC_DRBG (SHA-1)	~80–100	~0.012–0.010
HMAC_DRBG (SHA-256)	~60–70	~0.017–0.014
HMAC_DRBG (SHA-512)	~45–55	~0.022–0.018
Dual_EC_DRBG (P-256)	5 000–6 000	0.00020–0.00017
Dual_EC_DRBG (P-384)	10 000–12 000	0.00010–0.00008

За даними проведеного аналізу бачимо, що генератори на основі симетричних алгоритмів мають значно вищу швидкодію завдяки меншій обчислювальній складності. Натомість, реалізації Dual_EC_DRBG на еліптичних кривих, забезпечують вищу криптостійкість, проте мають найменшу продуктивність через складність операцій множення точок на кривій.

Результати тестування CTR_DRBG

Результати проведеного статистичного тестування показали, що генератор CTR-DRBG на основі DES успішно пройшов усі базові тести пакета NIST STS, а p-значення перебували в межах 0.05–0.96.

Незначне зниження спостерігалося лише в тесті Non-Overlapping Template, проте пропорція проходження залишалася в межах норми. Це підтверджує коректність формування послідовностей, однак через обмежену довжину ключа (56 біт) алгоритм DES не відповідає сучасним вимогам криптографічної стійкості і може використовуватись лише для демонстраційних цілей, що підтверджує недосконаліть цього алгоритму.

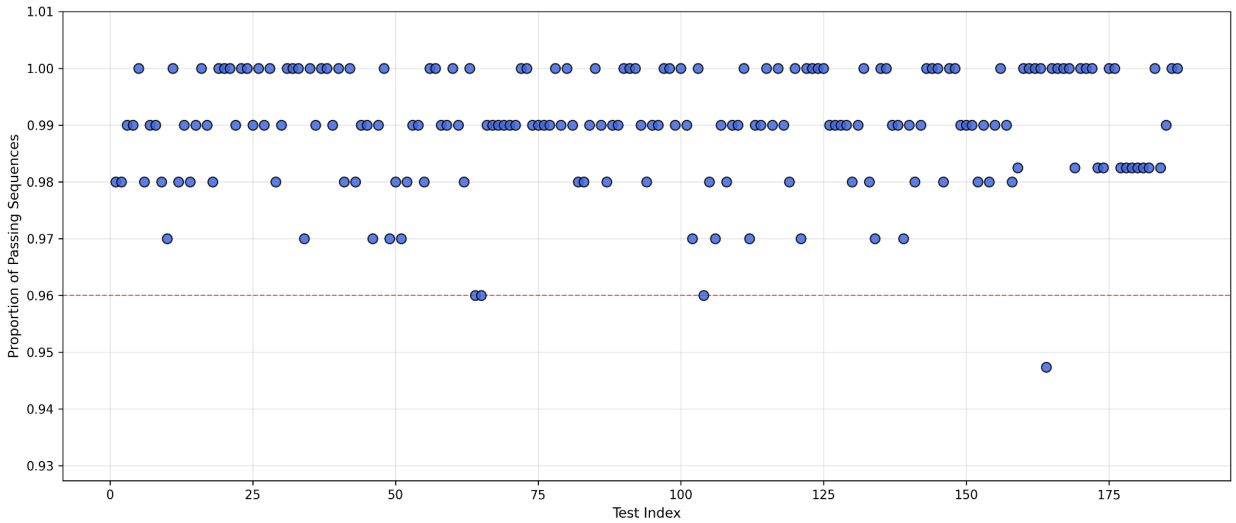


Рис. 1. Результати статистичного оцінювання генератора CTR_DRBG (на основі DES) за допомогою NIST Statistical Test Suite v2.1.2

Тестування CTR-DRBG, реалізованого з використанням Triple DES (TDES), показало рівномірний розподіл p-значень у межах 0.1–0.95. Тести Frequency, Runs, Cumulative Sums і FFT засвідчили стабільність, а для Random Excursions та Random Excursions Variant зафіксовано проходження понад 70 з 73 послідовностей, що перевищує мінімально допустимий поріг. Генератор формує статистично якісні послідовності, однак поступається за швидкодією через потрійне шифрування і має схожі на DES недоліки щодо криптографічної стійкості.

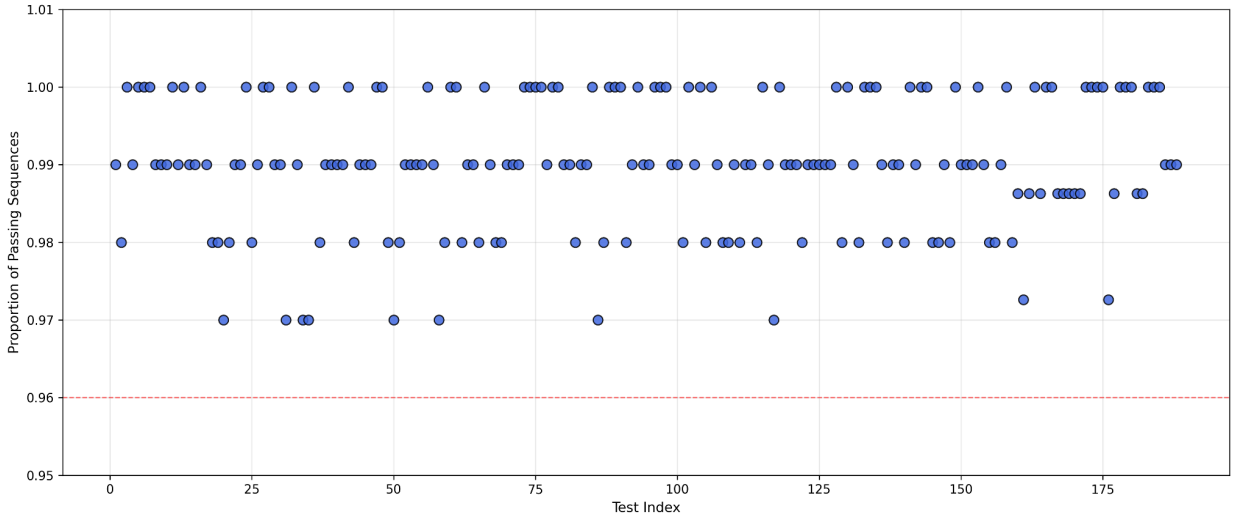


Рис. 2. Результати статистичного оцінювання генератора CTR_DRBG (на основі TDES) за допомогою NIST Statistical Test Suite v2.1.2

Перевагою є підвищена стійкість ($\approx 2^{112}$), за рахунок лише збільшення довжини ключової послідовності, а недоліком – зниження швидкодії через потрійне шифрування.

CTR-DRBG, побудований на основі AES-256, продемонстрував найкращі результати серед усіх реалізацій. Усі статистичні тести пройдено зі 100 % успішністю, *p*-значення рівномірно розподілені в межах 0.17–0.97. Тести Approximate Entropy, Serial і Linear Complexity не виявили відхилень, що підтверджує високу ентропію й однорідність згенерованих послідовностей. Це відповідає вимогам стандартів NIST SP 800-22 та NIST SP 800-90A Rev. 1.

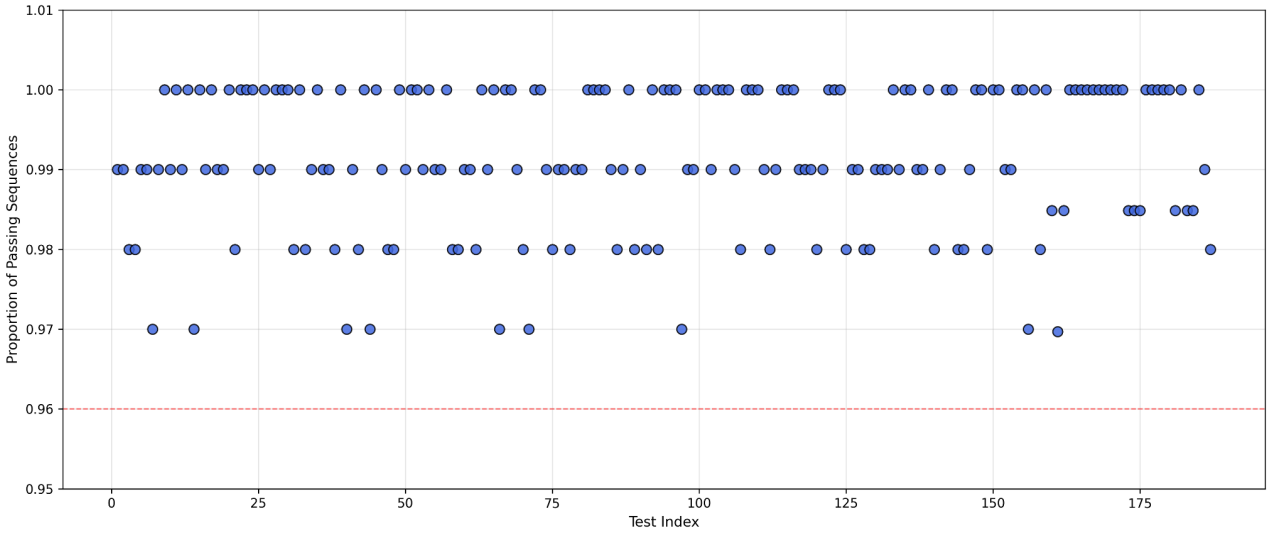


Рис. 3. Результати статистичного оцінювання генератора CTR_DRBG (на основі AES) за допомогою NIST Statistical Test Suite v2.1.2

Алгоритм забезпечує максимальну ентропію, рівномірність вихідних даних і найвищу криптографічну стійкість ($\sim 2^{256}$).

Узагальнені результати свідчать, що всі досліджувані реалізації CTR-DRBG – на основі DES, TDES та AES – формують статистично випадкові послідовності, які відповідають критеріям NIST SP 800-22. Найкращі показники продемонстрував CTR-DRBG(AES) зі стандарту NIST SP 800-90A Rev. 1, який поєднує високу швидкодію, максимальну ентропію та криптографічну стійкість, тоді як реалізації на базі DES і TDES є менш ефективними та не відповідають сучасним вимогам практичної безпеки.

Результати тестування HASH_DRBG

Результати статистичного тестування показали, що генератор HASH_DRBG, реалізований на основі SHA-1, формує послідовності з рівномірним розподілом p-значень і високою пропорцією проходження базових тестів пакета NIST STS. Це підтверджує відсутність статистично значущих відхилень та випадковість згенерованих даних (рис. 4).

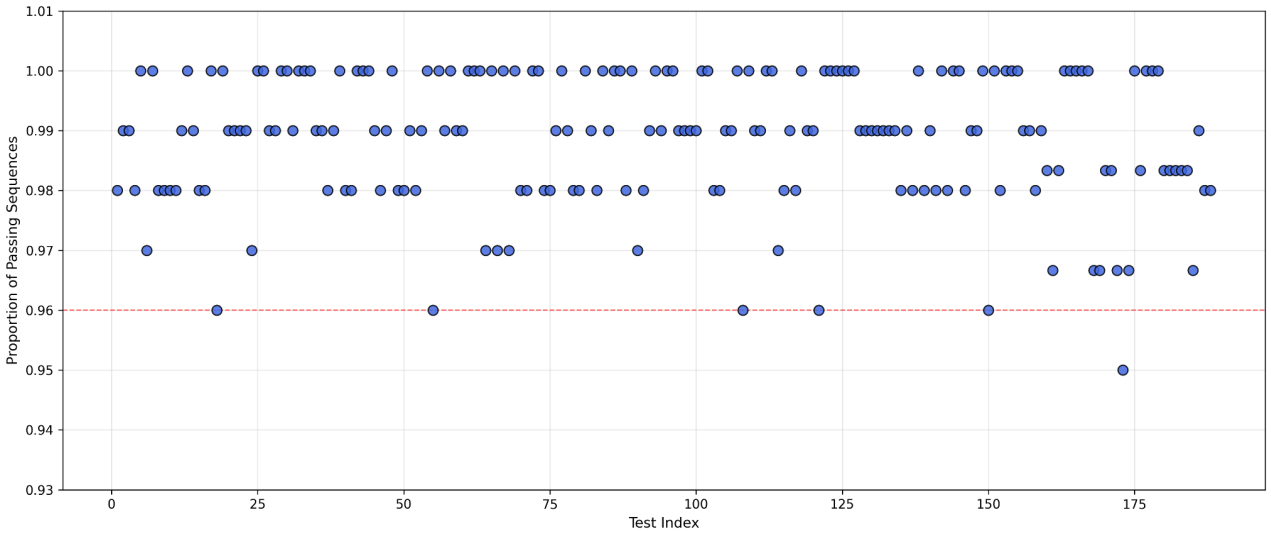


Рис. 4. Результати статистичного оцінювання генератора HASH_DRBG (на основі SHA1) за допомогою NIST Statistical Test Suite v2.1.2

Алгоритм забезпечує, в цілому, задовільні статистичні властивості, однак використання SHA1 на сьогодні не забезпечує достатній рівень стійкості до колізій геш-функцій, в зв'язку з чим рекомендовано до використання алгоритми не гірше за SHA256.

Тестування HASH_DRBG на основі SHA-256 показало рівномірний розподіл p-значень і пропорцію проходження, що відповідає вимогам стандарту NIST SP 800-22. Усі тести отримали задовільні статистичні властивості без відхилень, що свідчить про придатність алгоритму для практичного використання у криптографічних системах (рис. 5).

Переваги – достатня статистична безпека генератора, достатня криптографічна стійкість без явних недоліків.

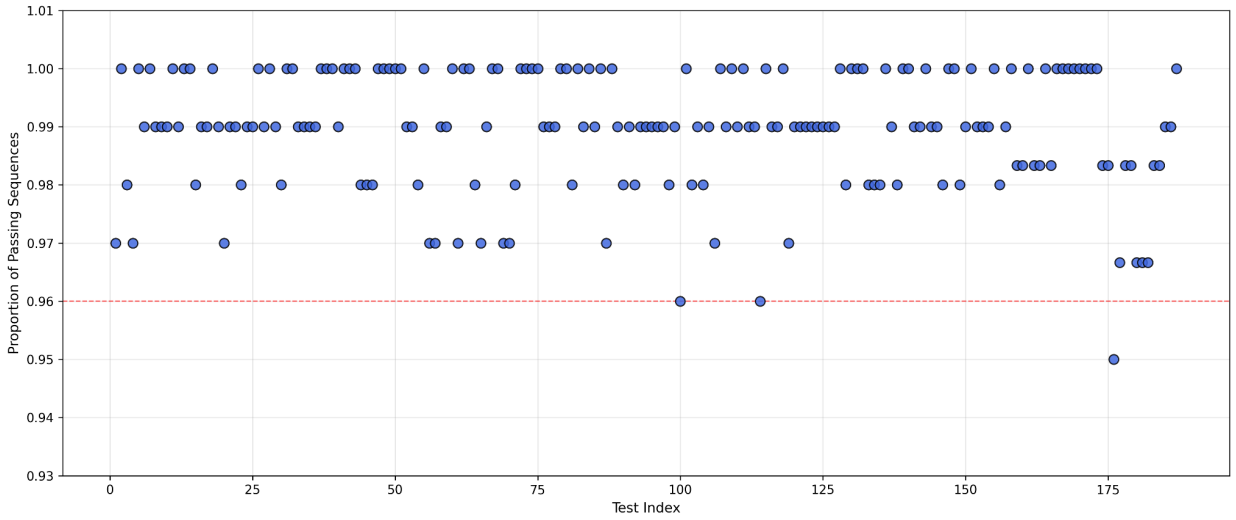


Рис. 5. Результати статистичного оцінювання генератора HASH_DRBG (на основі SHA256) за допомогою NIST Statistical Test Suite v2.1.2

Для HASH_DRBG на основі SHA512 отримано найвищій рівень статистичної безпеки серед усіх протестованих реалізацій: *p*-значення розподілені рівномірно в межах допустимих значень, а частка успішного проходження тестів перевищує мінімальні пороги (0.96 для 100 зразків і 0.49 для 52 зразків). Це підтверджує повну відповідність послідовностей критеріям випадковості та непередбачуваності (рис. 6).

Алгоритм демонструє максимальну статистичну безпеку і криптографічну стійкість, проте має підвищені обчислювальні витрати порівняно з SHA256.

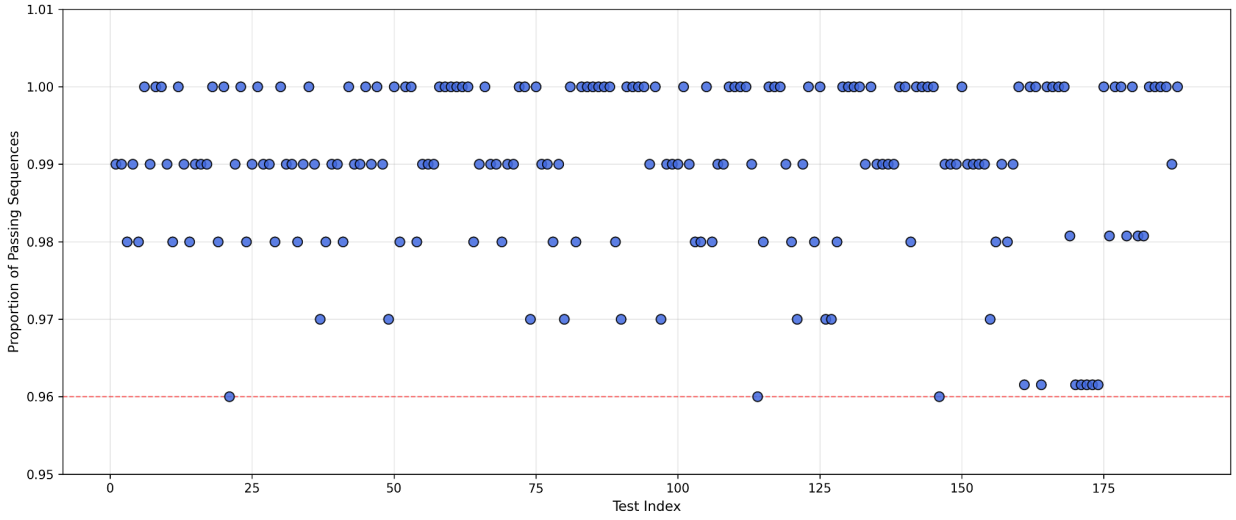


Рис. 6. Результати статистичного оцінювання генератора HASH_DRBG (на основі SHA512) за допомогою NIST Statistical Test Suite v2.1.2.

Узагальнюючи результати, наведені на рисунках 4–6, можна зробити висновок, що всі протестовані реалізації HASH_DRBG забезпечують статистично випадкові, рівномірні та непередбачувані послідовності, які відповідають вимогам стандартів NIST SP 800-22 та NIST SP 800-90A Rev. 1. Найкращий баланс між швидкодією та рівнем стійкості продемонстрував HASH_DRBG(SHA-256), тоді як SHA-512 характеризується максимальною стійкістю, а SHA1 поступається через застарілий алгоритм гешування.

Результати тестування HMAC_DRBG

Результати узагальненого тестування показано на рисунку 7, де подано перевірку рівномірності p-значень та частки послідовностей, що успішно пройшли кожен із тестів. Отримані значення розподілені в межах допустимого інтервалу [0;1] без ознак систематичних відхилень, а пропорції проходження перевищують мінімальні пороги, визначені методикою NIST STS. Це свідчить про відсутність статистичних аномалій у згенерованих даних.

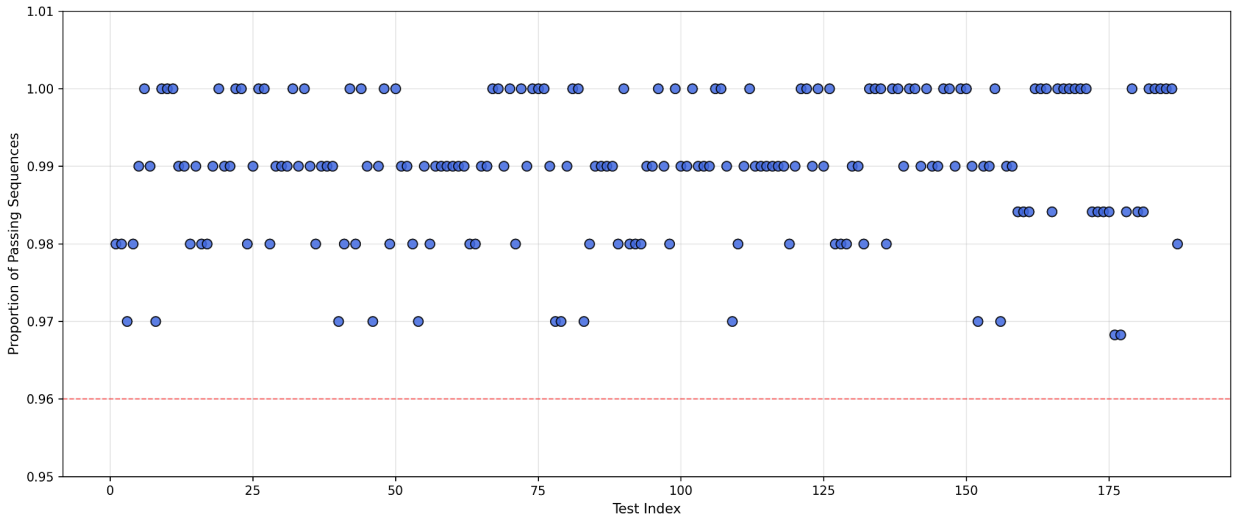


Рис. 7. Результати статистичного оцінювання генератора HMAC_DRBG (на основі SHA1) за допомогою NIST Statistical Test Suite v2.1.2

Отримано рівномірний розподіл *p*-значень і повне проходження тестів; недолік – використання застарілої хеш-функції SHA1.

Згідно з результатами тестування, представленими на рисунку 8, реалізація HMAC DRBG на основі SHA256 демонструє аналогічно високу статистичну якість: *p*-значення рівномірно розподілені, усі тести пройдено успішно, а пропорції проходження відповідають вимогам стандарту NIST SP 800-22. Це підтверджує надійність генерації псевдовипадкових послідовностей для криптографічних систем, що потребують високої ентропії та передбачуваної стійкості.

Алгоритм забезпечує високу ентропію та рівномірність вихідних даних; рекомендований для практичного застосування.

На основі результатів, наведених на рисунках 7–8, можна зробити висновок, що обидві реалізації HMAC_DRBG – на базі SHA-1 та SHA-256 – формують статистично випадкові та рівномірно розподілені послідовності, які відповідають критеріям випадковості, визначеним стандартом NIST SP 800-22. При цьому SHA256 забезпечує вищу криптографічну стійкість і є більш доцільним для сучасних систем криптографічного захисту інформації.

Результати тестування Dual_EC_DRBG

Статистичне оцінювання генератора Dual_EC_DRBG, реалізованого на еліптичних кривих P-256 та P-384, показало відповідність вимогам стандарту NIST SP 800-22. Для реалізації на кривій P-256 усі основні тести пакета NIST STS успішно пройдено: p-значення розподілені рівномірно в межах 0.004–0.98, а частка проходження перевищує мінімально

допустимий поріг (96 % для 100 послідовностей). Незначні відхилення спостерігались у тестах Non-Overlapping Template, однак вони не вплинули на загальну оцінку випадковості (рис. 9).

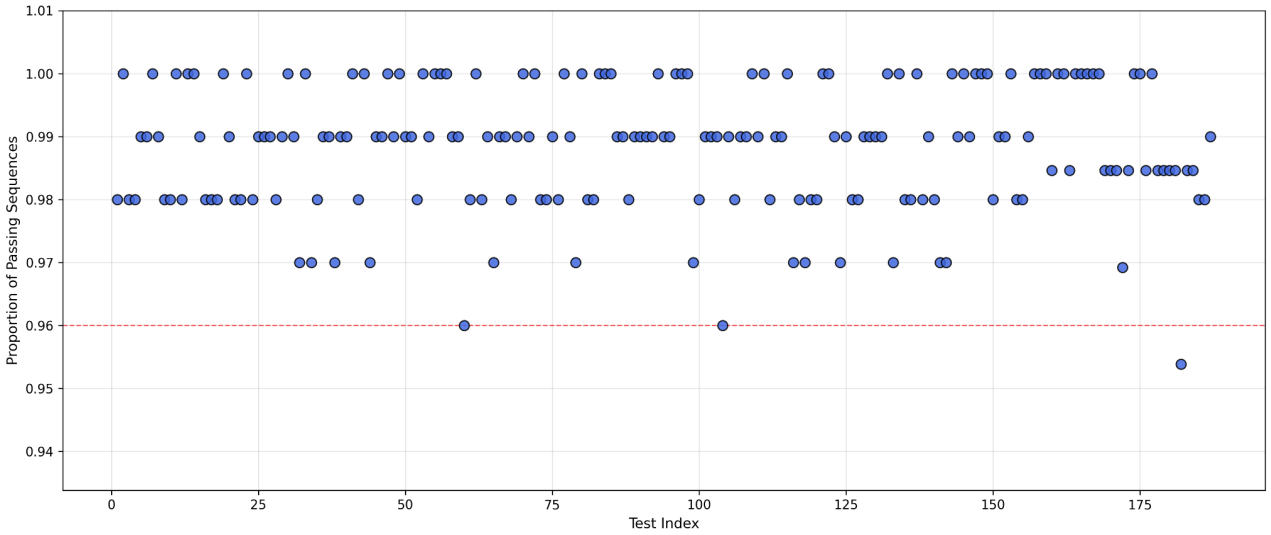


Рис. 8. Результати статистичного оцінювання генератора HMAC DRBG (на основі SHA256) за допомогою NIST Statistical Test Suite v2.1.2

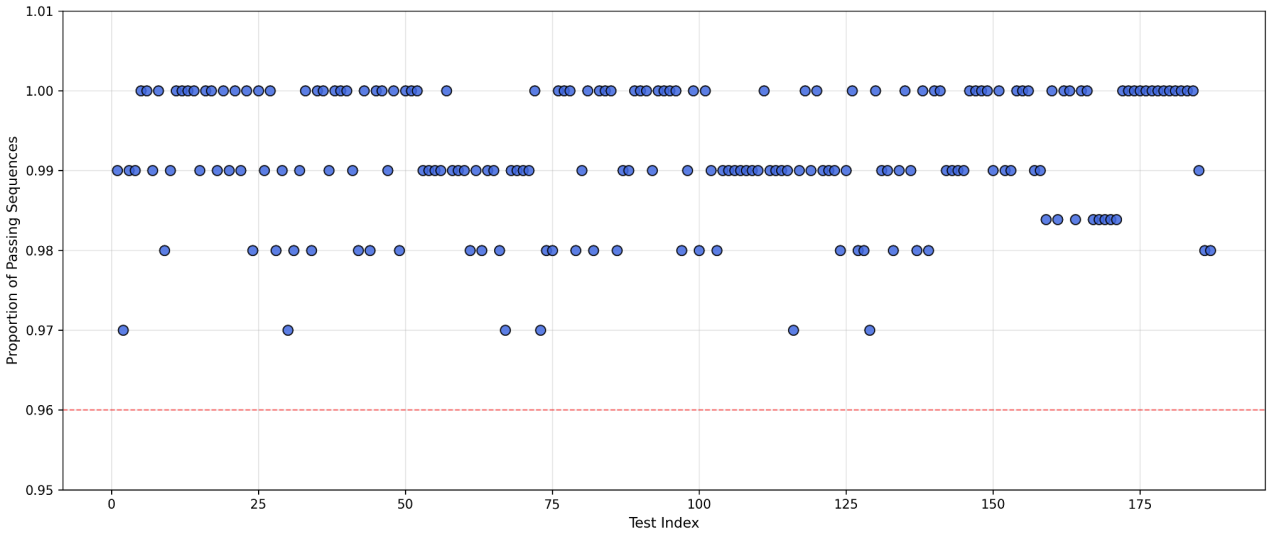


Рис. 9. Результати статистичного оцінювання генератора Dual_EC_DRBG (256 біт) за допомогою NIST Statistical Test Suite v2.1.2

Перевагою генератора є висока статистична якість та відсутність систематичних аномалій, а недоліком – значна обчислювальна складність процесу генерації.

Для реалізації на кривій P-384 отримано аналогічно високі показники випадковості: *p*-значення рівномірно розподілені в діапазоні 0.004–0.99, усі базові тести пройдено з часткою успіху понад 97 %. Додаткові тести Random Excursions та Random Excursions Variant підтвердили відсутність статистично значущих відхилень, що засвідчує правильність роботи генератора (рис. 10).

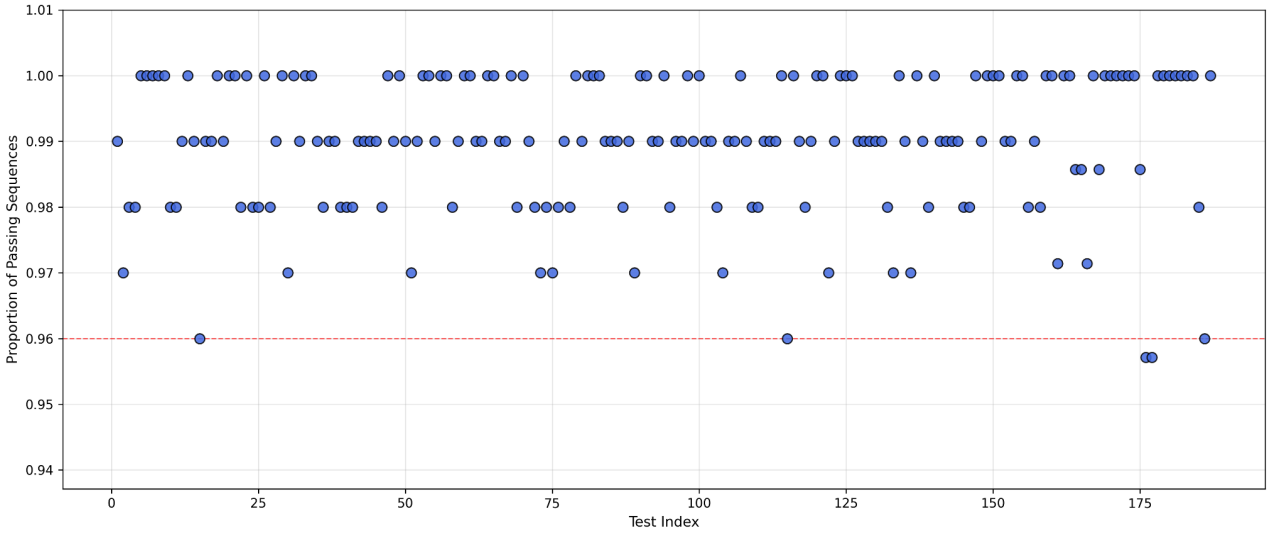


Рис. 10. Результати статистичного оцінювання генератора Dual_EC_DRBG (384 біт) за допомогою NIST Statistical Test Suite v2.1.2

Генератор характеризується рівномірним розподілом, високою ентропією та стабільністю результатів, однак має низьку швидкодію й значні часові витрати через обчислення на еліптичних кривих.

Узагальнюючи, Dual_EC_DRBG демонструє найвищу статистичну якість серед протестованих генераторів, проте має найнижчу продуктивність, що обмежує його практичне застосування у високошвидкісних системах.

Висновки

Таким чином, оцінки статистичної безпеки отримані для таких генераторів ПВП як CTR_DRBG (AES), CTR_DRBG (DES), CTR_DRBG (TDES), HASH_DRBG (SHA256), HASH_DRBG (SHA384), HASH_DRBG (SHA512), HMAC_DRBG (SHA1), HMAC_DRBG (SHA-256), Dual_EC_DRBG (P-256), Dual_EC_DRBG (P-384) показали перевагу генераторів ПВП на основі перетворень в групі точок еліптичної кривої, а саме генератор на основі еліптичних кривих Dual_EC_DRBG (256 біт) дозволив отримати псевдовипадкові послідовності 97 % яких пройшли всі тести NIST STS. Однак цей клас генераторів програє за швидкодією класу CTR_DRBG. Так, для генерації 10^8 бітів генератор Dual_EC_DRBG (P-256) витрачає 49.46 [c], Dual_EC_DRBG (P-384) – 84.09 [c], порівняно з CTR_DRBG (AES-256) – 5.227 [c] та HASH_DRBG (SHA-256) – 0.384 [c] відповідно.

Серед усіх генераторів ПВП, що досліджувалися, найкращій за швидкодією виявився лінійний генератор псевдовипадвоких властивостей PCG з показником 0.25–0.67 [1/cpb] та LFSR з показником 0.5 [1/cpb], але стійкість цього класу генераторів не задовольняє вимоги стандарту NIST SP 800-90A і не може використовуватися для захисту конфіденційної інформації. Найкращу оцінку обчислювальної швидкодії генераторів DRBG в класі генераторів CTR_DRBG отримав генератор CTR_DRBG(AES128) з показником 0.08–0.066 [1/cpb], але слід зауважити щодо цей тип генераторів на основі блокових шифрів не забезпечує доведену криптографічну стійкість, як це дозволяють зробити алгоритми на основі факторизації цілих чисел, дискретного логарифмування в простому полі, в групі точок еліптичної кривої або в ізогеніях еліптичної кривої.

Таким чином, процес вибору генераторів DRBG для реальних криптографічних додатків є складним та потребуючим комплексного підходу до вибору між максимальною криптографічною стійкістю та порівняльною якістю криптографічних послуг за причиною невеликої швидкодії криптоперетворень та якісними криптографічними послугами з відносно невеликим рівнем криптографічної стійкості генераторів ПВП.

Рішенням цього протиріччя є наступні наукові дослідження, а саме розробка нових методів генерації ПВП стійких до квантового криптоаналізу до повного переходу на постквантові криптосистеми, які планується впроваджувати в різноманітні сучасні технології такі як блокчейн, смартміcто, системи з використанням штучного інтелекту та інші системи, що потребують конфіденційності та автентичності даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. S. Coretti, Y. Dodis, H. Karthikeyan, and S. Tessaro. Seedless fruit is the sweetest: Random number generation, revisited. In Annual International Cryptology Conference, pages 205–234. Springer, 2019.

2. G. Bertoni, J. Daemen, S. Hoffert, M. Peeters, G. Van Assche, R. Van Keer, and B. Viguier. TurboSHAKE. Cryptology ePrint Archive, 2023.

3. John Kelsey, Stefan Lucks, Stephan Müller. XDRBG: A Proposed Deterministic Random Bit Generator Based on Any XOF. March 1, 2024

4. Woohyuk Chung, Seongha Hwang, Hwigyeom Kim, Jooyoung Lee. Enhancing Provable Security and Efficiency of Permutation-based DRBGs. Korea Advanced Institute of Science and Technology. A major revision of an IACR publication in CRYPTO 2025.

5. Josef Pieprzyk, Marcin Pawłowski, Paweł Morawiecki, Arash Mahboubi, Jarek Duda & Seyit. Pseudorandom bit generation with asymmetric numeral systems. International Journal of Information Security. Volume 24, article number 82, (2025).

6. Kelsey J., Ferguson N. Cryptographic Random Number Generation: Design, Implementation, and Evaluation // IEEE Security & Privacy. 2005. Vol. 3(2). P. 28–38.

7. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators (NIST SP 800-90A Rev. 1). Gaithersburg: NIST, 2015.

8. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Hoboken: Wiley, 2010.

9. Shannon C. E. A Mathematical Theory of Communication // Bell System Technical Journal. 1948. Vol. 27. P. 379–423, 623–656.

10. Eastlake D., Schiller J., Crocker S. Randomness Requirements for Security. RFC 4086, IETF, June 2005.

11. National Institute of Standards and Technology. FIPS PUB 140-3: Security Requirements for Cryptographic Modules. Gaithersburg: NIST, 2019.

12. Daniel R. L. Brown & Kristian Gjøsteen. A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator. Advances in Cryptology - CRYPTO 2007. P. 466–481.

13. Rukhin A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (SP 800-22 rev.1a). NIST, 2010.

14. BSI. TR-02102-1: Cryptographic Mechanisms – Recommendations and Key Lengths. Bonn: Federal Office for Information Security (BSI), 2023.

15. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. New York: John Wiley & Sons, 1996. 784 p.

16. Чевардін В. Є. Методи побудови генераторів псевдовипадкових послідовностей на основі ізоморфних перетворень еліптичних кривих : дисертація доктора технічних наук : 05.13.21 – Системи захисту інформації / Чевардін Владислав Євгенійович ; Харків. нац. ун-т ім. В. Н. Каразіна. Харків, 2017. 340 с. Державний реєстр № 0518U000308.

АВТОРИ НОМЕРА

1. ***Абрабаєв Максим Андрійович*** – курсант Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

2. ***Бернацький Андрій Петрович*** – доктор філософії, старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

3. ***Бовда Едуард Миколайович*** – кандидат технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

4. ***Власенко Олександр Володимирович*** – доктор філософії, заступник начальника кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

5. ***Восколович Олексій Іванович*** – кандидат технічних наук, доцент Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

6. ***Гурський Тарас Григорович*** – кандидат технічних наук, доцент, начальник відділу Науково-дослідного інституту воєнної розвідки, м. Київ, Україна.

7. ***Данилюк Ігор Андрійович*** – кандидат технічних наук, доцент, головний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

8. ***Дімітров Павло Євстафійович*** – науковий співробітник Науково-дослідного інституту воєнної розвідки, м. Київ, Україна.

9. ***Єрохін Віктор Федорович*** – доктор технічних наук, професор, головний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

10. ***Загоровець Олег Вікторович*** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

11. ***Залужний Олексій Вікторович*** – кандидат технічних наук, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

12. ***Зарубенко Артур Олександрович*** – доктор філософії, начальник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

13. ***Зінченко Наталія Романівна*** – заступник начальника навчального відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

14. ***Каптур Вадим Анатолійович*** – кандидат технічних наук, старший науковий співробітник, начальник відділення перспективного розвитку Окремого спеціального центру електронної підтримки Сухопутних військ Збройних Сил України, м. Київ, Україна.

15. ***Клименко Віктор Михайлович*** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

16. ***Коваленко Ілля Григорович*** – кандидат технічних наук, начальник відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

17. ***Коваленко Олексій Олександрович*** – начальник Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

18. ***Комаров Володимир Олександрович*** – кандидат технічних наук, провідний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

19. ***Кондрусь Андрій Володимирович*** – заступник начальника кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

20. ***Костюк Богдан Михайлович*** – курсант Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

21. ***Котенко Володимир Миколайович*** – кандидат технічних наук, доцент, професор кафедри Житомирського військового інституту імені С. П. Корольова, м. Житомир, Україна.

22. ***Кравчик Роман Сергійович*** – викладач кафедри зенітних ракетних комплексів малої дальності факультету зенітних ракетних військ Харківського національного університету Повітряних Сил імені Івана Кожедуба, м. Харків, Україна.

23. ***Кузавков Василій Вікторович*** – доктор технічних наук, професор, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

24. ***Куйбіда Назар Сергійович*** – курсант Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

25. ***Куцаєв Володимир Вікторович*** – молодший науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

26. ***Лисенко Дмитро Олександрович*** – аспірант кафедри технічного захисту кібербезпеки Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна.

27. ***Ломакін Єгор В'ячеславович*** – курсант Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

28. ***Мазулевский Олег Євгенович*** – кандидат технічних наук, начальник управління Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

29. ***Макаренко Карина Леонидівна*** – слухач Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

30. ***Максимов Іван Олексійович*** – ад'юнкт Національного університету оборони України, м. Київ, Україна.

31. ***Масич Віталій Володимирович*** – курсант Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

32. ***Меркотан Дмитро Юрійович*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

33. ***Мірoненко Ольга Всеволодівна*** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

34. ***Панченко Ігор В'ячеславович*** – кандидат технічних наук, доцент, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

35. ***Пилипчук Ігор Юрійович*** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

36. ***Погребняк Сергій Васильович*** – доктор філософії, старший викладач, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

37. ***Прийма Олексій Олегович*** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

38. ***Радзівілов Григорій Данилович*** – кандидат технічних наук, професор, заступник начальника Військового інституту телекомунікацій та інформатизації імені Героїв Крут з наукової роботи, м. Київ, Україна.

39. ***Романенко Марія Михайлівна*** –доктор філософії, старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

40. ***Романенко Сергій Олексійович*** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

41. ***Сайко Володимир Григорович*** – доктор технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

42. ***Салій Олександр Сергійович*** – науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

43. ***Самохвалов Юрій Якович*** – доктор технічних наук, професор кафедри інтелектуальних технологій Київського національного університету імені Тараса Шевченка, м. Київ, Україна.

44. ***Семитківська Ірина Володимирівна*** – старший помічник начальника науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

45. ***Симоненко Олександр Анатолійович*** – кандидат технічних наук, доцент, начальник відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

46. ***Соловйова Тетяна Василівна*** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

47. ***Субач Ігор Юрійович*** – доктор технічних наук, професор, завідувач спеціальної кафедри Інституту спеціального зв’язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна.

48. ***Терещенко Тетяна Павлівна*** – старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

49. ***Тлустий Андрій Олександрович*** – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

50. ***Троцько Олександр Олександрович*** – кандидат технічних наук, доцент, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

51. ***Туровський Олександр Леонідович*** – доктор технічних наук, професор, завідувач кафедри технічного захисту кібербезпеки Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна.

52. ***Устинов Дмитро Андрійович*** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

53. ***Фесенко Олексій Дмитрович*** – доктор філософії, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

54. ***Фесьоха Віталій Вікторович*** – доктор філософії, доцент, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

55. ***Фомін Микола Миколайович*** – доктор філософії, заступник начальника факультету Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

56. ***Хоменко Павло Володимирович*** – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

57. ***Хусаінов Павло Валентинович*** – кандидат технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

58. ***Чевардін Владислав Євгенійович*** – доктор технічних наук, професор, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

59. ***Череушенко Вікторія Борисівна*** – слухач Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

60. ***Штаненко Сергій Станіславович*** – кандидат технічних наук, доцент, заступник начальника центру Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

ПАМ'ЯТКА АВТОРУ

Наукові статті у фахових виданнях повинні мати такі необхідні елементи:

анотація як стисла стаття;

постановка проблеми у загальному вигляді та її зв'язок із важливими науково-практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано розв'язання зазначеної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується стаття;

формулювання мети статті (**постановка наукового завдання**);

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів;

висновки з цього дослідження і **перспективи** подальших досліджень у зазначеному напрямку;

список використаних джерел: 10–15 посилань терміном **не більше 10 років.**

Редакція не рекомендує використання джерел інформації держав-агресорів.

До друку приймаються оригінальні наукові праці, які не було відправлено до інших редакцій та не опубліковано раніше в інших виданнях.

Рукопис статті потрібно подавати разом з наступними документами:

довідка про результати перевірки на академічний плагіат;

акт експертної оцінки про можливість відкритого опублікування (1 примірник);

згода на публікацію статті та оприлюднення персональних даних;

відомості про автора (авторів) за формою: прізвище, ім'я та по батькові; науковий ступінь, вчене звання, посада; назва установи, де працює автор, її місце розташування (місто, країна); обліковий запис автора ORCID, електронна адреса та номер телефону.

Відомості про автора (авторів) подаються окремим супровідним файлом. Наприклад:

№ з/п	Українська мова	Англійська мова
1	**Шевченко Олександр Іванович** Кандидат технічних наук Доцент Старший викладач Військовий інститут телекомунікацій та інформатизації імені Героїв Крут; м. Київ, Україна https://orcid.org/0000-0000-0000-0000 e-mail _____, телефон _____	**Shevchenko Oleksandr** Candidate of Technical Sciences Associate Professor Senior Lecturer Military Institute of Telecommunications and Informatization Technologies named after Heroes of Kruty; Kyiv, Ukraine https://orcid.org/0000-0000-0000-0000

Рукопис подається в друкованому та електронному вигляді у текстовому редакторі Microsoft Word, а також може бути надісланий за електронною адресою: naukaviti@viti.edu.ua.

Якщо стаття подається в електронному вигляді, супровідні документи подаються у сканованому вигляді.

Обсяг рукопису – не менше 7 повних аркушів українською або англійською мовами.

Формат аркушу – А4 (210 мм × 297 мм).

Параметри сторінки: зліва – 20 мм, справа – 20 мм, зверху – 20 мм, знизу – 20 мм.

Основний шрифт статті – Times New Roman, розмір 12 пт, міжрядковий інтервал – 1,0; абзацний відступ – 1,0 см; вирівнювання – по ширині; із виключенням переносів.

У лівому кутку першої сторінки на першому рядку друкується шифр УДК, розмір 12 пт, у правому кутку першої сторінки на другому рядку – дані про авторів: науковий ступінь, вчене звання, ініціали і прізвище автора, ORCID, в дужках назва установи, де він працює. Наприклад: к. т. н. Шевченко О. І. ORCID: 0000-0000-0000-0000 (ВІТІ ім. Героїв Крут). Далі через рядок друкується назва статті (відцентрована, великими напівжирними літерами).

Пропуск (перед і після назви статті та кожного розділу) – 1 рядок.

Анотацію друкують курсивом, шрифт Times New Roman, розмір 10 пт. Анотацію та ключові слова приводять українською та англійською мовами. Обсяг кожної з них не менше **1800 знаків з пробілами**, включаючи ключові слова. Анотація повинна бути структурована таким чином: вступ, проблематика, мета, матеріали й методи, результати, висновки. Іншими словами, анотація повинна відображати послідовну логіку опису результатів, описувати основну мету дослідження та підсумовувати найбільш значимі результати. Скорочення слів в анотації не застосовувати.

Після анотації вказати 6–8 ключових слів окремо українською та англійською мовами.

Список використаних джерел оформлюється шрифтом Times New Roman, розмір 11 пт, та складається з урахуванням Національного стандарту України ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання».

Посилання на використані джерела наводяться у тексті статті у квадратних дужках […] із зазначенням порядкового номеру бібліографічного посилання у списку.

Редакційна колегія залишає за собою право вносити зміни в рукопис редакційного характеру.

Телефон для довідок: (044) 256-22-37.

Адреса сайту збірника: https://journal.viti.edu.ua/index.php/cicst/issue/archive.

Електронна адреса для надання статей: naukaviti@viti.edu.ua.