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
№ 6

Communication, informatization and cybersecurity systems and technologies
№ 6

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 – 2024 – Kyiv

УДК 621
ББК Ц4 (4Укр) 39
З – 415

Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. – Київ: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. – 2024. – № 6. – 280 с. – DOI: 10.58254/viti.6.2024.

ISSN 2786-6610прг\в

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@gmail.com

Відповідальний за випуск: Куцаєв В. В.
Зам. № 307. Друк. арк. 35,00. Ум.-друк. арк. 32,55. Обл.-вид. арк. 30,27.
Формат паперу 60×84/8. Тираж 55 прим.
Адреса друкарні ВІТІ імені 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.6.2024.01.5

УДК 621.396

Артюх С. Г. ORCID: 0000-0003-2142-1552 (ВІТІ ім. Героїв Крут)
д-р техн. наук, професор Жук О. В. ORCID: 0000-0002-3546-1507 (НУОУ)
канд. техн. наук, доцент Симоненко О. А. ORCID: 0000-0001-8511-2017 (ВІТІ ім. Героїв Крут)
Марченко П. А. ORCID: 0009-0006-7261-6316 (НТУУ "КПІ ім. Ігоря Сікорського")

МОДЕЛІ ТА МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ВІЙСЬКАМИ

Безпроводові сенсорні мережі є важливим елементом сучасних військових операцій, що забезпечують моніторинг та передачу даних у реальному часі. Однак ці мережі вразливі до фізичних і кібератак через обмеженість ресурсу, відсутність фізичного контролю над сенсорами та викликами, що пов'язані з використання безпроводових каналів зв'язку. Метою статті є проведення порівняльного аналізу моделей та методів виявлення вторгнень у безпроводових сенсорних мережах тактичної ланки управління військами.

Аналіз охоплює централізовані та децентралізовані підходи до управління безпекою з акцентом на моделі виявлення, що базуються на сигнатурах, аномаліях та специфікаціях. Також у статті розкрито можливості використання гібридних методів, що комбінують переваги вищезазначених підходів. Для порівняння ефективності моделей використовувалися загальнодоступні набори даних (KDD, NSL-KDD, WSN-DS) та синтетичні набори даних отриманих з використанням мережевих симуляторів. Результати показують, що централізовані моделі більш ефективні для малих мереж, але створюють навантаження на базову станцію, що може спричиняти затримки при виявленні атак. Децентралізовані моделі знижують навантаження та підвищують швидкість реагування на атаки, проте також мають свої недоліки. У статті зазначено, що жоден з існуючих методів не забезпечує повного захисту, тому комбінування підходів є найбільш ефективним рішенням.

Моделі та методи виявлення вторгнень на основі аномалій класифікуються залежно від їх функціональних можливостей: на основі статистики, на основі інтелектуального аналізу даних, на основі машинного навчання та на основі штучного інтелекту. Використання штучних нейронних мереж і машинного навчання значно покращує точність виявлення аномалій, але такі системи вимагають великих обчислювальних ресурсів та складні в налаштуванні.

Основний аналітичний висновок статті полягає в необхідності створення гібридної системи виявлення вторгнень з використанням штучних нейронних мереж і машинного навчання, яка поєднує централізовані та децентралізовані методи з урахуванням специфічних загроз для безпроводових сенсорних мереж тактичної ланки управління військами.

Напрямом подальших досліджень слід вважати розроблення функціональної моделі системи виявлення вторгнень для підсистеми безпеки у безпроводових сенсорних мережах тактичної ланки управління військами.

Ключові слова: *безпроводові сенсорні мережі, виявлення вторгнень, управління безпекою, тактична ланка управління, нейронні мережі, виявлення аномалії.*

S. Artiukh, O. Zhuk, O. Simonenko, P. Marchenko Models and methods of intrusion detection in wireless sensor networks of the tactical level of troop control

Wireless sensor networks are an important element of modern military operations, providing real-time monitoring and data transmission. However, these networks are vulnerable to both physical and cyber attacks due to limited resources, lack of physical control over the sensors, and challenges associated with using wireless communication channels. The aim of the article is to conduct a comparative analysis of models and methods for intrusion detection in tactical command-level wireless sensor networks.

The analysis covers centralized and decentralized security management approaches with a focus on detection models based on signatures, anomalies, and specifications. The article also explores the potential of using hybrid methods that combine the advantages of the aforementioned approaches. Publicly available datasets (KDD, NSL-KDD, WSN-DS) and synthetic datasets generated using network simulators were used to compare the effectiveness of the models. The results show that centralized models are more effective for small networks but create a load on the base station, which can cause delays in attack detection. Decentralized models reduce the load and improve the speed of response to attacks, but they also have their drawbacks. The article notes that none of the existing methods provide complete protection, so a combination of approaches is the most effective solution.

Anomaly-based intrusion detection models and methods are classified according to their functional capabilities: statistics-based, data mining-based, machine learning-based, and artificial intelligence-based. The use of artificial neural networks and machine learning significantly improves the accuracy of anomaly detection, but such systems require large computational resources and are complex to configure.

The main analytical conclusion of the article is the need to create a hybrid intrusion detection system using artificial neural networks and machine learning, which combines centralized and decentralized methods while considering specific threats to tactical command-level wireless sensor networks.

Future research should focus on developing a functional model of an intrusion detection system for the security subsystem in tactical command-level wireless sensor networks.

Keywords: *wireless sensor networks, intrusion detection, security management, tactical control link, artificial neural networks, signature analysis, cryptographic methods, anomaly detection.*

Постановка завдання. Безпроводові сенсорні мережі (*Wireless Sensor Networks*) є різновидом розподілених мереж, що складаються з вузлів (сенсорів), з інтегрованими функціями моніторингу параметрів навколишнього середовища, обробки і передачі даних.

У безпроводових сенсорних мережах (БСМ) тактичної ланки управління військами існують специфічні вразливості, а саме:

− необхідність компромісного використання бездротових каналів зв'язку (дає змогу зловмиснику створювати активні та пасивні завади, здійснювати перехоплення й аналіз мережевого трафіку, спотворювати або знищувати пакети на найбільш завантажених каналах);

− відсутність фізичного контролю сенсорів (дає змогу зловмиснику отримати фізичний доступ до компонентів БСМ завдяки чому є змога підміни, захоплення або знищення вузлів).

− динамічні умови побудови топології, децентралізованого управління та процесів масштабування (ускладнюють процедуру сертифікації, реалізацію систем виявлення вторгнень, тощо);

− обмеженість ресурсів вузлів (ускладнюють реалізацію надійних механізмів безпеки та впровадження стійких криптографічних алгоритмів).

Наявність зазначених особливостей створює низку передумов для реалізації фізичних і кібернетичних атак на БСМ та висуває вимоги до розроблення ефективних підходів виявлення вторгнень, з урахуванням особливостей динаміки середовища функціонування мереж такого типу.

Вторгнення – це несанкціонований доступ до інформації, зміна інформації, скидання частини пакетів і перенаправлення на наступні вузли мережі. Захист від зовнішніх атак містить застосування криптографічних методів: шифрування інформації, використання цифрового підпису та ін. Водночас, криптографічні методи не мають змоги забезпечити захист від впливу противника за наявності скомпрометованих або захоплених вузлів. Для захисту від внутрішніх атак передбачається використання моделей та методів виявлення вторгнень у безпроводових сенсорних мережах [1].

Аналіз останніх досліджень і публікацій. У роботі [2] проведено дослідження енергоефективних методів виявлення вторгнень у БСМ, проведено їх класифікації та розглянуто різні підходи до управління безпекою мережі. Проте автори не проводять аналіз типів атак та на яких рівнях моделі Open Systems Interconnection (OSI) функціонують такі методи. Водночас у статті [3] проведено аналіз вразливостей, основних і додаткових вимог з безпеки БСМ та запропоновано класифікацію атак (характер дій, рівень моделі відкритих систем, мета впливу, об'єкт управління, позиціонування відносно мережі, тип атакуючого пристрою). Запропоновано класифікацію та проведено аналіз існуючих атак у безпроводових сенсорних мережах тактичної ланки управління військами, що дає змогу досліджувати моделі та методи виявлення вторгнень.

У роботах [4, 5, 6] проведено аналіз методів і моделей виявлення вторгнень для БСМ за останнє десятиліття, проте не враховано інтеграцію штучних нейронних мереж в галузі. Слід зазначити, що у [7] автори аналізують сучасні підходи, що ґрунтуються на штучних імунних системах, штучних нейронних мережах та генетичних алгоритмах стосовно виявлення атак певних типів, а саме: відмови в обслуговуванні, витоки інформації та аномалії мережі. Водночас інші атаки, зокрема на БСМ тактичної ланки управління військами не розглядаються.

Метою роботи є проведення порівняльного аналізу моделей та методів виявлення вторгнень у безпроводових сенсорних мережах тактичної ланки управління військами, їх основних переваг і недоліків для удосконалення підсистеми управління безпекою у таких мережах.

Виклад основного матеріалу дослідження. Виявлення вторгнень може здійснюватися в умовах централізованого або децентралізованого управління [2].

При централізованому управлінні всі дані з вузлів збираються та передаються до центрального вузла або базової станції (БС) для подальшої обробки та виявлення аномалій. Тобто всі сенсори виконують функції збору інформації, а процес аналізу, прийняття рішень та виявлення вторгнень здійснюється на рівні БС.

У децентралізованих моделях обробка даних і виявлення аномалій здійснюється на рівні сенсорних вузлів, що знижує навантаження на центральний вузол і зменшує кількість переданих даних. Кожен сенсорний вузол або група вузлів мають свої програмні засоби, які здійснюють локальне виявлення вторгнень і лише при виявленні атаки передають інформацію на вищий рівень до голови кластера (ГК) і БС.

Сьогодні існує декілька загальнодоступних еталонних наборів даних (DARPA, KDD, NSL-KDD та WSN-DS та інші), що використовуються для перевірки ефективності виявлення вторгнень. Також для якісного моделювання поведінки БСМ за звичайного сценарію та сценарію атаки дослідники створюють власний набір даних за допомогою мережевих симуляторів NS2, NS3, OMNeT, Cooja, TOSSIM тощо.

За функціональністю моделі та методи виявлення вторгнень класифікуються за такими групами: на основі сигнатур, на основі аномалій, на основі специфікації та гібридні [6].

Класифікація моделей та методи виявлення вторгнень для БСМ тактичної ланки управління військами з урахуванням методів машинного навчання та штучних нейронних мереж наведена на рисунку 1.

Рис. 1**.** Класифікація моделей та методів виявлення вторгнень для БСМ тактичної ланки управління військами

Моделі та методи виявлення вторгнень на основі сигнатур реалізуються шляхом порівняння моніторингових даних із базою даних сигнатур відомих загроз. Сигнатури можуть містити специфічні шаблони, що відображають відомі методи атак або зловмисну поведінку (шкідливі пакети даних або небезпечні послідовності команд).

Модель системи виявлення вторгнень (СВВ), що використовує набір еволюційно виведених правил для виявлення вторгнень у БСМ запропонована у роботі [8] на основі генетичного мережевого програмування (ГМП). Цей метод використовується для генерації правил виявлення вторгнень та контролю кількості цих правил та дає змогу удосконалювати правила, адаптуючись до змін у мережевій поведінці та нових типів атак. Правила вибираються на основі їх підтримки, достовірності та важливості (виміряної за допомогою статистики χ^2).

Тільки ті правила, які задовольняють певні порогові значення, вважаються важливими та зберігаються в наборі правил.

Для оцінювання та відбору правил автори використовують модифіковану відстань Жаккара, щоб виміряти схожість між правилами та між наборами правил. Мета запропонованого підходу полягає в тому, щоб мінімізувати відстань між правилами в одному наборі (зменшити редундантність) і максимізувати відстань між правилами в різних наборах (підвищити розрізнювальну здатність між нормальною поведінкою та вторгненнями).

Переваги: висока точність виявлення вторгнень шляхом точного налаштування параметрів системи, адаптивність до нових типів атак, можливість постійно оновлювати і вдосконалювати набір правил виявлення.

Недоліки: складність реалізації та налаштування, збільшені обчислювальні витрати, залежність ефективності роботи правил від повноти та точності вхідних даних.

Опис децентралізованої моделі СВВ для БСМ, що використовує фільтри Блума (ФБ) для зменшення розміру коду сигнатури атаки за допомогою хеш-функцій наведений у [9]. Створені сигнатури атак проходять через хеш-функції та поділяються за розміром на дві категорії, а потім відмічаються у відповідних масивах ФБ. Сигнатури розміром до 33 байт обробляються на мережевому рівні, а більші – на прикладному рівні. При передачі пакетів через мережу на кожному вузлі відбувається перевірка та порівняння з існуючими сигнатурами атак у масивах ФБ.

Переваги: енергоефективність, швидке виявлення атаки та оперативне реагування на потенційні загрози, гнучкість і адаптивність налаштування.

Недоліки: потреба в детальному налаштуванні та управлінні, ризик хибних спрацьовувань, проблеми з динамічним оновленням і видаленням сигнатур.

Для виявлення атак типу "вибіркової передачі" та "чорної діри" запропоновано метод на основі правил для побудови СВВ БСМ. Сигнатури атак зберігаються в БС з метою зниження енергоспоживання на сенсорних вузлах [10].

Принцип виявлення вторгнень базується на використанні контрольних пакетів (КП), які відправляються від ГК до БС на початку кожного сеансу зв'язку. Контрольний пакет містить інформацію про ГК та ідентифікатори вузлів-членів кластера. Для виявлення атак використовуються такі правила:

Затримки. *ЯКЩО* з вузла не надходять *КП* до БС до встановленого часу*, ТО* атака – "чорна діра".

Підмножини ідентифікаторів. *ЯКЩО* в КП відсутні ідентифікатори деяких членів кластеру*, ТО* атака – "вибіркова передача".

Переваги: простота управління та налаштування політики безпеки, мінімізація енергоспоживання сенсорних вузлів, висока швидкість реагування на інциденти БС.

Недоліки: високі вимоги до ресурсів БС та підвищенні ризики безпеки або компрометації БС, складність масштабованості.

Ієрархічна модель для виявлення аномальних вузлів у БСМ, що базується на використанні нечіткої логіки та правил "подія-умова-дія" була запропонована у [11]. Зазначена модель передбачає багаторівневу структуру, яка включає локальне виявлення на рівні вузлів кластера (ВК), групове виявлення на рівні кластерних агрегаторів (КА) та кластерне виявлення на рівні ГК.

Кожен ВК збирає дані про середовище та виконує локальний процес виявлення аномалій за допомогою нечіткої логіки. Для аналізу використовуються тимчасові семантичні кореляції. Кожен ВК зберігає короткострокову історію зібраних даних, які використовуються для побудови моделі ковзного вікна часу.

КА збирає локальні рішення від своїх сенсорних вузлів та використовує просторові багатовимірні кореляції для прийняття більш точного групового рішення.

ГК збирає групові рішення від ВК та використовує як просторово-часові атрибути (ПЧА) так і багатовимірні атрибути (БВА) кореляції для прийняття остаточного рішення щодо наявності аномальних вузлів.

Переваги: енергоефективність, зниження навантаження на центральний вузол через багаторівневу структуру СВВ, висока точність виявлення аномальних вузлів та зниження кількості хибних спрацьовувань.

Недоліки: складність налаштування та обслуговування, залежність від точності налаштувань правил та якості вхідних даних надісланих сенсорам, проблеми з динамічним оновленням і видаленням сигнатур.

У таблиці 1 наведено порівняльний аналіз методів і моделей виявлення вторгнень на основі сигнатур.

Таблиця 1

Методи та моделі виявлення вторгнень на основі сигнатур

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Nannan et al. [8]	Централізований	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Визначення топології/Homing Відмова в обслуговуванні/DoS	ГМП, відстань Жаккара	NSL-KDD	Канальний Мережевий Транспортний Прикладний
Cho et al. [9]	Децентралізований	Відмова в обслуговуванні/DoS	фільтри Блума	NS2	Прикладний
Hidoussi et al. [10]	Централізований	Чорна діра /Black Hole Вибіркова передача/Selective Forwarding	Правила затримки та підмножини ідентифікаторів	NS2	Мережевий
Berjab et al. [11]	Децентралізований	Відмова в обслуговуванні/DoS Десинхронізації/ Desynchronization	ПЧА БВА	NSL-KDD	Прикладний

Моделі та методи на основі сигнатур є надійним і точним інструментом для захисту від відомих атак, але їх ефективність залежить від актуальності бази сигнатур. Дані методи менш ефективні для боротьби з новими або складними атаками. Тому для підвищення ефективності виявлення потрібно їх використовувати в поєднанні з іншими методами, такими як евристичні або поведінкові аналізи.

Моделі та методи виявлення вторгнень на основі аномалій реалізуються шляхом порівняння поточних дій і станів мережі з моделлю нормальної поведінки для виявлення відхилень, що можуть свідчити про можливе вторгнення або іншу аномалію. Зазначені моделі та методи класифікуються залежно від їх функціональних можливостей: на основі статистики, на основі інтелектуального аналізу даних, на основі машинного навчання та на основі штучного інтелекту.

Процес виявлення вторгнень починається зі збору даних з сенсорних вузлів, зокрема датчиків температури, вологості, тиску, рівня вібрацій, трафіку та енергоспоживання. Зібрані дані очищуються і нормалізуються для видалення шуму та заповнення пропущених значень. На основі оброблених даних створюється модель нормальної поведінки вузла. Поточні дані постійно порівнюються з цією моделлю для виявлення значних відхилень, що можуть свідчити про аномалії.

Методи та моделі виявлення на основі статистики спрямовані на виявлення вторгнень через аналіз статистичних відхилень у поведінці БСМ. Ці методи базуються на зборі великих

обсягів даних про нормальну функціонування діяльність системи, після чого створюються математичні моделі, що відображають її стандартні характеристики, такі як середнє значення, стандартне відхилення, дисперсія та інші статистичних моделей (логістична регресія, авторегресія). Під час моніторингу поточної активності системи виявляються значні відхилення від цих характеристик, що вказують на можливі аномалії та потенційні загрози.

Так у [12] запропоновано модель СВВ для БСМ, що використовує статистичний інструмент бінарної логістичної регресії (БЛР) для аналізу зібраних даних з вузлів (кількість отриманих та відправлених пакетів даних, кількість перенаправлених та втрачених пакетів).

На основі результатів аналізу БЛР система класифікує активність сенсора зловмисною якщо ймовірність зловмисної активності перевищує певний поріг.

Переваги: енергоефективність, можливість виявлення нових типів атак та висока точність виявлення відомих атак, можливість адаптації та змін налаштування для конкретних потреб і специфікацій мережі.

Недоліки: залежить від якості та репрезентативності тренувальних даних, складність визначення оптимальних порогів для класифікації, неспроможність виявляти атаки, що імітують нормальну поведінку мережі.

Статистичний метод виявлення атак "створення завад" в БСМ з використанням техніки контролю статистичного процесу на основі моделі експоненційно зваженого ковзного середнього (Exponentially Weighted Moving Average, EWMA) запропоновано у [13].

Основною ідеєю є використання моделі EWMA для моніторингу значення часу між прибуттями пакетів і виявлення випадків, коли його середнє значення відхиляється від норми, що може вказувати на створення завад зловмисником.

Визначення EWMA в момент часу *t* здійснюється за виразом [13]:

$$z(t) = \lambda \cdot x(t) + (1 - \lambda) \cdot z(t - 1),$$

де $x(t)$ – спостережуване значення в момент часу *t*; λ – коефіцієнт згладжування, який визначає вагу останніх спостережень відносно попередніх.

Переваги: енергоефективність, легкість імплементації та інтеграції в існуючі СВВ, швидкість виявлення аномалій.

Недоліки: низька ефективність у мережах з високою змінністю трафіку або в мережах, що характеризуються частими змінами топології, слабка адаптивність до складних та поліморфних атак, можливість виявлення тільки атак пов'язаних із створенням завад.

Модель СВВ для БСМ, що використовує теорію ігор та авторегресивну модель (АРМ) для ефективного передбачення атак і мінімізації споживання енергії запропоновано [14]. Система моделює взаємодію між атакуючими та СВВ як гру з двома гравцями, де кожен учасник намагається максимізувати свою вигоду: атакуючий – успішно виконати атаку, а СВВ – ефективно запобігти атаці. Модель ураховує можливі стратегії обох сторін та використовує концепцію змішаної рівноваги Неша для визначення оптимальних стратегій захисту. Такий підхід дозволяє системі адаптуватися до різних стратегій атак і вибирати найефективнішу стратегію оборони з урахуванням енерговитрат.

Система використовує АРМ для аналізу історичних даних про атаки і передбачення часу та цілей наступних атак. АРМ дає змогу ідентифікувати закономірності в поведінці атакуючих, базуючись на попередніх атаках і передбачати майбутні атаки.

Авторегресивна модель порядку p (кількість попередніх значень, що використовуються для передбачення поточного значення) формалізується за виразом [14]:

$$X_t = \phi_1 X_{t-1} + \phi_2 X_{t-2} + \cdots + \phi_p X_{t-p} + \varepsilon_t,$$

де X_t – поточне значення часового ряду в час *t*; $\phi_1, \phi_2, \ldots, \phi_p$ – параметри моделі, які визначають вплив попередніх значень на поточне значення; ε_t – термін шуму або помилки

в час t (серія некорельованих випадкових змінних з нульовим середнім і постійною дисперсією).

Переваги: висока ефективність виявлення вторгнень, енергоефективність, можливість адаптуватися до нових або еволюційних загроз.

Недоліки: складність реалізації та інтеграції моделі, залежність від вибору та налаштування параметрів, залежність від якості та обсягу попередньо отриманих даних, потреба в постійному оновленні.

Для виявлення атаки типу "воронки" у БСМ використовується геостатистична модель розподіленого моніторингу (ГМРМ) [15]. Принцип виявлення вторгнень полягає в тому, що вузли навколо воронки втрачають енергію швидше, ніж інші вузли, оскільки маршрути через атакуючий вузол використовуються частіше. Це призводить до формування "енергетичної кризи" навколо атакуючого вузла. Використання ГМРМ дає змогу БС оцінити ризик атаки в кожному кластері на основі змін у залишковій енергії та інших метрик, що містять геолокаційні дані вузлів.

Швидкість відмови для вузла j в регіоні i у час описується формулою

$$z(t_{ij};\ x_{ij}) = z_0 \exp(-\beta x_{ij} + W_i),$$

де t_{ij}; x_{ij} – вектор асоційованих коваріат (наприклад, залишкова енергія); W_i – термін, що відображає варіабельність між регіонами (фрагільність регіону); z_0 – початковий рівень безпеки.

Переваги: висока точність ідентифікації атак "воронки", гнучкість налаштування та масштабованість, швидкість реагування на вторгнення.

Недоліки: складність налаштування та оновлення, залежність від якості та обсягу попередньо отриманих даних, високі вимоги до обчислювальних ресурсів.

Узагальнена стохастична мережа Петрі (Generalized Stochastic Petri Nets, GSPN) використовується для визначення позиції розгортання спеціальних вузлів-інспекторів (BI), що аналізують трафік у кластері та надсилають попередження до ГК у разі виявлення аномальної поведінки [16].

Модель використовує статичний і динамічний підходи до розміщення BI. При статичному підході BI розміщуються на стратегічних позиціях у топології мережі, а при динамічному – BI періодично обираються серед звичайних вузлів кожного атомарного кластера.

Переваги: гнучкість налаштування, адаптивність, масштабованість, швидкість виявлення аномалій у поведінці вузлів.

Недоліки: підвищена складність управління та координація динамічного вибору BI, менша ефективність проти нових або модифікованих атак, великі енергозатрати BI.

У таблиці 2 наведено порівняльний аналіз методів та моделей виявлення вторгнень на основі статистики.

Таблиця 2

Методи та моделі виявлення вторгнень на основі статистики

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Ioannou et al. [12]	Децентралізований	Чорна діра /Black Hole Вибіркова передача/Selective Forwarding	БЛР	Cooja	Мережевий
Osanaiye et al. [13]	Децентралізований	Створення завад/Jamming	EWMA	CRAWDA	Фізичний
Han et al. [14]	Централізований	Шкідливе ПЗ/Malware	APM	MAT Lab	Прикладний
Shafiei et al. [15]	Децентралізований	Воронка/Sinkhole	ГМРМ	OMNeT++	Мережевий
Ballarini et al. [16]	Децентралізований	Відмова в обслуговуванні/DoS	GSPN	NS2	Прикладний

Моделі та методи виявлення вторгнень на основі статистики в якості переваги мають можливості моніторингу та аналізу мережевого трафіку з великою адаптивністю та

масштабованістю. В якості недоліка можливе використання зловмисних вузлів з метою перенавчання статистичних алгоритмів для неправильного визначення їх нормальної поведінки.

Методи та моделі виявлення вторгнень на основі інтелектуального аналізу даних (Data Mining) використовують алгоритми обробки даних такі як кластеризація, класифікація, асоціація, аналіз послідовностей і прогнозування, які ефективно виявляють приховані патерни та аномалії при великих обсягах зібраної інформації з сенсорних вузлів.

Модель СВВ для ідентифікації атаки "чорної діри" на основі аналізу поведінки вузлів мережі з метою ідентифікації їх аномальної поведінки запропоновано у [17]. Виявлення вторгнень базується на обробці даних за допомогою алгоритму кластеризації K-means та алгоритму класифікації J-48 для побудови дерева рішень. Спочатку набір даних з нормальною поведінкою вузлів піддається кластеризації та визначаються вузли з подібними поведінковими (функціональними) характеристиками. Наступним кроком є застосування алгоритму J-48 для побудови дерева рішень, яке допомагає класифікувати вузли на нормальні або зловмисні залежно від їх поведінки. Вибір атрибуту в J-48 (зиск інформації) проводиться за виразом [17]:

$$IG(S,A) = H(S) - \sum_{t\epsilon T} \frac{|S_t|}{|S|} H(S_t),$$

де $IG(S,A)$ – зиск інформації від атрибута A для множини S; $H(S)$ – ентропія множини S; T – множина всіх можливих значень атрибута A; S_t – підмножина S для якої атрибут A має значення t.

Переваги: висока точність ідентифікації атаки "чорної діри" та можливість їх раннього виявлення, адаптація до нових загроз завдяки можливості перенавчання моделі.

Недоліки: потреба значних обчислювальних ресурсів, залежність точності виявлення від вибору параметрів, потреба в затратах часу на навчання та оптимізацію.

Модель виявлення аномалій на основі кластеризації K-медоїдів для ідентифікації атаки "чорної діри" та атаки "вибіркової передачі" у БСМ розроблена у [18]. Вона працює за принципом моніторингу та аналізу мережевих параметрів вузлів. Використовуючи алгоритм K-медоїдів, вузли з подібними характеристиками групуються в кластери та обирається медоїд у кластері завдяки мінімізації суми попарних відстаней між точками в кластері.

Для кожного кластера обчислюються порогові значення для різних параметрів (наприклад, обсяг трафіку або затримка пакетів) та у разі перевищення порогу визначається аномальну поведінка вузла.

Переваги: висока точність та швидкість виявлення атак "вибіркової передачі" та "чорної діри", простота реалізації та стійкість до шуму.

Недоліки: обмежена масштабованість, залежність ефективності виявлення від початкового вибору медоїдів та налаштувань порогових значень.

Для виявлення атак "воронки" та "виснаження" запропоновано модель СВВ, що забезпечує дворівневе виявлення вторгнень, де локальні агенти швидко виявляють аномалії, а центральний агент проводить глибший аналіз для підтвердження вторгнень [19]. Локальний агент встановлюється в кожному вузлі та виконують менш складні функції виявлення аномалій. Вони збирають дані моніторингу та інформацію про маршрути. Центральний агент, що встановлюється на БС, аналізує отримані дані від локальних агентів та виконує їх класифікацію алгоритмом дерева рішень.

Переваги: ефективність проти відомих та нових атак, висока швидкість реагування та точність виявлення, зменшена кількість помилкових спрацювань, можливість збалансувати навантаження на обчислювальні та енергетичні ресурси вузлів мережі.

Недоліки: складність налаштування, залежність від якості набору даних, потенційна вразливість БС до DoS атак, потенційна проблема масштабування.

Для виявлення атаки "затоплення" використовується алгоритм класифікації K-найближчих сусідів (K-Nearest Neighbor, KNN), що реалізується моделлю СВВ, архітектура якої складається з модуля бездротового мережевого інтерфейсу, модуля зберігання даних, модуля аналізу та судження, а також модуля реагування на вторгнення [20].

Кожен вузол представляється як багатовимірний вектор ознак, що містить різні параметри поведінки вузла. Система визначає K-найближчих сусідів для кожного вузла та аналізує, до якої категорії (нормальні або аномальні) належить більшість цих сусідів. На основі аналізу відстані між вузлом та його найближчими сусідами визначається порогове значення, при перевищені якого СВВ класифікує вузол як аномальний і може вжити заходів щодо ізоляції вузла або сповіщення адміністратора мережі про вторгнення.

Переваги: адаптивність до змін у поведінці мережі, простота імплементації (реалізації та інтеграції) в БСМ, висока ефективність виявлення аномалій.

Недоліки: потреба зберігання великих обсягів даних в пам'яті вузла, залежність від вибору параметрів та незбалансованих даних, потреба в значних обчислювальних ресурсах.

У таблиці 3 наведено порівняльний аналіз методів і моделей виявлення вторгнень на основі інтелектуального аналізу даних.

Таблиця 3

Методи та моделі виявлення вторгнень на основі аналізу даних

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Kaur et al. [17]	Централізований	Чорна діра /Black Hole	K-means, J48	NS2	Мережевий
Ahmad et al. [18]	Централізований	Чорна діра /Black Hole Вибіркова передача/Selective Forwarding	K-медоїдів	NS2	Мережевий
Coppolino et al. [19]	Централізований	Воронка/Sinkhole Виснаження/Exhaustion	Дерево рішень	NS3	Канальний Мережевий
Li et al. [20]	Централізований	Затоплення/ Flooding	KNN	NSL-KDD	Транспортний

Моделі та методи виявлення вторгнень на основі інтелектуального аналізу даних, дозволяють ідентифікувати нові та складні атаки, здійснювати проактивний захист та можуть адаптуватися до змін у поведінці мережі. В якості недоліків можна зазначити велику обчислювальну складність та залежність від навчальних даних і вибору параметрів, які потрібно враховувати в процесі виявлення вторгнень.

Моделі та методи виявлення аномалій на основі машинного навчання орієнтовані на побудову моделей, які можуть генерувати точні прогнози або виявляти закономірності в наявних наборах даних. Їх головною метою є розробка алгоритмів і моделей, що здатні генерувати нові набори даних, прогнозувати або приймати рішення.

Модель СВВ, що ґрунтується на використанні архітектури з локальними агентами (ЛА) та центральним агентом (ЦА), доповнену застосуванням порогових метрик разом із деревами рішень для класифікації та виявлення атак типу "воронки" представлено у [21].

ЛА встановлюється на сенсорному вузлі та сповіщає ЦА про можливе вторгнення в мережу. ЛА спостерігає за певними характеристиками трафіку та інших змінних (кількість, частота та тип пакетів) мережі та визначає аномалії на основі порогових значень за допомогою методики експоненціального ковзного середнього (Exponential Moving Average, EMA).

Методика EMA використовується для згладжування даних та визначення напрямку їх зміни протягом певного часу. Значення EMA в момент часу *t* визначається за виразом;

$$EMA_t = \alpha \cdot M_t + (1 - \alpha) \cdot EMA_{t-1},$$

де M_t – поточне спостережуване значення параметра в момент t, EMA_{t-1} – значення ЕМА в попередній момент часу, $\alpha = \frac{2}{N+1}$ – коефіцієнт згладжування, N – кількість періодів.

ЦА діє як координатор між всіма ЛА і виконує більш складний аналіз отриманих сповіщень. За допомогою дерева рішень ЦА класифікує поведінку мережі як нормальну або аномальну, засновану на зібраних даних. Це дає змогу ідентифікувати більш складні атаки, які можуть не бути виявлені на рівні ЛА.

Переваги: здатність до самонавчання, високий рівень гнучкості та масштабованості системи, висока ефективність виявлення складних атак.

Недоліки: залежність ефективності від якості даних, потреба в обчислювальних ресурсах, ризик підвищення хибних спрацювань пов'язаних з перенавчання моделі.

Модель СВВ запропонована у [22] базується на комбінації кооперативної теорії ігор та нечіткого Q-навчання, що використовується для моделювання взаємодії між гравцями (атаковані вузли, БС, зловмисник). Кожен гравець обирає свою стратегію для досягнення максимальної вигоди. Для вузлів та БС стратегії спрямовані на виявлення та запобігання атакам, а для зловмисника – успішна реалізація атаки. Модель використовує спеціалізовані функції вигоди для моделювання наслідків різних комбінацій стратегій.

Для оптимізації процесу прийняття рішень використовується нечітке Q-навчання, що дає змогу адаптуватися до змін у середовищі мережі та ефективно вибирати стратегії для максимізації вигоди [22]:

$$Q(s,a) \leftarrow Q(s,a) + a[r + \gamma \max_{a'} Q(s',a') - Q(s,a)],$$

де a – дія або швидкість навчання; a' – наступна можлива дія $Q(s,a)$ – значення Q-функції для стану s та дії; r – винагорода за дію a у стані s; γ – коефіцієнт дисконтування, що відображає важливість майбутніх винагород; s' – наступний стан після виконання дії a.

Переваги: адаптивність, висока точність та ефективність виявлення, ефективне використання ресурсів, можливість виявлення потенційних загроз (проактивне виявлення).

Недоліки: складність реалізації та налаштування, потенційна складність масштабування, потреба зберігання великої кількості даних про попередні взаємодії та вибори стратегій.

Метод виявлення вторгнень на основі глибокого навчання з використанням архітектури багатошарового автоматичного кодера (Stacked Denoising Autoencoder, SDA) дає змогу ідентифікувати атаки, аналізуючи та класифікуючи характеристики місцеположення разом із топологічними індексами [23].

Різниця потужності сигналу (RSSI) між неатакованими та атакованими вузлами визначається за виразом:

$$RSSIDIFF_{ij} = RSSI_{N,ij} - RSSI_{A,ij},$$

де $RSSI_{N,ij}$ та $RSSI_{A,ij}$ – потужність сигналу між вузлом-маяком i та невідомим вузлом j в неатакованих та атакованих сценаріях відповідно.

Архітектура SDA використовується для здобуття корисних характеристик із сировинних даних через послідовні шари автоенкодерів, що призначені для відновлення вхідного сигналу на виході.

Переваги: висока точність класифікації та виявлення складних атак, зменшене навантаження на вузли, здатність до самонавчання.

Недоліки: необхідність великої кількості даних та витрати певного часу для навчання, залежність від якості даних, потреба в значних обчислювальних ресурсах.

Для виявлення атак "чорної діри "та "затоплення", запропоновано метод, що поєднує алгоритм нечіткої кластеризації c-means, однокласового методу опорних векторів (Support Vector Machine, SVM) і процедури ковзного вікна [24].

Алгоритм нечіткої кластеризації c-means використовується для розділення даних моніторингу на кластери, що представляють нормальні та аномальні стани сенсорних даних. Мета такого алгоритму визначити центри кластерів та призначити кожному виміру даних ступінь приналежності до кожного кластера. Алгоритм мінімізує цільову функцію:

$$J(U,V) = \sum_{i=1}^{n}\sum_{j=1}^{c} u_{ij}^{m}||x_i - v_j||^2,$$

де n – кількість точок даних, c – кількість кластерів, u_{ij} – ступінь приналежності i-ої точки до j-го кластера, m – параметр, що визначає рівень нечіткості кластеризації, x_i – i-та точка даних, v_j – центр j-го кластера.

Однокласова SVM використовується для ідентифікації нових даних, що відхиляються від нормального шаблону поведінки, який був навчений моделлю. Це досягається максимізацією відстані між даними та походженням у просторі ознак, трансформованому завдяки ядра. Рішення моделі може бути представлене так:

$$f(x) = sign(\sum_{i=1}^{n} a_i K(x_i, x) - \rho),$$

де $K(x_i, x)$ – функція ядра між i-тим навчальним вектором і вектором, що тестується x, a_i –коефіцієнти, що визначаються під час навчання моделі, ρ – відступ від походження.

Процедура ковзного вікна використовується для аналізу часових залежностей між послідовними точками даних, щоб додатково оцінити підозрілий зразок даних.

Переваги: висока ефективність і точність розпізнавання аномалій, адаптивність і легкість впровадження, енергоефективність.

Недоліки: складність налаштування параметрів, висока залежність ефективності виявлення від вибірки даних, потреба у великих обсягах даних для регулярного оновлення моделі.

Модель СВВ на основі алгоритму SMOTE (Synthetic Minority Over-sampling Technique) , який проводить балансування набору даних KDDCup'99 шляхом створення синтетичних прикладів міноритарного класу (тобто класу, який має менше представництво у наборі даних) запропоновано в [25]. Для кожного зразка міноритарного класу визначається кількість його найближчих сусідів k, а потім вибирається один з цих сусідів і створюється новий синтетичний зразок шляхом інтерполяції між розглянутим зразком та вибраним сусідом. Після балансування датасету за допомогою SMOTE використовується алгоритм випадкового лісу для класифікації зразків.

Переваги: масштабованість та висока швидкість обробки даних при великій кількісті вузлів, здатність моделі точно класифікувати рідкісні типи атак, малий ризик перенавчання.

Недоліки: великі енергозатрати через складність обчислень потреба у великих обсягах даних для регулярного оновлення моделі, залежність від налаштування параметрів.

У таблиці 4 наведено порівняльний аналіз методів і моделей виявлення вторгнень на основі машинного навчання.

Таблиця 4

Методи та моделі виявлення вторгнень на машинного навчання

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Garofalo et al. [21]	Децентралізований	Воронка/Sinkhole	EMA	NS3	Мережевий
Shamshirband et al. [22]	Децентралізований	Відмова в обслуговуванні/DoS	нечітке Q-навчання	NS2, WSN-DS	Прикладний

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Wang et al. [23]	Централізований	Сивілли/Sybil Нерівномірність доступу/Unfairness Тунелювання/Wormhole Колізії/Collision	SDA	NS2	Канальний Мережевий
Qu et al. [24]	Централізований	Чорна діра/Black Hole Затоплення/Flooding	c-means SVM	OMNeT++	Мережевий Транспортний
Tan et al. [25]	Централізований	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Відмова в обслуговуванні/DoS	SMOTE Випадковий ліс	KDD Cup'99	Прикладний Мережевий Транспортний

Методи та моделі на основі машинного навчання дають змогу виявляти відомі та невідомі атаки за допомогою аналізу великих обсягів даних та ідентифікації аномалій у поведінці мережі. Перевагами методів є адаптивність, висока точність та можливість роботи в реальному часі. Як недолік слід зазначити наявність чутливості до шуму, складність обчислення та необхідність специфічного налаштування особливо в умовах обмежених ресурсів.

Для виявлення атак у реальному часі для зменшеним втручання людини використовують **методи виявлення вторгнень на основі штучних нейронних мереж**, що імітують алгоритми роботи людського мозку, використовуючи нейрони та їх взаємозв'язки.

Модель СВВ, що використовує метаевристичні алгоритми вовчої зграї та еволюційних систем для оптимізації нейронної мережі досліджено в [26]. Алгоритм вовчої зграї оптимізує ваги і параметри нейронної мережі для підвищення точності та ефективності виявлення аномалій. Він моделює соціальну структуру і полювання сірих вовків, використовуючи лідерів (альфа, бета, дельта) для керівництва пошуком оптимальних рішень в просторі рішень. Алгоритм еволюційних систем використовується для покращення процесу виявлення аномалій шляхом адаптації нейронної мережі до змін у даних і умовах роботи мережі. Він використовує принципи еволюції для ефективного пошуку в просторі параметрів, адаптуючи і вдосконалюючи модель нейронної мережі.

Визначення відстані D між вовком (поточним рішенням) та здобиччю (оптимальним рішенням) здійснюється за виразом:

$$D = |C \cdot X_p(t) - X(t)|,$$

де $X_p(t)$ – позиція здобичі (оптимального рішення) на ітерації t, $X(t)$ – позиція вовка, C – коефіцієнт, що визначає вплив здобичі на рух вовка.

Переваги: висока точність виявлення аномалій та потенційних атак, адаптивність до змін у поведінці мережі, масштабованість, ефективність у режимі реального часу завдяки швидкому навчанню нейронної мережі.

Недоліки: значні вимоги до обчислювальних ресурсів, складність налаштування, залежність ефективності виявлення та ризик перенавчання від якості та актуальності даних.

Модель СВВ у БСМ на основі ройового інтелекту (Swarm Intelligence for Wireless sensor networks Cybersecurity, SIWC), містить три основні рівні: сенсорів, безпеки та прийняття рішень [27].

Рівень сенсорів (Sensor Layer) складається з різних вузлів (датчиків), що періодично вимірюють набір критичних параметрів (кількість колізій, швидкість передачі пакетів тощо) у своєму радіусі дії та відповідають за збір та передачу даних до рівня безпеки.

Рівень безпеки (Security Layer) складається з вузлів-захисників, що відповідають за виявлення аномальних поведінок безпеки та атак у кластері. Кожен вузол-захисник є ГК і використовує метод оцінювання максимальної правдоподібності для визначення рівня безпеки свого кластера. Цей метод тренується за допомогою алгоритму ройового інтелекту для пошуку найкращих значень, що підвищують ймовірність виявлення атак.

Найвищий рівень прийняття рішень (Decision Layer) розгортається на рівні БС мережі, яка отримує повідомлення про загрози від ГК та вживає відповідних заходів, таких як пом'якшення атаки або вимкнення атакованого вузла.

Переваги: адаптивність до нових видів атак, висока швидкість виявлення та реагування на вторгнення, масштабованість, мала потреба в обчислювальних ресурсах.

Недоліки: складність налаштування, потреба в регулярних оновленнях та підтримці, залежність точності від параметрів та якості набору даних.

Для виявлення атаки "чорної діри" модель СВВ поєднує алгоритм мурашиних колоній (Ant Colony Optimization, ACO) та алгоритм рою частинок (Particle Swarm Optimization, PSO) [28]. Кожна частинка розміщуються в пошуковому просторі та має вектори положення та швидкості. Вона оцінює своє поточне положення за допомогою функції пристосування, що визначає, наскільки добре дане положення задовольняє критерії виявлення атак. Це може містити аналіз шаблонів трафіку, часових інтервалів між пакетами та інших властивостей даних.

Кожна частинка запам'ятовує найкраще знайдене нею положення та визначає найкраще положення серед усіх частинок у рої. Положення частинки i в час t+1 оновлюється на основі її нової швидкості $v_i^{(t+1)}$:

$$x_i^{(t+1)} = x_i^{(t)} + v_i^{(t+1)},$$

де $x_i^{(t)}$ – положення частинки i в час t.

Частинки, які консистентно показують високі значення функції пристосування в потенційно аномальних областях, можуть вказувати на наявність вторгнення.

Переваги: висока точність виявлення атаки "чорної діри", масштабованість, адаптивність.

Недоліки: складність реалізації через необхідність інтеграції хеш-таблиць та управління роєм частинок, залежність від параметрів та якості набору даних, потреба в обчислювальних ресурсах.

Модель СВВ, що реалізується на синтезі алгоритмів adaboost, зграї (косяка) риб та культурного обміну для свого навчання використовує набір даних NSL-KDD [29]. Алгоритм adaboost інтегрує багато слабких класифікаторів у сильний, стабільний та адаптивний класифікатор. Ієрархічна структура допомагає відсіювати більшість нормальних даних на перших рівнях, залишаючи для подальшого аналізу лише потенційно аномальні дані.

Для виявлення зловживань використовується нейронна мережа зворотного поширення помилок, оптимізована за допомогою алгоритму культурного обміну та зграї (косяка) риб. Вихідний сигнал нейронної мережі для k-го нейрону вихідного шару, обчислюється за виразом:

$$O_k = f(\sum_{j=1}^{l} H_j w_{jk} - b_k),$$

де H_j – вихідний сигнал j-го нейрона прихованого шару, w_{jk} – вага між j-м нейроном прихованого шару та k -м нейроном вихідного шару.

Переваги: висока адаптивність та масштабованість, зниження навантаження на обчислювальні та енергетичні ресурси вузлів, комплексність і точність системи.

Недоліки: складність налаштування та інтеграції, затрати часу на тренування та оптимізацію моделі, залежність ефективності від якості набору даних.

Метод виявлення вторгнень запропонований у [30] базується на поєднанні алгоритму спектральної кластеризації та множини глибоких нейронних мереж. Спочатку застосовується алгоритм спектральної кластеризації для поділу набору даних на кластери на основі схожості даних. Потім кожен кластер обробляється окремою нейронною мережею із використанням декількох шарів автоенкодерів для попереднього навчання глибокої нейронної мережі. Після чого виконується дрібна настройка з учителем для кінцевого завдання класифікації, що дає змогу моделі вчитися на особливостях кожного кластера.

Переваги: висока ефективність, адаптивність до змін у поведінці мережевого трафіку, можливість виявлення нових типів атак, малі затрати часу на тренування і тестування моделі.

Недоліки: потреба у великому наборі даних для тренування, складність налаштування параметрів, потреба в значних обчислювальних ресурсах, велика залежність ефективності від якості кластеризації.

У таблиці 5 наведено порівняльний аналіз методів та моделей на основі штучних нейронних мереж.

Таблиця 5

Методи та моделі виявлення вторгнень на основі штучних нейронних мереж

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Mansouri et al. [26]	Централізований	Воронка/Sinkhole Відмова в обслуговуванні/DoS Сивілли/Sybil Визначення топології /Homing	алгоритми вовчої зграї та еволюційних систем	NS3	Канальний Мережевий Прикладний
Bitam et al. [27]	Децентралізований	Відмова в обслуговуванні/DoS Сивілли/Sybil Тунелювання/Wormhole Виснаження/Exhaustion	SIWC	NS3	Канальний Мережевий Прикладний
Nithiyanandam et al. [28]	Централізований	Воронка/Sinkhole	ACO, PSO	NS2	Мережевий
Sun et al. [29]	Децентралізований	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Відмова в обслуговуванні/DoS	алгоритми adaboost, зграї риб та культурного обміну	NSL-KDD	Канальний Мережевий Транспортний Прикладний
Ma et al. [30]	Централізований	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Визначення топології /Homing Відмова в обслуговуванні/DoS	спектральна кластеризація та множина глибоких нейронних мереж	NSL-KDD	Канальний Мережевий Транспортний Прикладний

Моделі та методи виявлення вторгнень на основі штучних нейронних мереж, мають високу точність, адаптивність та ефективність роботи у реальному часі при використанні метаевристичних алгоритмів вовчої зграї, ройового інтелекту і мурашиної колонії. Недоліками таких методів є складність налаштування, високі вимоги до ресурсів і ризик перенавчання.

Моделі та методу виявлення вторгнень на основі специфікацій використовують чітко визначені правила і моделі, що описують допустимі форми поведінки системи. Основу такого підходу є детальне розроблення специфікацій, що відображають всі етапи створення цих правил від мережевих протоколів до файлових операцій для моніторингу та аналізу системної активності. Під час роботи СВВ постійно перевіряє системні операції на відповідність встановленим специфікаціям, що дає змогу ідентифікувати аномалії, які свідчать про вторгнення [6].

Шляхом аналізу поведінки кожного вузла та порівнянні його з встановленими нормами модель СВВ використовує специфікацію на основі правил для виявлення аномалій у мережі [31].

Для цього використовується список аудиту (*A_List*), який містить інформацію про кількість відправлених, отриманих, переспрямованих та повторно відправлених пакетів для кожного вузла.

$$A\_List = \{Node\_ID, A\_snt, A\_rec, A\_fwd, A\_rtm\},$$

де *Node_ID* – ідентифікатор вузла, *A_snt* – кількість відправлених пакетів, *A_rec* – кількість отриманих пакетів, *A_fwd* – кількість переспрямованих пакетів, *A_rtm* – кількість повторно відправлених пакетів.

На основі цих даних формується список прапорців (*F_List*), що вказує на відхилення поведінки вузла від норми:

$$F\_List = \{Node\_ID, F\_snt, F\_rec, F\_fwd, F\_rtm\},$$

де *F_snt, F_rec, F_fwd, F_rtm* – прапорці, що можуть приймати одне з трьох значень: *N (miN)* – якщо значення менше мінімального порогу; *X* (*maX*) – якщо значення більше максимального порогу; *L* – якщо значення знаходиться в межах норми (*normaL*).

На основі *F_List* визначається рівень підозрілості вузла в списку *ML_List*:

$$ML\_List = \{Node\_ID, Maliciousness\_Level\},$$

де *Maliciousness_Level* – рівень підозрілості може бути одним з трьох значень: *Hig* (високий) – якщо кількість L менше або дорівнює двом; *Med* (середній) – якщо кількість L дорівнює трьом; *Low* (низький) – якщо поведінка вузла не відповідає жодному з вищезазначених критеріїв.

Переваги: висока точність виявлення вторгнень з низьким рівнем помилкових спрацювань, зниження навантаження на окремі вузли мережі.

Недоліки: потреба в постійному оновленні правил, збільшення службового трафіку між вузлами, вразливість до складних атак, складність виявлення нових типів атак, залежність від налаштування порогових значень та інших параметрів.

Гібридні моделі та методи виявлення вторгнень використовує переваги підходу, заснованого на сигнатурах, аномаліях і специфікаціях. Гібридний підхід підвищує точність до виявлення вторгнень, але збільшує складність реалізації [6].

Гібридний метод виявлення вторгнень, що полягає в комбінації різних методів виявлення на кожному з рівнів мережі запропоновано в [32].

На рівні вузлів використовується метод виявлення на основі специфікацій із встановленням певних правил для кожного типу атаки. На рівні ГК здійснюється виявлення аномалій на основі алгоритму бінарної класифікації SVM.

На рівні БС (високий рівень) використовує механізм голосування для прийняття остаточного рішення щодо підозрілих вузлів на основі звітів від ГК.

Переваги: ефективність та точність ідентифікації різних типів атак, можливість оптимізації обробки даних і розподілу навантаження, енергоефективність, адаптивність.

Недоліки: складність реалізації та налаштування, залежність ефективності від правильності налаштування параметрів, можливість затримки в реакції на атаки.

Модель гібридної СВВ, що складається з двох основних модулів запропоновано в [33]. Модуль виявлення зловживань порівнює поведінку мережі з відомими моделями атак використовуючи заздалегідь визначені сигнатури атак або патерни. Модуль виявлення аномалій використовує нейронну мережу зворотного поширення помилок (Back Propagation Network, BPN), що дає змогу системі класифікувати поведінку як нормальну чи аномальну на основі навчених вагових коефіцієнтів та взаємодій між нейронами у мережі.

Рішення про вторгнення приймається на основі результатів обох модулів. Якщо модуль виявлення аномалій фіксує атаку, але модуль виявлення зловживань не виявляє атаку, система

вважає, що атаки не було, і це розцінюється як помилкове спрацьовування модуля виявлення аномалій. Якщо обидва модулі виявляють атаку, система підтверджує факт вторгнення і визначає клас атаки на основі результатів роботи модуля виявлення зловживань.

Переваги: висока точність виявлення, енергоефективність, адаптивність, можливість ідентифікації відомих та невідомих атак.

Недоліки: складність реалізації та налаштування, залежність ефективності виявлення від правильності налаштування параметрів, можливість затримки в реакції на атаки.

Багаторівневою гібридною модель СВВ, що використовує правила специфікації та нейронні мережі для ідентифікації зловмисних вузлів запропоновано в [34]. Система здійснює моніторинг на трьох рівнях: рівні вузла, ГК та БС.

На найнижчому рівні вузлів розміщено агентів СВВ, які здійснюють моніторинг діяльність сенсорів в кластері за допомогою набору специфікацій та правил. Ці правила базуються на таких параметрах, як частота отримання пакетів, частота пересилання пакетів, дублювання пакетів та індикатор сили сигналу. Взаємодія між СВВ і вузлом відбувається на основі теорії ігор з двома учасниками. СВВ адаптує свої стратегії моніторингу на основі Байєсівського рівноважного стану Неша (Bayesian Nash Equilibrium, BNE), що дає змогу мінімізувати обсяг введеного в мережу трафіку СВВ.

Гра визначається як $G = \{N, S, U\}$, де $N = \{P_i, P_j\}$ є множиною гравців, де P_i є потенційно зловмисним вузлом, а P_j – захисником (СВВ); $S = S_i \cdot S_j$ представляє простір стратегій гри, з S_i і S_j як просторами стратегій для P_i, і P_j відповідно; $U = U_i \cdot U_j$ – визначає простір виграшів, з $U_i \cdot$ і U_j як виграшами для P_i, і P_j.

На середньому рівні ГК виконують моніторинг інших ГК завдяки комбінації правил специфікації та легкої нейронної мережі, що дає змогу класифікувати дії інших ГК як нормальні або аномальні.

На найвищому рівні БС збирає інформацію від кількох ГК для виявлення зловмисних ГК. Якщо ГК виявляється зловмисним, він видаляється з мережі, а на його місце обирається новий ГК.

Переваги: висока точність і швидкість виявлення енергоефективність, масштабованість, адаптивність, мінімізація службового трафіку

Недоліки: складність розгортання та налаштування системи, залежність ефективність від точності встановлених параметрів складність управління та обслуговування

Гібридну модель СВВ поєднує підсистему виявлення на основі сигнатур та підсистему виявлення аномалій [35].

Підсистема виявлення на основі сигнатур призначена для ідентифікації відомих інтрузивних поведінок за допомогою сигнатур або визначених ознак цих поведінок. Алгоритм випадкового лісу генерує багато дерев рішень на основі підмножини навчальних даних та ознак, а потім використовує голосування більшості для прийняття рішення.

Підсистема виявлення аномалій базується на алгоритмі кластеризації E-DBSCAN (Enhanced Density-Based Spatial Clustering of Applications with Noise), що групує дані на основі їх щільності, ідентифікуючи області високої щільності, які відокремлені областями низької щільності. Важливим аспектом є використання ієрархічної та довіреної агрегації даних, що передбачає оцінку довіри між ГК та відповідними вузлами всередині кожного кластера.

Довіра до агрегатора T_{agg} визначається за виразом:

$$T_{agg} = \frac{\sum_{n=1}^{k}(T_n+1)\cdot W_n}{\sum_{n=1}^{k}(T_n+1)},$$

де T_n – довіра до вузла n у кластері з k сенсорів; W_n – призначена вага для кожного вузла на основі його довіри.

Переваги: висока точність виявлення, адаптивність, можливість виявляти відомі та невідомі атаки, ефективність управління потоками даних.

Недоліки: складність реалізації, налаштування та обслуговування, залежність від якості навчальних даних, значні вимоги до обчислювальних ресурсів.

У таблиці 6 наведено порівняльний аналіз гібридних методів та моделей виявлення вторгнень.

Таблиця 6

Гібридні методи та моделі виявлення вторгнень

Автор	Підхід	Атаки	Метод	Набір даних	Рівні OSI
Sedjelmaci et al. [32]	Децентралізо-ваний	Чорна діра/Black Hole Вибіркова передача/Selective Forwarding Hello флуд/HELLO flood Тунелювання/Wormhole	База специфіка-цій, SVM	TOSSIM	Мережевий
Yan et al. [33]	Децентралізо-ваний	Виснаження /Exhaustion Затоплення/ Flooding Шкідливе ПЗ/Malware Визначення топології /Homing Відмова в обслуговуванні/DoS	BPN База сигнатур	KDDCup'99	Канальний Мережевий Транспортний Прикладний
Subba et al. [34]	Децентралізо-ваний	Чорна діра/Black Hole Вибіркова передача/Selective Forwarding Тунелювання/Wormhole Відмова в обслуговуванні/DoS Сивілли/Sybil	BNE, База специфікацій легка нейронна мережа	NS2	Канальний Мережевий Транспортний Прикладний
Otoum et al. [35]	Централізований	Виснаження/Exhaustion Затоплення/Flooding Шкідливе ПЗ/Malware Визначення топології/Homing	Випадковий ліс E-DBSCAN	NS2	Канальний Мережевий Транспортний Прикладний

Гібридні моделі та методи виявлення вторгнень дають змогу комбінувати переваги вищезазначених методів (сигнатури, аномалії та специфікації) для підвищення точності та адаптивності. Вони вимагають значних зусиль для налаштування, управління та підтримки, мають велику обчислювальну складність.

Висновки. У статті проведено класифікацію та порівняльний аналіз моделей та методів виявлення вторгнень у безпроводових сенсорних мережах тактичної ланки управління військами, на основі підходу управління, протидії атакам та реалізації по рівнях моделі OSI. Результати порівняльного аналізу свідчать, що універсального методу, що задовольняє вимогам безпеки безпроводових сенсорних мереж не існує.

При централізованому підході управляння на єдиний вузол виявлення здійснюється більше навантаження та зростають витрати часу на ідентифікацію вторгнення. Але при децентралізованому підході модуль виявлення вторгнень розгортається на різних рівнях (вузол, ГК, БС), що вимагає більшого споживання енергії для обміну службовою інформацією.

Методи та моделі виявлення вторгнень на основі сигнатур, аномалій, специфікації дають змогу виявляти відомі та невідомі атаки, проте мають ряд недоліків та складнощів пов'язаних з первинним налаштуванням мережі. Водночас вибір гібридного підходу виправданий у випадках, коли потрібна висока точність та адаптивність до нових загроз.

Саме тому для підвищення ефективності виявлення в реальних умовах потрібно розробити гібридний метод, що поєднує різні моделі та методи виявлення вторгнень з автоматичним налаштуванням параметрів та адаптацією до змін у мережевому середовищі.

Напрямом подальших досліджень слід вважати розроблення функціональної моделі системи виявлення вторгнень для підсистеми безпеки у безпроводових сенсорних мережах тактичної ланки управління військами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Міночкін А. І., Романюк В. А., Шаціло П. В. Виявлення атак в мобільних радіомереж. *Збірник наукових праць № 1*. – Київ. ВІТІ НТУУ "КПІ". – 2005. – С. 102-111.

2. Ghosal A., Halder S. A survey on energy efficient intrusion detection in wireless sensor networks. *Journal of Ambient Intelligence and Smart Environments*. 2017. Vol. 9, no. 2. P. 239–261. URL: https://doi.org/10.3233/ais-170426 (date of access: 07.10.2024).

3. Артюх С.Г., Жук О.В., Чернега В.М. Класифікація атак у безпроводових сенсорних мережах тактичної ланки управління військами. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023.Т. 48. № 3, 2023. С.11-19.

4. On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks / A. Abduvaliyev et al. *IEEE Communications Surveys & Tutorials*. 2013. Vol. 15, no. 3. P. 1223–1237. URL: https://doi.org/10.1109/surv.2012.121912.00006 (date of access: 08.10.2024)..

5. Alrajeh N. A., Khan S., Shams B. Intrusion Detection Systems in Wireless Sensor Networks: A Review. *International Journal of Distributed Sensor Networks*. 2013. Vol. 9, no. 5. P. 167575. URL: https://doi.org/10.1155/2013/167575 (date of access: 07.10.2024).

6. Osanaiye O. A., Alfa A. S., Hancke G. P. Denial of Service Defence for Resource Availability in Wireless Sensor Networks. *IEEE Access*. 2018. Vol. 6. P. 6975–7004. URL: https://doi.org/10.1109/access.2018.2793841 (date of access: 08.10.2024).

7. Alrajeh N. A., Lloret J. Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*. 2013. Vol. 9, no. 10. P. 351047. URL: https://doi.org/10.1155/2013/351047 (date of access: 08.10.2024).

8. Intrusion Detection System Based on Evolving Rules for Wireless Sensor Networks / N. Lu et al. *Journal of Sensors*. 2018. Vol. 2018. P. 1–8. URL: https://doi.org/10.1155/2018/5948146 (date of access: 08.10.2024).

9. A Partially Distributed Intrusion Detection System for Wireless Sensor Networks / E. Cho et al. *Sensors*. 2013. Vol. 13, no. 12. P. 15863–15879. URL: https://doi.org/10.3390/s131215863 (date of access: 08.10.2024).

10. Centralized IDS Based on Misuse Detection for Cluster-Based Wireless Sensors Networks / F. Hidoussi et al. *Wireless Personal Communications*. 2015. Vol. 85, no. 1. P. 207–224.

11. Hierarchical Abnormal-Node Detection Using Fuzzy Logic for ECA Rule-Based Wireless Sensor Networks / N. Berjab et al. *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, Taipei, Taiwan, 4–7 December 2018. 2018. URL: https://doi.org/10.1109/prdc.2018.00051 (date of access: 08.10.2024).

12. Ioannou C., Vassiliou V. An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression. *MSWIM '18: 21st ACM Int'l Conference on Modelling, Analysis and Simulation of Wireless and Mobile Systems*, Montreal QC Canada. New York, NY, USA, 2018. URL: https://doi.org/10.1145/3242102.3242145 (date of access: 08.10.2024).

13. Osanaiye O. A., Alfa A. S., Hancke G. P. Denial of Service Defence for Resource Availability in Wireless Sensor Networks. *IEEE Access*. 2018. Vol. 6. P. 6975–7004. URL: https://doi.org/10.1109/access.2018.2793841 (date of access: 08.10.2024).

14. Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model / L. Han et al. *Information Sciences*. 2019. Vol. 476. P. 491–504. URL: https://doi.org/10.1016/j.ins.2018.06.017 (date of access: 08.10.2024).

15. Detection and mitigation of sinkhole attacks in wireless sensor networks / H. Shafiei et al. *Journal of Computer and System Sciences*. 2014. Vol. 80, no. 3. P. 644–653. URL: https://doi.org/10.1016/j.jcss.2013.06.016 (date of access: 08.10.2024).

16. Ballarini P., Mokdad L., Monnet Q. Modeling tools for detecting DoS attacks in WSNs. *Security and Communication Networks*. 2013. Vol. 6, no. 4. P. 420–436.

17. Kaur G., Singh M. Detection of black hole in Wireless Sensor Network based on Data Mining. *2014 5th International Conference- Confluence The Next Generation Information Technology Summit*, Noida, India, 25–26 September 2014. 2014. URL: https://doi.org/10.1109/confluence.2014.6949343 (date of access: 08.10.2024).

18. Hybrid Anomaly Detection by Using Clustering for Wireless Sensor Network / B. Ahmad et al. *Wireless Personal Communications*. 2018. Vol. 106, no. 4. P. 1841–1853. URL: https://doi.org/10.1007/s11277-018-5721-6 (date of access: 08.10.2024).

19. Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks / L. Coppolino et al. *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, COMPIEGNE, France, 28–30 October 2013. 2013.

20. A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network / W. Li et al. *Journal of Electrical and Computer Engineering*. 2014. Vol. 2014. P. 1–8. URL: https://doi.org/10.1155/2014/240217 (date of access: 08.10.2024).

21. Garofalo A., Di Sarno C., Formicola V. Enhancing Intrusion Detection in Wireless Sensor Networks through Decision Trees. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2013. P. 1–15. URL: https://doi.org/10.1007/978-3-642-38789-0_1 (date of access: 08.10.2024)..

22. Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks / S. Shamshirband et al. *Engineering Applications of Artificial Intelligence*. 2014. Vol. 32. P. 228–241. URL: https://doi.org/10.1016/j.engappai.2014.02.001 (date of access: 08.10.2024).

23. Wang H., Wen Y., Zhao D. Identifying localization attacks in wireless sensor networks using deep learning. *Journal of Intelligent & Fuzzy Systems*. 2018. Vol. 35, no. 2. P. 1339–1351. URL: https://doi.org/10.3233/jifs-169677 (date of access: 08.10.2024).

24. A Lightweight Intrusion Detection Method Based on Fuzzy Clustering Algorithm for Wireless Sensor Networks / H. Qu et al. *Advances in Fuzzy Systems*. 2018. Vol. 2018. P. 1–12. URL: https://doi.org/10.1155/2018/4071851 (date of access: 08.10.2024).

25. Wireless Sensor Networks Intrusion Detection Based on SMOTE and the Random Forest Algorithm / X. Tan et al. Sensors. 2019. Vol. 19, no. 1. P. 203. URL: https://doi.org/10.3390/s19010203 (date of access: 08.10.2024).

26. Mansouri A., Majidi B., Shamisa A. Metaheuristic neural networks for anomaly recognition in industrial sensor networks with packet latency and jitter for smart infrastructures. *International Journal of Computers and Applications*. 2018. P. 1–10. URL: https://doi.org/10.1080/1206212x.2018.1533613 (date of access: 08.10.2024).

27. Bitam S., Zeadally S., Mellouk A. Bio-inspired cybersecurity for wireless sensor networks. *IEEE Communications Magazine*. 2016. Vol. 54, no. 6. P. 68–74.

28. N. Nithiyanandam, P. Latha Parthiban, B. Rajalingam. Effectively Suppress the Attack of Sinkhole in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique. *International Journal of Pure and Applied Mathematics*, Vol. 118, No. 9, pp. 313-329, 2018.

29. An Integrated Intrusion Detection Model of Cluster-Based Wireless Sensor Network / X. Sun et al. *PLOS ONE*. 2015. Vol. 10, no. 10. P. e0139513. URL: https://doi.org/10.1371/journal.pone.0139513 (date of access: 08.10.2024).

30. A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks / T. Ma et al. *Sensors*. 2016. Vol. 16, no. 10. P. 1701. URL: https://doi.org/10.3390/s16101701 (date of access: 08.10.2024).

31. A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks / T. Ma et al. *Sensors*. 2016. Vol. 16, no. 10. P. 1701. URL: https://doi.org/10.3390/s16101701 (date of access: 08.10.2024).

32. Sedjelmaci H., Senouci S. M., Feham M. An efficient intrusion detection framework in cluster-based wireless sensor networks. *Security and Communication Networks*. 2013. Vol. 6, no. 10. P. 1211–1224. URL: https://doi.org/10.1002/sec.687 (date of access: 08.10.2024).

33. Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network / K. Q. Yan et al. *2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010)*, Chengdu, China, 9–11 July 2010. 2010. URL: https://doi.org/10.1109/iccsit.2010.5563886 (date of access: 08.10.2024).

34. Subba B., Biswas S., Karmakar S. A Game Theory Based Multi Layered Intrusion Detection Framework for Wireless Sensor Networks. *International Journal of Wireless Information Networks*. 2018. Vol. 25, no. 4. P. 399–421. URL: https://doi.org/10.1007/s10776-018-0403-6 (date of access: 08.10.2024).

35. Otoum S., Kantarci B., Mouftah H. T. Detection of Known and Unknown Intrusive Sensor Behavior in Critical Applications. *IEEE Sensors Letters*. 2017. Vol. 1, no. 5. P. 1–4. URL: https://doi.org/10.1109/lsens.2017.2752719 (date of access: 08.10.2024).

DOI: 10.58254/viti.6.2024.02.24

УДК 621.3:623.4:629.07-044.4

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

СУЧАСНІ МЕТОДИ І АЛГОРИТМИ ПЛАНУВАННЯ ШЛЯХУ ДЛЯ АВТОНОМНИХ МОБІЛЬНИХ РОБОТІВ, ЇХ ЦІЛЬОВІ ФУНКЦІЇ

Сучасна ситуація в світі алгоритмів дослідження планування шляху автономними роботами показує, що існує велика кількість алгоритмів та їх модифікацій, які вимагають від дослідників та інженерів автономної робототехніки тонкого розуміння фундаментальних аспектів їх функціонування. Загальною метою дослідження є проведення аналізу існуючих алгоритмів, методів та їх модифікацій з точки зору складової математичного апарата, а саме їх цільових функцій.

В дослідженні розглянуто 38 сучасних алгоритмів і методів планування шляху автономними роботами. Розглянута важливість і критичність розуміння цільової функції для галузі робототехніки. Наведені приклади, що ілюструють важливість цього аспекту. В процесі дослідження алгоритми представлені в виді формалізованих узагальнених математичних формул з урахуванням можливих мінімізації/максимізації, їх вдосконалень і покращень.

До кожного розглянутого алгоритму і методу наданий висновок стосовно його цільової функції.

У дослідженні окремо виділено методи "Динамічних ігор" та розглянуто застосування фундаментального "Методу розв'язуючих функцій А. О. Чикрія" для планування шляху.

В загальних висновках, надана інформація переваг та важливості розуміння математичного апарата алгоритмів пошуку шляху автономними роботами задля вирішення наукових завдань. Узагальнені результати зведені до єдиної порівняльної таблиці, що надає формалізовану основну функцію алгоритмів, розкриває основну ідею, переваги/недоліки, сферу застосування і приклад використання. Порівняльна таблиця представлена в формі узагальненого допоміжного довідкового елемента дослідження.

Ключові слова: *алгоритми, дослідження, автономний робот, методи, планування шляху, ЦФ, оптимізація.*

A. Bernatskyi Modern methods and algorithms of path planning of autonomous robots and their objective functions.

The current situation in the world of research algorithms for path planning by autonomous robots shows that there are a large number of algorithms and their modifications that require researchers and engineers of autonomous robotics to have a fine understanding of the fundamental aspects of their functioning. The general goal of the research is to conduct an analysis of existing algorithms, methods and their modifications from the point of view of the component of the mathematical apparatus, namely their target functions.

The research examines 38 modern algorithms and methods of path planning by autonomous robots. Considered the importance and criticality of understanding the objective function for the field of robotics. Examples illustrating the importance of this aspect are given. In the process of research, algorithms are presented in the form of formalized generalized mathematical formulas taking into account possible minimization/maximization, their improvements and improvements.

For each considered algorithm and method, a conclusion is given regarding its target function.

In the study, the methods of "Dynamic games" are separately highlighted and the application of the fundamental "Method of solving functions of A.O. Chikryi" for path planning is considered.

In general, information on the advantages and importance of understanding the mathematical apparatus of path-finding algorithms by autonomous robots for solving scientific problems is provided. The generalized results are summarized in a single comparative table, which provides the main formalized function of the algorithms, reveals the main idea, advantages/disadvantages, the scope of application and an example of use. The comparative table is presented in the form of a generalized auxiliary reference element of the study.

Keywords: *algorithms, autonomous robot, methods, path planning, research, objective function, optimization*

Постановка завдання. На сучасному етапі розвитку інформаційних технологій, інформаційне поле заповнено й перенасичено дослідженнями, порівняльними аналізами алгоритмів побудови шляху мобільними роботами (МР) [1].

Розуміння цільової функції є критично важливим при дослідженні алгоритмів пошуку шляху, оскільки вона визначає, що саме алгоритм намагається оптимізувати. Цільова функція (ЦФ) може включати різні критерії, такі як мінімізація відстані, часу, витрат або ризиків [2].

Наведемо кілька прикладів, які ілюструють важливість цього аспекту [1]:

– *Мінімізація відстані*. У класичному алгоритмі А* ЦФ зазвичай спрямована на мінімізацію відстані між початковою та кінцевою точками. Це досягається шляхом використання евристичної функції, яка оцінює відстань від поточної точки до цільової. Якщо ЦФ правильно визначена, алгоритм ефективно знаходить найкоротший шлях;

– *Логістика.* В логістиці ЦФ може включати мінімізацію витрат на транспортування або часу доставки. Наприклад, при плануванні маршруту для доставки товарів, алгоритм повинен враховувати не лише відстань, але й інші фактори, такі як дорожні умови, трафік та витрати на паливо. Вибір правильної цільової функції дозволяє оптимізувати ці параметри і забезпечити ефективну доставку;

– *Військові транспортні системи.* У військових транспортних системах, таких як планування військової операції з задіянням багатомодової складової автономних мобільних роботів (АМР), ЦФ може включати мінімізацію зіткнення з уникненням утворення заторів в урбанізованому середовищі та оптимізацію потоку дронів. Алгоритми повинні враховувати різні фактори, такі як час доби, погодні умови, вплив РЕБ противника, засідки. Вибір відповідної цільової функції дозволяє ефективно керувати військовим трафіком і зменшувати час виконання завдання АМР;

– *Відеоігри.* У відеоіграх ЦФ може бути більш складною і включати не лише мінімізацію відстані, але й уникнення перешкод та ворогів. Наприклад, у стратегіях реального часу алгоритми пошуку шляху повинні враховувати динамічні зміни на карті, такі як рухомі об'єкти або змінні перешкоди. Правильне визначення цільової функції дозволяє персонажам гри ефективно досягати своїх цілей, уникаючи небезпек;

– Ройові алгоритми й алгоритми оптимізації мурашиної колонії *(ant colony optimization – ACO).* АСО використовує цільову функцію для знаходження найкоротшого шляху, імітуючи поведінку мурах. Мурахи залишають феромонові сліди на шляху до їжі, і інші мурахи схильні слідувати цим слідам, що призводить до знаходження оптимального шляху. ЦФ в цьому випадку включає мінімізацію відстані та максимізацію феромонових слідів.

Розуміння *цільових функцій алгоритмів* та їх порівняння знаходження оптимального шляху з точки зору вирішення наукових завдань, надає багато важливих переваг, а саме:

– *Оцінка ефективності.* Порівняння цільових функцій дозволяє оцінити, наскільки ефективно різні алгоритми виконують свої завдання в різних умовах;

– *Вибір оптимального алгоритму.* Різні задачі можуть вимагати різних підходів до оптимізації. Порівняння цільових функцій допомагає визначити, який алгоритм найкраще підходить для конкретної задачі;

– *Виявлення сильних і слабких сторін.* Аналіз цільових функцій дозволяє виявити сильні та слабкі сторони кожного алгоритму. Це може включати виявлення ситуацій, в яких алгоритм працює неефективно, або умов, за яких він дає найкращі результати;

– *Поліпшення алгоритмів.* Порівняння цільових функцій може вказати на можливості для поліпшення існуючих алгоритмів. Це може включати модифікацію цільової функції або інтеграцію нових евристик для підвищення ефективності;

– *Теоретичний внесок.* Наукове порівняння цільових функцій сприяє розвитку теорії алгоритмів та оптимізації. Це дозволяє краще розуміти фундаментальні принципи, які лежать в основі роботи алгоритмів, і може призвести до відкриття нових методів та підходів до вирішення задач оптимізації.

Аналіз останніх публікацій. Відомо багато досліджень та порівнянь алгоритмів побудови шляху. Так, наприклад в дослідженні [3], Ші Вей Лі (Shi Wei Li) аналізує оптимізацію цільової функції на основі класичної оптимізації рою частинок для двовимірного планування шляху. В дослідженні [4], Каур Каріндер (Harinder, Kaur Sidhu) оцінює продуктивність різних алгоритмів пошуку шляху, зокрема, як вони оптимізують цільову функцію для знаходження найкоротшого маршруту на заданій карті. В роботі [5], Самрид Гарг

(Samridh Garg) й Бхану Деві (Bhanu Devi) пропонують модифікований алгоритм Дейкстри з адаптивною штрафною функцією для знаходження оптимального найкоротшого шляху між початковою та кінцевою точками. Аналітичне дослідження [6], Стефана Вейсер (Stephan Weiser), Ганса Вулфа (Hans Wulf) і Йорна Іхлеманна (Jörn Ihlemann), демонструє застосування алгоритму найглибшого шляху для кращого розуміння ландшафтів цільової функції. Також відомі порівняльні дослідження алгоритмів пошуку шляху [7], в якому автори Матвійчук Р. Д. і Данильчук О. М. порівнюють деякі алгоритми на рівні псевдо-кодової конструкції. В дослідженні [8] А. А. Проценко і В. Г. Іванов розглядають 35 алгоритмів пошуку шляху та методів оптимізації на понятійному рівні карт зі словесним описом виконання дії алгоритмом. Взагалі основна маса досліджень націлені на розгляд основних проблем, що виникають під час виконання задачі пошуку шляхів АМР.

Але важливим елементом будь-якого алгоритму є в першу чергу математична складова, а саме його цільова функція та її трансформації.

Метою статті є наукове дослідження з *урахуванням математичного апарата цільових функцій,* існуючих методів і алгоритмів, що дозволяють МР виконувати завдання в автономному режимі.

Виклад основного матеріалу: велика кількість сучасних алгоритмів та їх модифікацій вимагають від дослідників та інженерів автономної робототехніки тонкого розуміння фундаментальних аспектів їх функціонування. Для чого розглянемо найбільш відомі сучасні алгоритми та модифікації, а саме: VCD, BCD, Morse decomposition, Exhaustive path planning with exact cell decomposition, Approximate cell decomposition, Sensor path planning with approximate cell decomposition, QB decomposition, FQD, K-Framed quadtrees decomposition, Adaptive decomposition, Probabilistic cell decomposition, Probabilistic cell decomposition with harmonic functions, Ariadne's clew, Expansive configuration spaces, PRM, RRM, Lazy PRM, Gaussian sampling for PRM, Halton sampling for PRM, D*, Goal-directed and randomized search, SANDROS, APF, DAPF, IAPF, Artificial potential field based subgoal network, Dynamic subgoal path planner, Hierarchical motion planner, Two-layered subgoal algorithm, RRT with local trees, Obstacle-based RRT, RRT-connect, Bi-RRT, RRT*, Informed-RRT*, MBD-RRT*FFT, Динамічні ігри та Метод розв'язуючих функцій А.О. Чикрія для планування шляху. Проведемо їх детальний опис і зазначимо основні характеристики, переваги та недоліки[9–85].

1. Алгоритм *вертикального клітинного розбиття* (Vertical Cellular Decomposition) розбиває простір на вертикальні клітини, що дозволяє створити карту для планування шляху. Основні переваги включають простоту реалізації та високу точність, але можливі проблеми з масштабованістю та високі вимоги до обчислювальних ресурсів [9, 10]. ЦФ для цього алгоритму може бути виражена як математична формула (1.1), яка мінімізує або максимізує певний параметр, пов'язаний з розбиттям простору.

Зазвичай, ЦФ для таких алгоритмів може бути пов'язана з мінімізацією кількості клітин або з максимізацією ефективності покриття простору.

$$\text{Minimize } \sum_{i=1}^{n} A_i, \tag{1.1}$$

де A_i – площа *i*-тої клітини, а n – загальна кількість клітин.

Таким чином, розуміючи, що обчислювальна складність алгоритму залежить від кількості перешкод у просторі і може бути значною, особливо для просторів з великою кількістю перешкод. Бачимо спрямованість цільової функції на мінімізацію довжини шляху та часу виконання, що робить його ефективним для багатьох практичних застосувань, але вимагає оптимізації для роботи з великими даними.

2. Алгоритм *Boustrophedon Cellular Decomposition* (BCD) розбиває простір на клітини, які покриваються простими зворотно-поступальними рухами. Це забезпечує ефективне покриття простору та простоту реалізації, але можливі проблеми з масштабованістю та високі вимоги до обчислювальних ресурсів [11].

ЦФ цього алгоритму може бути виражена як математична формула, яка мінімізує певні параметри, такі як загальна довжина шляху або кількість переходів між клітинами.

ЦФ (2.1) що мінімізує загальну довжину шляху для алгоритму BCD має вигляд:

$$\text{Minimize } \sum_{i=1}^{n}(L_i + T_i), \tag{2.1}$$

де L_i – довжина шляху для покриття і-тої клітини, T_i – довжина переходу від і-тої клітини до $(i+1)$-тої клітини, n – загальна кількість клітин.

Таким чином, ЦФ для алгоритму Boustrophedon Cellular Decomposition може бути виражена як математична формула, яка мінімізує загальну довжину шляху або кількість переходів між клітинами, залежно від конкретних вимог задачі.

3. Алгоритм *Morse Decomposition* використовує теорію Морзе для розбиття простору на клітини, що дозволяє аналізувати динамічні системи шляхом розбиття фазового простору на інваріантні множини, які називаються Morse sets. Основні переваги включають глибокий математичний підхід та можливість аналізу топології, але алгоритм складний у реалізації та має високі вимоги до обчислювальних ресурсів [12, 13, 14].

Цільову функцію можемо виразити як математичну формулу (3.1), що пов'язана з мінімізацією складності розбиття або з максимізацією точності виявлення інваріантних множин. тобто мінімізує або максимізує певний параметр, пов'язаний з розбиттям простору.

Цільова функція, яка мінімізує суму відхилень від інваріантних множин має вигляд (3.1):

$$\text{Minimize } \sum_{i=1}^{n}\int_{M_i} \parallel \dot{x} - f(x)^2 \parallel dx, \tag{3.1}$$

де M_i – i-та Morse множина, $\dot{x}$ – похідна траєкторії, $f(x)$ – векторне поле динамічної системи, n – загальна кількість Morse множин.

Таким чином, ЦФ для алгоритму Morse Decomposition може бути виражена як математична формула, яка мінімізує суму відхилень від інваріантних множин або кількість Morse множин, залежно від конкретних вимог задачі.

4. Алгоритм *планування шляхів з використанням точного розбиття на клітини* (Exhaustive Path Planning with Exact Cell Decomposition) забезпечує вичерпне планування шляху з точним розбиттям простору на клітини, щоб знайти оптимальний шлях від початкової до кінцевої точки, уникаючи перешкод. Це гарантує високу точність планування, але алгоритм складний у реалізації та має високі вимоги до обчислювальних ресурсів [15, 16].

ЦФ для цього алгоритму може бути виражена як математична формула, яка мінімізує певний параметр, наприклад, загальну довжину шляху або час проходження.

ЦФ, яка мінімізує загальну довжину шляху, мінімізує суму відстаней між послідовними клітинами на шляху, що дозволяє знайти найкоротший шлях через розбитий простір, має вигляд (4.1):

$$\text{Minimize } \sum_{i=1}^{n} d(C_i, C_{i+1}), \tag{4.1}$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, n – загальна кількість клітин на шляху.

ЦФ, що мінімізує час проходження шляху AMP, враховує як відстань, так і швидкість руху в кожній клітині, це дозволяє мінімізувати загальний час проходження шляху (4.2):

$$\text{Minimize } \sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i}, \tag{4.2}$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, v_i – швидкість руху в клітині C_i, n – загальна кількість клітин на шляху.

Таким чином, ЦФ для алгоритму планування шляхів з використанням точного розбиття на клітини може бути виражена як математична формула, яка мінімізує загальну довжину шляху або час проходження, залежно від конкретних вимог задачі.

5. Алгоритм *Approximate Cell Decomposition* розбиває простір на регулярні клітини, такі як прямокутники або квадрати з метою спрощення задачі планування шляху. Основні переваги включають швидкість обчислень та простоту реалізації, але точність менша порівняно з точними методами, і можливі помилки через наближення [17].

ЦФ для цього алгоритму, яка мінімізує загальну довжину шляху, мінімізує суму відстаней між послідовними клітинами на шляху, що дозволяє знайти найкоротший шлях через розбитий простір має вигляд:

$$\mathcal{OCB}_j[k^u] = \cup_{t=1}^{k_u}\{\ \mathcal{CB}_j[[x_k, x'_k] \cdot [y_k, y'_k] \cdot (\gamma_k + l \triangle \theta)]\}, \quad (5.1)$$

де $\mathcal{CB}_j$ – відстань між центрами клітин x_k, y_k та $\gamma_k + l \triangle \theta$, k_u – загальна кількість клітин на шляху.

ЦФ що мінімізує кількість клітин, через які проходить шлях, спрямована на зменшення кількості клітин, через які проходить шлях, що може бути корисним для зменшення складності обчислень:

$$\mathcal{ICT}_j[k^u] = \cup_{t=1}^{k_u}\{\ \mathcal{CT}_j[[x_k, x'_k] \cdot [y_k, y'_k] \cdot (\gamma_k + l \triangle \theta)]\}, \quad (5.2)$$

де k_u – загальна кількість клітин на шляху.

Таким чином, ЦФ для алгоритму Approximate Cell Decomposition може бути виражена як математична формула, яка мінімізує загальну довжину шляху або кількість клітин, через які проходить шлях, залежно від конкретних вимог задачі.

6. Алгоритм планування шляху сенсора з використанням наближеного розбиття на клітини (Sensor Path Planning with Approximate Cell Decomposition) використовує метод декомпозиції простору, за рахунок розбивки конфігураційного простору на дискретні клітини для планування шляху сенсором. Цей підхід дозволяє ефективно працювати в складних середовищах з різними типами перешкод, але має високі вимоги до обчислювальних ресурсів і потребує складних налаштування параметрів [18, 19].

ЦФ для цього алгоритму виражена як математична формула, що мінімізує певний параметр, такий як, загальна довжина шляху, час проходження або кількість клітин, через які проходить шлях.

ЦФ, яка мінімізує загальну довжину шляху сенсора має вигляд (6.1):

$$\text{Minimize } \sum_{i=1}^{n} d(C_i, C_{i+1}), \quad (6.1)$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, n – загальна кількість клітин на шляху.

ЦФ враховує як відстань, так і швидкість руху сенсора в кожній клітині, що дозволяє мінімізувати загальний час проходження шляху (6.2):

$$\text{Minimize } \sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i}, \quad (6.2)$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, v_i – швидкість руху в клітині C_i, n – загальна кількість клітин на шляху.

Таким чином, ЦФ для алгоритму планування шляху сенсора з використанням наближеного розбиття на клітини може бути виражена як математична формула, яка мінімізує загальну довжину шляху (6.1), час проходження (6.2) або кількість клітин, через які проходить шлях, залежно від конкретних вимог задачі.

7. Алгоритм *Quadtree-based decomposition* використовує декомпозицію простору на квадрати, з метою аналізу, зберігання або обробки даних, що дозволяє ефективно працювати у високовимірних просторах. Основні переваги включають простоту реалізації, але можливі проблеми з масштабованістю та необхідність налаштування параметрів [20, 21].

ЦФ для цього алгоритму мінімізує певний параметр, такий як неоднорідність даних у квадрантах або кількість розподілу.

Мінімізація неоднорідності даних у квадрантах:

$$\text{Minimize } \sum_{i=1}^{n} Var(Q_i), \quad (7.1)$$

де $Var(Q_i)$ – дисперсія даних у i-му квадранті Q_i, n – загальна кількість квадрантів.

Таким чином, ЦФ для алгоритму Quadtree-based decomposition є математична формула, яка мінімізує неоднорідність даних у квадрантах (7.1) або кількість розбиттів, залежно від конкретних вимог задачі.

8. Алгоритм *Framed-Quadtree Decomposition* використовується для ефективного розбиття простору на клітини з метою планування шляху є вдосконаленою версією quadtree, що зменшує кількість вузлів за рахунок використання рамок. Це підвищує ефективність, але алгоритм складніший у реалізації і має високі вимоги до обчислювальних ресурсів [22, 23, 24].

ЦФ для цього алгоритму мінімізує певний параметр, такий як, загальна довжина шляху або час проходження.

8.1. Мінімізація загальної довжини шляху:

$$\text{Minimize } \sum_{i=1}^{n} d(C_i, C_{i+1}), \tag{8.1}$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, n – загальна кількість клітин на шляху.

Ця ЦФ мінімізує суму відстаней між послідовними клітинами на шляху, що дозволяє знайти найкоротший шлях через розбитий простір.

8.2. Мінімізація часу проходження враховує як відстань, так і швидкість руху в кожній клітині, що дозволяє мінімізувати загальний час проходження шляху:

$$\text{Minimize } \sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i}, \tag{8.2}$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, v_i – швидкість руху в клітині C_i, n – загальна кількість клітин на шляху.

Таким чином, ЦФ для алгоритму Framed-Quadtree Decomposition може бути виражена як математична формула, яка мінімізує загальну довжину шляху (8.1), час проходження (8.2) або кількість клітин (8.3), через які проходить шлях, залежно від конкретних вимог задачі.

9. Алгоритм *K-Framed Quadtrees Decomposition* поєднує квадратно-рамкову декомпозицію, що дозволяє зменшити кількість вузлів та підвищити точність. Цей підхід забезпечує підвищену ефективність та точність у порівнянні з framed-quadtree, але також має високі вимоги до обчислювальних ресурсів і складний у реалізації [24, 25].

ЦФ для цього алгоритму є математична формула, яка мінімізує або максимізує певний параметр, залежно від конкретної задачі.

9.1. Мінімізація загальної довжини шляху при плануванні траєкторії:

$$\text{Minimize } \sum_{i=1}^{n} d(C_i, C_{i+1}), \tag{9.1}$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, n – загальна кількість клітин на шляху.

9.2. Мінімізація неоднорідності даних у клітинах:

$$\text{Minimize } \sum_{i=1}^{n} Var(C_i), \tag{9.2}$$

де $Var(C_i)$ – дисперсія (або інший показник неоднорідності) даних у i-ій клітині C_i, n – загальна кількість клітин.

Таким чином, ЦФ для алгоритму K-Framed Quadtrees Decomposition може бути виражена як математична формула, яка мінімізує загальну довжину шляху (9.1), кількість клітин або неоднорідність даних у клітинах (9.2), залежно від конкретних вимог задачі.

10. Алгоритм *Adaptive Decomposition* використовує адаптивний підхід для декомпозиції простору і розбиття сигналів або простору на адаптивні компоненти, що дозволяє алгоритму адаптуватися до різних умов з метою аналізу, обробки або оптимізації. Основні переваги включають високу гнучкість та адаптивність, але алгоритм складний у реалізації та має високі вимоги до обчислювальних ресурсів [26, 27, 28].

ЦФ для цього алгоритму є математична формула, що мінімізує певний параметр, такий як, похибку реконструкції сигналу або неоднорідність даних у розбитих компонентах.

10.1. Мінімізація похибки реконструкції сигналу:

$$\text{Minimize } \sum_{i=1}^{n} \left| x(t) - \sum_{j=1}^{m} C_j(t) \right|^2, \tag{10.1}$$

де $x(t)$ – оригінальний сигнал, $C_j(t)$ – j-та адаптивна компонента сигналу, n – кількість точок в сигналі, m – кількість адаптивних компонент.

10.2. Мінімізація неоднорідності даних у розбитих компонентах:

$$\text{Minimize } \sum_{i=1}^{n} Var(C_i), \tag{10.2}$$

де $Var(C_i)$ – дисперсія даних у i-тій компоненті C_i, n - загальна кількість компонентів.

Таким чином, ЦФ для алгоритму Adaptive Decomposition може бути виражена як математична формула, яка мінімізує похибку реконструкції сигналу (10.1), неоднорідність даних у компонентах (10.2) або кількість компонентів, залежно від конкретних вимог задачі.

11. Алгоритм *Probabilistic Cell Decomposition* (Ймовірнісне розбиття на клітини) використовує розбиття простору на комірки, які оцінюються на основі ймовірності проходження через них та використовується для планування шляху в середовищах з невизначеністю. Цей метод ефективний у високовимірних просторах і складних середовищах, але має високі вимоги до обчислювальних ресурсів і складний у реалізації [29, 30].

ЦФ для цього алгоритму є математична формула, яка мінімізує певний параметр, такий як ймовірність зіткнення або загальну довжину шляху з урахуванням ймовірностей.

11.1. Мінімізація ймовірності зіткнення:

$$\text{Minimize } \sum_{i=1}^{n} P(C_i), \tag{11.1}$$

де $P(C_i)$ – ймовірність того, що клітина C_i містить перешкоди, n – загальна кількість клітин на шляху.

11.2. Мінімізація загальної довжини шляху з урахуванням ймовірностей:

$$\text{Minimize } \sum_{i=1}^{n} d(C_i, C_{i+1}) \cdot P(C_i), \tag{11.2}$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, $P(C_i)$ – ймовірність того, що клітина C_i містить перешкоди, n – загальна кількість клітин на шляху.

11.3. Мінімізація часу проходження з урахуванням ймовірностей:

$$\text{Minimize } \sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i} \cdot P(C_i), \tag{11.3}$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, v_i – швидкість руху в клітині C_i, $P(C_i)$ – ймовірність того, що клітина C_i містить перешкоди, n – загальна кількість клітин на шляху.

Таким чином, ЦФ для алгоритму Probabilistic Cell Decomposition може бути виражена як математична формула, яка мінімізує ймовірність зіткнення (11.1), загальну довжину шляху (11.2) або час проходження з урахуванням ймовірностей (11.3), залежно від конкретних вимог задачі.

12. Алгоритм *Probabilistic Cell Decomposition with Harmonic Functions,* поєднує ймовірнісне розбиття простору на ймовірнісні комірки з використанням гармонічних функцій для покращення точності планування шляху. Гармонічні функції мають властивість уникати локальних мінімумів, що робить їх корисними для планування шляху в складних середовищах. Цей метод має високі вимоги до обчислювальних ресурсів і складний у реалізації [30].

ЦФ для такого алгоритму є математична формула, яка мінімізує певний параметр, такий як, ймовірність зіткнення або загальна довжину шляху з урахуванням гармонічних потенціалів.

12.1. Мінімізація ймовірності зіткнення з урахуванням гармонічних функцій:

$$\text{Minimize } \sum_{i=1}^{n} P(C_i) \cdot H(C_i), \tag{12.1}$$

де $P(C_i)$ – ймовірність того, що клітина C_i містить перешкоди, $H(C_i)$ – значення гармонічної функції в клітині C_i, n – загальна кількість клітин на шляху.

12.2. Мінімізація загальної довжини шляху з урахуванням гармонічних функцій:

$$\text{Minimize } \sum_{i=1}^{n} d(C_i, C_{i+1}) \cdot H(C_i), \tag{12.2}$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, $H(C_i)$ – значення гармонічної функції в клітині C_i, n – загальна кількість клітин на шляху.

12.3. Мінімізація часу проходження з урахуванням гармонічних функцій:

$$\text{Minimize } \sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i} \cdot H(C_i), \tag{12.3}$$

де $d(C_i, C_{i+1})$ – відстань між центрами клітин C_i та C_{i+1}, v_i – швидкість руху в клітині C_i, $H(C_i)$ – значення гармонічної функції в клітині C_i, n – загальна кількість клітин на шляху.

Таким чином, ЦФ для алгоритму Probabilistic Cell Decomposition з використанням гармонічних функцій, може бути виражена як математична формула, яка мінімізує ймовірність зіткнення (12.1), загальну довжину шляху (12.2) або час проходження з урахуванням гармонічних потенціалів (12.3), залежно від конкретних вимог задачі.

13. Алгоритм *Ariadne's Clew* (нитка Аріадни) використовується для планування траєкторії в високовимірних безперервних просторах і складних середовищах та застосовується для АМР з багатьма ступенями свободи як у статичних, так і в динамічних середовищах. Цей алгоритм, будує дерево, що досліджує нові області простору в кожній ітерації. Має високі вимоги до обчислювальних ресурсів і складний у реалізації [31, 32]. Алгоритм складається з двох підалгоритмів, SEARCH (пошук) і EXPLORE (дослідження), що виконуються почергово.

ЦФ для алгоритму Ariadne's Clew визначається як оптимізаційна задача, яка мінімізує певний параметр, такий як, відстань до цілі або час проходження, з урахуванням інформації про доступний простір.

Загальна ЦФ для алгоритму Ariadne's Clew має вигляд:

$$\text{Minimize } f(q) = \sum_{i=1}^{n} \left(d(q_i, q_{goal}) + \lambda \cdot g(q_i) \right), \tag{13.1}$$

де $f(q)$ – загальна ЦФ, q – поточне положення МР, q_{goal} – положення цільової точки, $d(q_i, q_{goal})$ – відстань від поточного положення q_i до цільової точки, $g(q_i)$ – функція, що враховує інформацію про доступний простір, зібрану підалгоритмом EXPLORE, λ – ваговий коефіцієнт, що визначає вплив функції $g(q_i)$, n – кількість кроків на шляху.

13.1. *Підалгоритм SEARCH* намагається знайти шлях до цілі, мінімізуючи відстань до цільової точки:

$$\text{Minimize } d(q_i, q_{goal}). \tag{13.2}$$

13.2. *Підалгоритм EXPLORE* збирає інформацію про доступний простір, що визначено через функцію $g(q_i)$, яка враховує параметри, такі як, щільність перешкод або доступність шляхів:

$$g(q_i) = \sum_{j=1}^{m} \left(\frac{1}{\left\| q - q_{obs_j} \right\|} \right), \tag{13.3}$$

де q_{obs_j} – положення перешкоди j, а m – кількість перешкод.

13.3. *Загальна ЦФ* для алгоритму Ariadne's Clew, що враховує обидва підалгоритми, має вигляд:

$$\text{Minimize } f(q) = \sum_{i=1}^{n} \left(d(q_i, q_{goal}) + \lambda \cdot \sum_{j=1}^{m} \left(\frac{1}{\left\| q - q_{obs_j} \right\|} \right) \right). \tag{13.4}$$

Таким чином, ЦФ алгоритму (13.4) Ariadne's Clew формується на основі двох підалгоритмів (13.2), (13.3), які використовують оптимізаційні методи для пошуку цілі та дослідження простору. Складність цільової функції визначається високовимірністю простору, динамічністю середовища та використанням оптимізаційних методів. Це робить алгоритм ефективним, але водночас і складним з точки зору обчислювальних ресурсів.

14. Алгоритм *Expansive Configuration Spaces* (ECS) використовує випадкове зразкування для дослідження конфігураційного простору. Алгоритм використовується для планування траєкторій у складних просторах конфігурацій, де важливо ефективно досліджувати простір і знаходити з'єднання між різними областями. Алгоритм ефективний у складних просторах й високовимірних середовищах, але має високі вимоги до обчислювальних ресурсів і складний у реалізації [33].

ЦФ для цього алгоритму зазвичай включає компоненти, які враховують як розширення простору, так і з'єднання між конфігураціями.

Загальна вигляд цільової функції для алгоритму Expansive Configuration Spaces:

$$\text{Minimize } U_{total}(q) = U_{exp}(q) + U_{conn}(q), \quad (14.1)$$

де $U_{total}(q)$ – загальний потенціал у точці q, $U_{exp}\ (q)$ – потенціал розширення, який стимулює дослідження нових областей простору конфігурацій, $U_{conn}(q)$ – потенціал з'єднання, який стимулює з'єднання між різними конфігураціями.

14.1. *Потенціал розширення* зазвичай визначається як функція, що стимулює вибір конфігурацій, що знаходяться на межі вже досліджених областей:

$$U_{exp}(q) = -\alpha \cdot boundary_{measure}(q), \quad (14.2)$$

де α – коефіцієнт, що визначає вагу розширення, а $boundary_{measure}(q)$ – міра, яка оцінює, наскільки конфігурація q знаходиться на межі дослідженої області.

14.2. *Потенціал з'єднання* зазвичай визначається як функція, яка стимулює з'єднання між конфігураціями, що знаходяться на відстані одна від одної:

$$U_{conn}(q) = \beta \cdot \sum_{i=1}^{n} distance\ (q, q_i), \quad (14.3)$$

де β – коефіцієнт, що визначає вагу з'єднання, $distance(q, q_i)$ – відстань між конфігурацією q_i іншими конфігураціями q_i, n – кількість конфігурацій, з якими потрібно з'єднатися.

14.3. *Загальна ЦФ* для алгоритму Expansive Configuration Spaces має вигляд:

$$\text{Minimize } U_{total}(q) = -\alpha \cdot boundary_{measure}(q) + \beta \cdot \sum_{i=1}^{n} distance\ (q, q_i). \quad (14.4)$$

Таким чином, ЦФ (14.4) алгоритму Expansive Configuration Spaces зазвичай спрямована на мінімізацію відстані або часу, необхідного для досягнення цільової конфігурації, і може включати різні компоненти вартості. Складність цільової функції залежить від розміру конфігураційного простору, кількості перешкод, вибору евристики та методів випадкового зразкування. Цей підхід дозволяє ефективно досліджувати релевантні ділянки простору, що робить його корисним для різних застосувань у робототехніці.

15. Алгоритм *Probabilistic Roadmap* (PRM) використовує випадкове зразкування для побудови графа, що представляє можливі шляхи в просторі і використовується для планування траєкторії МР у складних середовищах. Алгоритм ефективний у високовимірних просторах, але має високі вимоги до обчислювальних ресурсів і потребує налаштування параметрів [34, 35].

ЦФ для алгоритму Probabilistic Roadmap не є традиційною цільовою функцією, як у методах штучного потенційного поля. Натомість, PRM використовує графові алгоритми для пошуку найкоротшого шляху в побудованому графі. Основна мета алгоритму PRM знайти шлях, який мінімізує відстань або іншу метрику між початковою та цільовою конфігураціями.

Враховуючи, що *основні компоненти* алгоритму PRM складаються з фази *побудови* (Construction Phase) і фази *запиту* (Query Phase), ЦФ для алгоритму PRM може бути виражена як задача мінімізації відстані в графі:

$$\text{Minimize } d_{\text{total}} = \sum_{(q_i,q_j)\in P} d\left(q_i, q_j\right), \quad (15.1)$$

де d_{total} – загальна відстань шляху P від початкової конфігурації q_{start} до цільової конфігурації q_{goal}, $\left(q_i, q_j\right)$ – ребро графу між конфігураціями q_i та q_j, $d\left(q_i, q_j\right)$ – відстань між конфігураціями q_i та q_j.

Така функція мінімізує загальну відстань шляху в графі, що дозволяє МР ефективно планувати траєкторію від початкової до цільової конфігурації, уникаючи перешкод

Таким чином, ЦФ (15.1) алгоритму Probabilistic Roadmap спрямована на мінімізацію довжини або часу шляху, а складність залежить від кількості зразків, перевірки на колізії та обраного алгоритму пошуку найкоротшого шляху. Завдяки своїй гнучкості та ефективності, PRM широко використовується для вирішення задач планування шляху в різних робототехнічних застосуваннях.

16. Алгоритм *Randomized Roadmap Method* (RRM) є одним із методів планування траєкторії для АМР у складних середовищах. Він використовує випадкові зразки для побудови

графа (roadmap), який представляє можливі шляхи від початкової точки до цілі. Ефективний у складних просторах і високовимірних середовищах, але має високі вимоги до обчислювальних ресурсів і потребує налаштування параметрів [36, 37, 38].

ЦФ для цього алгоритму включає мінімізацію відстані або часу проходження між початковою і кінцевою точками через побудований граф.

Загальна ЦФ для алгоритму Randomized Roadmap Method може бути виражена як:

$$\text{Minimize } C_{\text{total}}(q_{start}, q_{goal}) = \sum_{(q_i,q_j)\in P} c(q_i, q_j), \tag{16.1}$$

де $C_{total}(q_{start}, q_{goal})$ – загальна вартість шляху від початкової точки q_{start} до цільової точки q_{goal}, P– послідовність з'єднань (шлях) від q_{start} до q_{goal}, $c(q_i, q_j)$ – вартість переходу між двома конфігураціями q_i і q_j.

Вартість переходу між двома конфігураціями зазвичай визначається як евклідова відстань між ними:

$$c(q_i, q_j) = \| q_i - q_j \|. \tag{16.2}$$

Алгоритм складається з двох основних фаз, фази побудови графа (Roadmap Construction) і фази запиту (Query Phase).

Загальна ЦФ для алгоритму Randomized Roadmap Method має вигляд:

$$\text{Minimize } C_{total}(q_{start}, q_{goal}) = \sum_{(q_i,q_j)\in P} c \| q_i - q_j \|. \tag{16.3}$$

Таким чином, ЦФ (16.3) алгоритму Randomized Roadmap Method зазвичай включає мінімізацію відстані або часу, а її складність залежить від розміру конфігураційного простору, щільності перешкод та кількості вибірок. Завдяки своїй гнучкості та ефективності, RRM широко використовується в робототехніці та інших областях, де необхідно вирішувати задачі планування руху.

17. Алгоритм *Lazy Probabilistic Roadmap* (Lazy PRM) є варіантом алгоритму Probabilistic Roadmap (PRM), який відкладає перевірку на зіткнення до моменту, коли це необхідно для відповіді на запит. Це зменшує час виконання, але можливі проблеми з масштабованістю та необхідність налаштування параметрів [39, 40].

ЦФ для алгоритму Lazy PRM може бути виражена як оптимізаційна задача, яка мінімізує загальну вартість шляху з урахуванням відстані між конфігураціями та перевірок на зіткнення.

Загальна ЦФ для алгоритму Lazy PRM має вираз:

$$\text{Minimize } C_{\text{total}}(q) = \sum_{(q_i,q_j)\in P} \left(d(q_i, q_j) + \lambda \cdot c(q_i, q_j)\right), \tag{17.1}$$

де $C_{total(q)}$ – загальна вартість шляху, P – шлях, що складається з послідовності конфігурацій q_i, $d(q_i, q_j)$ – відстань між конфігураціями q_i та q_j, $c(q_i, q_j)$ – вартість перевірки на зіткнення між конфігураціями q_i та q_j, λ – ваговий коефіцієнт, що визначає вплив вартості перевірки на зіткнення.

Враховуючи, що *відстань між конфігураціями,* $\mathrm{q_i}$ та $\mathrm{q_j}$ визначається як евклідова відстань,

$$d(q_i, q_j) = \| q_i - q_j \|, \tag{17.2}$$

а *вартість перевірки на зіткнення* $\mathrm{c(q_i, q_j)}$ може бути визначена як бінарна функція, яка приймає значення 1, якщо перевірка на зіткнення необхідна, і 0, якщо перевірка непотрібна:

$$c(q_i, q_j) = \begin{cases} 1, & \text{якщо перевірка на зіткнення необхідна} \\ 0, & \text{якщо перевірка на зіткнення не потрібна} \end{cases}. \tag{17.3}$$

Враховуючи (17.2) і (17.3), *загальна ЦФ* (20.1) для алгоритму Lazy PRM буде мати вираз:

$$\text{Minimize } C_{\text{total}}(q) = \sum_{(q_i,q_j)\in P} \left(\| q_i - q_j \| + \lambda \cdot c(q_i, q_j)\right). \tag{17.4}$$

Таким чином, ЦФ (17.4) в Lazy PRM спрямована на мінімізацію загальної вартості шляху, а складність алгоритму залежить від кількості вершин та ребер у графі. Основна

перевага алгоритму полягає в мінімізації кількості перевірок на зіткнення, що дозволяє зменшити час виконання алгоритму.

18. Алгоритм *Gaussian Sampling for PRM* є варіацією стандартного PRM. Модифікація пов'язана з можливістю краще покривати складні області простору, зменшуючи кількість необхідних зразків. Основні переваги включають ефективність у складних просторах, але алгоритм має високі вимоги до обчислювальних ресурсів і потребує налаштування параметрів [41]. Це дозволяє більш ефективно досліджувати складні області простору, особливо поблизу перешкод.

Враховуючи, що *основні компоненти* алгоритму *Gaussian Sampling for PRM* включають етапи, *вибір* і *перевірка зразків*, *побудову графу* й *пошук шляху*, ЦФ для алгоритму формалізовано може бути виражена як задача мінімізації відстані в графі, з урахуванням гауссового розподілення для вибору зразків:

$$\text{Minimize } d_{\text{total}} = \sum_{(q_i,q_j)\in P} d(q_i, q_j), \tag{18.1}$$

де d_{total} – загальна відстань шляху P від початкової конфігурації q_{start} до цільової конфігурації q_{goal}, (q_i, q_j) – ребро графу між конфігураціями q_i та q_j, $d(q_i, q_j)$ – відстань між конфігураціями q_i та q_j.

Для вибору зразків використовується гауссове розподілення. Спочатку виконується генерація випадкового зразка q1 у просторі конфігурацій й генерація другого зразка σ^2 з гауссового розподілення з центром у q_1:

$$q_2 \sim N(q_1, \sigma^2), \tag{18.2}$$

де $N(q_1, \sigma^2)$ – гауссове розподілення з середнім q_1 і дисперсією σ^2.

Загальна ЦФ для Gaussian Sampling for PRM буде мати вираз:

$$C_r = \{p \in C_{free} \mid \|p - q\| < d \wedge q \in \mathcal{IB} \cup \mathcal{OB}\}. \tag{18.3}$$

Таким чином, використання цільовою функцією (18.3) алгоритму Gaussian Sampling for PRM гауссового вибіркового розподілення, дозволяє краще охоплювати складні області простору, що підвищує ймовірність знаходження оптимального шляху. Хоча обчислювальна та просторова складність має завищені показники, загальна ефективність алгоритму часто виправдовує ці витрати.

19. Алгоритм *Halton Sampling for PRM* є варіацією класичного PRM, де для генерації зразків у конфігураційному просторі використовує послідовність Халтона для зразкування простору конфігурацій. Послідовність Халтона є низькодисперсійною послідовністю, яка забезпечує більш рівномірне покриття простору порівняно з випадковим зразкуванням. Це забезпечує рівномірний розподіл зразків, що зменшує кількість необхідних зразків і покращує ефективність алгоритму. Основні переваги включають рівномірний розподіл зразків і зменшення кількості зразків, але алгоритм складний у реалізації та має високі вимоги до обчислювальних ресурсів [42, 43].

Враховуючи, що *основні компоненти* алгоритму *Halton Sampling for PRM* включають етапи *генерації зразків за допомогою послідовності Халтона, перевірку на прохідність, побудова графа і пошук шляху, ЦФ* для алгоритму може бути виражена як задача мінімізації загальної вартості шляху в графі:

$$\text{Minimize } C_{\text{total}}(q_{start}, q_{goal}) = \sum_{(q_i,q_j)\in P} c(q_i, q_j), \tag{19.1}$$

де $C_{total}(q_{start}, q_{goal})$ – загальна вартість шляху від початкової точки q_{start} до цільової точки q_{goal}, P – послідовність з'єднань (шлях) від q_{start} до q_{goal}, $c(q_i, q_j)$ – вартість переходу між двома конфігураціями q_i і q_j.

Враховуючи, що вартість переходу між двома конфігураціями зазвичай визначається як евклідова відстань між ними:

$$c(q_i, q_j) = \| q_i - q_j \|, \tag{19.2}$$

а послідовність Халтона генерується за допомогою радикальної оберненої функції з різними базами для кожного виміру:

$$H(i) = \left(\phi_{b_1}(i), \phi_{b_2}(i), \dots, \phi_{b_d}(i)\right), \tag{19.3}$$

де $H(i)$ – i-та точка послідовності Халтона, $\phi_{b_k}(i)$ – радикальна обернена функція з базою b_k для k-го виміру, d – кількість вимірів у конфігураційному просторі.

Загальний вигляд цільової функції для *Halton Sampling for PRM* отримає вигляд:

$$\text{Minimize } C_{total}(q_{start}, q_{goal}) = \sum_{(q_i,q_j)\in P} c \parallel q_i - q_j \parallel. \tag{19.4}$$

Таким чином, ЦФ (19.4) алгоритму *Halton Sampling for PRM* завдяки своїй здатності генерувати рівномірно розподілені точки з низькою дискретністю, забезпечує краще покриття конфігураційного простору та підвищує ефективність алгоритму планування шляху.

20. Алгоритм D* (Dynamic A*) це інкрементальний пошуковий алгоритм, який використовує евристики, є розширенням алгоритму A*, призначеним для планування траєкторій у динамічних середовищах, де можуть змінюватися умови, такі як поява нових перешкод. Він підходить для частково відомих та змінних середовищ, але має високі вимоги до обчислювальних ресурсів і складний у реалізації [44, 45, 46].

Основна мета алгоритму D*, знайти найкоротший шлях від початкової точки до цільової, враховуючи зміни в середовищі в реальному часі.

ЦФ для алгоритму D* може бути виражена як задача мінімізації загальної вартості шляху від початкової конфігурації q_{start} до цільової конфігурації q_{goal}:

$$\text{Minimize } C_{\text{total}}(q_{start}, q_{goal}) = \sum_{(q_i,q_j)\in P} c(q_i, q_j), \tag{20.1}$$

де $C_{total}(q_{start}, q_{goal})$ – загальна вартість шляху від початкової точки q_{start} до цільової точки q_{goal}, P – послідовність з'єднань (шлях) від q_{start} до q_{goal}, $c(q_i, q_j)$ – вартість переходу між двома конфігураціями q_i і q_j.

Вартість переходу між двома конфігураціями зазвичай визначається як евклідова відстань між ними або інша метрика, що враховує особливості середовища:

$$c(q_i, q_j) = \parallel q_i - q_j \parallel. \tag{20.2}$$

З урахуванням виразу (20.2) *ЦФ* для алгоритму D* отримаємо вираз:

$$\text{Minimize } C_{total}(q_{start}, q_{goal}) = \sum_{(q_i,q_j)\in P} \left(\parallel q_i - q_j \parallel + h(q_i, q_{goal})\right), \tag{20.3}$$

де $h(q_i, q_{goal})$ – евристична функція, що оцінює вартість найкоротшого шляху від конфігурації q_j до цільової конфігурації q_{goal} .

А з урахуванням, що *евристична функція* $h(q_j, q_{goal})$ зазвичай визначається як евклідова відстань або *мангеттенська відстань* між конфігураціями:

$$h(q_j, q_{goal}) = \parallel q_j - q_{goal} \parallel. \tag{20.4}$$

Загальна ЦФ для алгоритму D* набуває вигляду:

$$\text{Minimize } C_{total}(q_{start}, q_{goal}) = \sum_{(q_i,q_j)\in P}(\parallel q_i - q_j \parallel + \parallel q_j - q_{goal} \parallel). \tag{20.5}$$

Таким чином, алгоритм Dynamic A* використовує адаптивну цільову функцію (20.5) для ефективного знаходження оптимальних шляхів у змінних умовах. Його складність може варіюватися залежно від конкретного застосування та умов середовища, але в цілому він пропонує значні переваги в адаптивності та ефективності порівняно з класичними методами.

21. Алгоритми цілеспрямованого та випадкового пошуку (*Goal-directed and Randomized Search*) поєднує цілеспрямований пошук, який спрямовує пошук у бік цільової точки, та випадковий пошук, який забезпечує дослідження простору конфігурацій. Використовується для вирішення задач оптимізації, де необхідно знайти оптимальне рішення шляхом мінімізації або максимізації цільової функції. Це дозволяє ефективно працювати у великих просторах, поєднуючи переваги обох підходів. Основні переваги включають ефективність у великих

просторах, але алгоритм складний у реалізації та потребує налаштування параметрів [47, 48, 49].

ЦФ виражена як математична формула, яка визначає мету оптимізації.

21.1. *Цілеспрямований пошук (Goal-directed Search),* спрямований на досягнення конкретної мети, і ЦФ для такого алгоритму може бути виражена як:

$$\text{Strong (Minimize} \vee \text{Maximize } f(x)), \tag{21.1}$$

де $f(x)$ – ЦФ, яку необхідно мінімізувати або максимізувати, а x – набір змінних, що визначають стан системи або рішення задачі

21.2. *Випадковий пошук (Randomized Search),* використовує випадкові комбінації параметрів для знаходження оптимального рішення. ЦФ для випадкового пошуку може бути виражена аналогічно:

$$\text{Rand (Minimize} \vee \text{Maximize } f(x)), \tag{21.2}$$

де $f(x)$ – ЦФ, яку необхідно мінімізувати або максимізувати, а x – набір випадково обраних змінних.

Таким чином, ЦФ для алгоритмів цілеспрямованого та випадкового пошуку може бути виражена як математична формула (21.1), (21.2), що мінімізує або максимізує певну функцію $f(x)$, залежно від конкретної задачі оптимізації.

22. Алгоритм *SANDROS* (Search And Nonuniform Dynamic Resolution Optimization Strategy) використовує комбінацію ієрархічного, нерівномірного багаторівневого та найкращого пошуку для знаходження майже оптимального рішення. Основні переваги включають високу ефективність у складних середовищах та високу точність, але алгоритм складний у реалізації та має високі вимоги до обчислювальних ресурсів [50].

ЦФ для цього алгоритму мінімізує або максимізує певний параметр, пов'язаний з оптимізацією. Нажаль автори дослідження, для алгоритму SANDROS не була явно вказана конкретна ЦФ. Тому враховуючи, що загальна форма цільової функції для оптимізаційних алгоритмів може бути виражена як:

$$\text{Minimize } f(x), \tag{22.1}$$

де $f(x)$ – це ЦФ, яку потрібно мінімізувати, а x – вектор змінних, що оптимізуються.

Автор цього дослідження пропонує вважати, що ЦФ для алгоритму SANDROS має більш специфічні властивості залежно від конкретної задачі. Наприклад, якщо задача полягає в мінімізації відхилення потужності антен, ЦФ може бути виражена як:

$$\text{Minimize } \max_i \left|P_i - P_{target}\right|, \tag{22.2}$$

де P_i – потужність і-тої антени, а P_{target} – цільова потужність.

Враховуючи (22.3) загальна ЦФ мінімізації загальної потужності отримає вигляд:

$$\text{Minimize } \sum_{i=1}^{n} \left|P_i - P_{target}\right|, \tag{22.3}$$

де n – загальна кількість антен.

Таким чином, ЦФ (22.3) алгоритму SANDROS може бути складною і включати кілька компонентів, що враховують різні аспекти руху МР. Складність цільової функції залежить від розмірності простору, кількості перешкод і динамічності середовища. Незважаючи на це, SANDROS демонструє високу ефективність у вирішенні задач планування шляхів завдяки своєму динамічному графовому пошуку.

23. Алгоритм *Artificial Potential Field* (APF) використовується для планування траєкторії МР, де робот використовує потенційні поля для планування шляху, де цільова точка притягує, а перешкоди відштовхують робота. Основні переваги включають простоту реалізації та швидкість обчислень, але алгоритм може застрягати в локальних мінімумах і не підходить для складних середовищ [29, 51].

ЦФ для цього алгоритму включає компоненти, які враховують як притягувальні, так і відштовхувальні потенціали.

Загальний формалізований вид цільової функції для алгоритму APF має вигляд:

$$\text{Minimize } U_{total}(q) = U_{att}(q) + U_{rep}(q), \tag{23.1}$$

де $U_{total}(q)$ – загальний потенціал у точці q, $U_{att}(q)$ – притягувальний потенціал, який притягує робота до цільової точки, $U_{rep}(q)$ – відштовхувальний потенціал, який відштовхує МР від перешкод.

23.1. *Притягуючий потенціал* зазвичай визначається як квадратична функція відстані до цілі:

$$U_{att}(q) = \frac{1}{2} k_{att} \left\| q - q_{goal} \right\|^2, \tag{23.2}$$

де k_{att} – коефіцієнт привабливості, q – поточне положення МР, q_{goal} – положення цільової точки.

23.2. *Відштовхувальний потенціал* зазвичай визначається як функція, яка швидко зростає при наближенні до перешкоди:

$$U_{rep}(q) = \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\|q - q_{obs}\|} - \frac{1}{d_0} \right)^2 & if \ \|q - q_{obs}\| \le d_0, \\ 0 & if \ \|q - q_{obs}\| > d_0. \end{cases}, \tag{23.3}$$

де k_{rep} – коефіцієнт відштовхування, q_{obs} – положення перешкоди, d_0 – порогова відстань, за якою відштовхувальний потенціал дорівнює нулю.

23.3. *Загальна ЦФ* для алгоритму Artificial Potential Field має вигляд як:

$$\text{Minimize } U_{total}(q) = \frac{1}{2} k_{att} \left\| q - q_{goal} \right\|^2 + \sum_{i=1}^{m} \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\left\| q - q_{obs_i} \right\|} - \frac{1}{d_0} \right)^2 & if \ \left\| q - q_{obs_i} \right\| \le d_0, \\ 0 & if \ \left\| q - q_{obs_i} \right\| > d_0. \end{cases}, \tag{23.4}$$

де m – кількість перешкод.

Складність алгоритму APF можна розглядати з кількох точок зору:

– Обчислювальна складність. APF має низьку обчислювальну складність, оскільки обчислення потенціалів і градієнтів є досить простими і можуть бути виконані в реальному часі. Це робить алгоритм привабливим для застосувань, де потрібна швидка реакція, наприклад, у МР.

– Проблеми локальних мінімумів: Однією з основних проблем APF є можливість потрапляння АМР в локальні мінімуми потенційного поля, де він може застрягти і не досягти цілі. Це обмежує застосування алгоритму в складних середовищах з багатьма перешкодами.

Таким чином, ЦФ (23.4) алгоритму Artificial Potential Field складається з притягувальних (23.2) і відштовхувальних (23.3) потенціалів, що дозволяє МР рухатися до цілі, уникаючи перешкод. Однак, основною проблемою є можливість потрапляння в локальні мінімуми, що обмежує його застосування в складних середовищах. Модифікації алгоритму можуть допомогти вирішити ці проблеми і покращити його ефективність.

24. Алгоритм *Dynamic Artificial Potential Field* (DAPF) є модіфікованою версією алгоритму Artificial Potential Field, що використовує динамічні потенційні поля для планування шляху, де цільова точка притягує, а перешкоди відштовхують АМР і використовується для планування траєкторії МР у динамічних середовищах, де перешкоди можуть змінювати своє положення з часом. Основні переваги включають простоту реалізації та швидкість обчислень, але алгоритм може застрягати в локальних мінімумах і не підходить для складних середовищ [51].

ЦФ для цього алгоритму включає компоненти, які враховують як притягувальні, так і відштовхувальні потенціали, щоб забезпечити безпечний і ефективний рух до цілі.

Загальний вигляд *цільової функції* алгоритму Dynamic Artificial Potential Field:

$$\text{Minimize } U_{total}(q) = U_{att}(q) + U_{rep}(q), \tag{24.1}$$

де $U_{total}(q)$ – загальний потенціал у точці q, $U_{att}(q)$ – притягуючий потенціал, який притягує робота до цільової точки, $U_{rep}(q)$ – відштовхувальний потенціал, який відштовхує робота від перешкод.

24.1. *Притягувальний потенціал* зазвичай визначається як квадратична функція відстані до цілі:

$$U_{att}(q) = \frac{1}{2} k_{att} \left\| q - q_{goal} \right\|^2, \tag{24.2}$$

де k_{att} – коефіцієнт привабливості, q – поточне положення МР, q_{goal} – положення цільової точки.

24.2. *Відштовхувальний потенціал* зазвичай визначається як функція, яка швидко зростає при наближенні до перешкоди:

$$U_{rep}(q) = \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\|q - q_{obs}\|} - \frac{1}{d_0} \right)^2 & if \ \|q - q_{obs}\| \le d_0, \\ 0 & if \ \|q - q_{obs}\| > d_0. \end{cases}, \tag{24.3}$$

де k_{rep} – коефіцієнт відштовхування, q_{obs} – положення перешкоди, d_0 – порогова відстань, за якою відштовхувальний потенціал дорівнює нулю.

24.3. *Динамічний компонент.* Для врахування динамічних змін у середовищі, ЦФ може включати додатковий елемент, що враховує швидкість зміни положення перешкоди:

$$U_{dyn}(q, t) = \alpha \left\| \dot{q}_{obs}(t) \right\|, \tag{24.4}$$

де α – коефіцієнт, що визначає вплив динамічних змін, $\dot{q}_{obs}(t)$ – швидкість зміни положення перешкоди в момент часу t.

24.4. Остаточна ЦФ з урахуванням динамічного компонента, отримує наступний вираз:

$$\text{Minimize } U_{total}(q, t) = \frac{1}{2} k_{att} \left\| q - q_{goal} \right\|^2 + \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\|q - q_{obs}\|} - \frac{1}{d_0} \right)^2 & if \ \|q - q_{obs}\| \le d_0, \\ 0 & if \ \|q - q_{obs}\| > d_0. \end{cases} + \alpha \left\| \dot{q}_{obs}(t) \right\| . \tag{24.5}$$

Таким чином, ЦФ (24.5) алгоритму Dynamic Artificial Potential Field складається з атрактивних (24.2), (24.3) та репульсивних (24.4) компонентів, що дозволяє АМР ефективно досягати цілі, уникаючи перешкод. Основні виклики включають вирішення проблеми локальних мінімумів та високу обчислювальну складність, що компенсується адаптивністю та здатністю до роботи в реальному часі.

25. Алгоритм *Improved Artificial Potential Field* (IAPF) є вдосконаленою версією алгоритму штучного потенційного поля, який вирішує деякі його недоліки. Покращення включають використання додаткових методів для уникнення проблем з локальними мінімумами та підвищення ефективності уникнення перешкод [52, 53, 54].

ЦФ для цього алгоритму включає як привабливі, так і відштовхувальні потенціали, а також додаткові компоненти для уникнення локальних мінімумів.

Загальна ЦФ для алгоритму Improved Artificial Potential Field має вираз:

$$\text{Minimize } U_{total}(q) = U_{att}(q) + U_{rep}(q) + U_{improved}(q), \tag{25.1}$$

де $U_{total}(q)$ – загальний потенціал у точці q, $U_{att}(q)$– притягувальний потенціал, який притягує робота до цільової точки, $U_{rep}(q)$ – відштовхувальний потенціал, що відштовхує робота від перешкод, $U_{improved}(q)$ – додатковий компонент для покращення алгоритму.

25.1. *Притягувальний потенціал* зазвичай визначається як квадратична функція відстані до цілі:

$$U_{att}(q) = \frac{1}{2} k_{att} \left\| q - q_{goal} \right\|^2, \tag{25.2}$$

де k_{att} – коефіцієнт притягування, q – поточне положення МР, q_{goal} – положення цільової точки.

25.2. *Відштовхувальний потенціал* зазвичай визначається як функція, яка швидко зростає при наближенні до перешкоди:

$$U_{rep}(q) = \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\|q - q_{obs}\|} - \frac{1}{d_0} \right)^2 & if \ \|q - q_{obs}\| \le d_0, \\ 0 & if \ \|q - q_{obs}\| > d_0. \end{cases} \quad (25.3)$$

де k_{rep} – коефіцієнт відштовхування, q_{obs} – положення перешкоди, d_0 – порогова відстань, за якою відштовхувальний потенціал дорівнює нулю.

25.3. Для уникнення локальних мінімумів і покращення досяжності цілі, може бути доданий *додатковий компонент для покращення алгоритму*, такі як, використання віртуальних цілей або модифікація відштовхувального потенціалу:

$$U_{improved}(q) = \sum_{i=1}^{m} \frac{1}{2} k_{virt} \left\| q - q_{virt,i} \right\|^2, \quad (25.4)$$

де k_{virt} – коефіцієнт притягування до віртуальних цілей, $q_{virt,i}$ – положення віртуальної цілі і, m – кількість віртуальних цілей.

25.4. *Загальна ЦФ з урахуванням покращень* може бути виражена як:

$$\text{Minimize } U_{total}(q) = \frac{1}{2} k_{att} \left\| q - q_{goal} \right\|^2 + \sum_{j=1}^{m} \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\left\| q - q_{obs_j} \right\|} - \frac{1}{d_0} \right)^2 & if \ \|q - q_{obs_i}\| \le d_0, \\ 0 & if \ \|q - q_{obs_i}\| > d_0. \end{cases} + \sum_{i=1}^{m} \frac{1}{2} k_{virt} \left\| q - q_{virt,i} \right\|^2. \quad (25.5)$$

Таким чином, алгоритм Improved Artificial Potential Field пропонує значні покращення у порівнянні з класичним APF (24.5) завдяки модифікаціям цільової функції (25.5) та додатковим евристикам (25.4). Ці вдосконалення приводять до збільшення обчислювальної складності, вони забезпечують більш ефективне планування траєкторій та уникнення перешкод, що робить IAPF більш придатним для складних і динамічних середовищ.

26. Алгоритм *на основі штучного потенційного поля з використанням мережі підцілей* (Artificial Potential Field Based Subgoal Network) використовує потенційні поля для створення мережі підцілей, що допомагає МР уникати перешкод, є вдосконаленням традиційного методу штучного потенційного поля (APF), який використовується для планування траєкторії МР. Цей метод допомагає уникнути проблеми локальних мінімумів та забезпечує більш гладкі та ефективні траєкторії. Основні переваги включають простоту реалізації та швидкість обчислень, але алгоритм може застрягати в локальних мінімумах і не підходить для складних середовищ [55, 56, 57].

ЦФ для алгоритму Artificial Potential Field Based Subgoal Network може бути виражена як сума потенційних функцій, що включають притягувальні та відштовхувальні компоненти, а також додаткові компоненти для підцілей. Формула може бути записана наступним чином:

$$U(x) = U_{att}(x) + U_{rep}(x) + U_{subgoal}(x), \quad (26.1)$$

де U_x – загальний потенціал у точці x, $U_{att}(x)$ – привабливий потенціал, що притягує робота до цільової точки, $U_{rep}(x)$ – відштовхувальний потенціал, що відштовхує робота від перешкод, $U_{subgoal}(x)$ – додатковий потенціал, що враховує підцілі для уникнення локальних мінімумів та оптимізації траєкторії.

З урахуванням, що притягувальний потенціал $U_{att}(x)$ може бути визначений як:

$$U_{att}(x) = \frac{1}{2} k_{att} \left\| x - x_{goal} \right\|^2, \quad (26.2)$$

де k_{att} – коефіцієнт привабливості, і x_{goal} – координати цільової точки.

Відштовхувальний потенціал $U_{rep}(x)$ може бути визначений як:

$$U_{rep}(x) = \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\|x - x_{obs}\|} - \frac{1}{d_0} \right)^2 & if \ \|x - x_{obs}\| \le d_0, \\ 0 & if \ \|x - x_{obs}\| > d_0. \end{cases} \quad (26.3)$$

де k_{rep} – коефіцієнт відштовхування, x_{obs} – координати перешкоди, d_0 – порогова відстань, на якій відштовхувальний потенціал починає діяти.

Додатковий потенціал підцілей $U_{subgoal}(x)$ може бути визначений як:

$$U_{subgoal}(x) = \sum_{i=1}^{n} \frac{1}{2} k_{subgoal} \left\| x - x_{subgoal_i} \right\|^2, \quad (26.4)$$

де $k_{subgoal}$ – коефіцієнт привабливості підцілей, $x_{subgoal_i}$ – координати i-ї підцілі, n – кількість підцілей.

Враховуючи всі необхідні компоненти для ефективного планування траєкторії АМР з використанням мережі підцілей, отримаємо що, *загальна ЦФ* для алгоритму Artificial Potential Field Based Subgoal Network отримає наступний вигляд:

$$U(x) = \frac{1}{2} k_{att} \left\| x - x_{goal} \right\|^2 + \sum_{i=1}^{n} \frac{1}{2} k_{subgoal} \left\| x - x_{subgoal_i} \right\|^2 + \\ + \sum_{j=1}^{m} \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\left\| x - x_{obs_j} \right\|} - \frac{1}{d_0} \right)^2 & if \ \left\| x - x_{obs_j} \right\| \le d_0, \\ 0 & if \ \left\| x - x_{obs_j} \right\| > d_0. \end{cases}, \quad (26.5)$$

де m – кількість перешкод.

Таким чином, ЦФ (26.5) алгоритму Artificial Potential Field Based Subgoal Network складається з атракційних та репульсивних компонент, а її складність визначається обчислювальними витратами, проблемами з локальними мінімумами та здатністю адаптуватися до змін у середовищі. Алгоритм поєднує переваги потенційних полів та субцілей, що дозволяє ефективно уникати перешкод і знаходити оптимальний шлях до цілі.

27. Алгоритм *динамічного планування шляху з підцілями* (Dynamic Subgoal Path Planner) генерує підцілі для обходу перешкод у динамічних середовищах з використанням підцілей для побудови оптимального шляху в динамічних середовищах. Алгоритм дозволяє швидко ухилятися від локальних мінімумів і ефективний у динамічних середовищах, але має високі вимоги до обчислювальних ресурсів і складний у реалізації [58].

ЦФ для такого алгоритму зазвичай включає кілька компонентів, таких як мінімізація відстані, уникнення перешкод та забезпечення плавності шляху.

ЦФ для Dynamic Subgoal Path Planner може бути виражена як:

$$\text{Minimize } J(x) = \alpha \cdot d(x) + \beta \cdot c(x) + \gamma \cdot s(x), \quad (27.1)$$

де $J(x)$ – загальна ЦФ, $d(x)$ – функція відстані, яка вимірює загальну відстань шляху, $c(x)$ – функція вартості, яка враховує вартість проходження через певні області (наприклад, уникнення перешкод), $s(x)$ – функція плавності, яка забезпечує плавність шляху, α, β, γ – вагові коефіцієнти, що визначають важливість кожного компонента.

До компонентів цільової функції відносяться:

27.1. Функція відстані $d(x)$:

$$d(x) = \sum_{i=1}^{n-1} \| x_{i+1} - x_i \|, \quad (27.2)$$

де x_i – координати точки на шляху, а n – кількість точок на шляху.

27.2. Функція вартості $c(x)$:

$$c(x) = \sum_{i=1}^{n} cost\ (x_i), \quad (27.3)$$

де $cost(x_i)$ – вартість проходження через точку x_i, яка може включати уникнення перешкод.

27.3. Функція плавност $s(x)$:

$$s(x) = \sum_{i=2}^{n-1} \| x_{i-1} - 2x_i + x_{i+1} \|, \quad (27.4)$$

де x_{i-1}, x_i, x_{i+1} – послідовні точки на шляху, що забезпечують плавність.

Алгоритм включає *динамічне генерування підцілей*, що допомагає уникати локальних мінімумів і забезпечує більш ефективний пошук шляху. Підцілі можуть бути визначені на основі поточного стану та цільового стану, а також враховувати динамічні зміни в середовищі.

З урахування (27.2, 27.3, 27,4) ЦФ (27.1) отримає вигляд:

$$\text{Minimize } J(x) = \alpha \cdot \sum_{i=1}^{n-1} \|x_{i+1} - x_i\| + \beta \cdot \sum_{i=1}^{n} cost\ (x_i) + \gamma \cdot \sum_{i=2}^{n-1} \|x_{i-1} - 2x_i + x_{i+1}\|. \quad (27.5)$$

Таким чином, ЦФ (27.5) для Dynamic Subgoal Path Planner включає мінімізацію відстані, вартості та забезпечення плавності шляху, що дозволяє ефективно планувати шлях у динамічних середовищах.

28. Алгоритм *ієрархічного планування руху* (Hierarchical Motion Planner) використовує багаторівневий підхід для вирішення задач планування траєкторій, де кожен рівень відповідає за різні аспекти задачі. Алгоритм підходить для роботи у високовимірних просторах, але має високі вимоги до обчислювальних ресурсів і складний у налаштуванні параметрів [59–61].

ЦФ для такого алгоритму може включати кілька компонентів, таких як мінімізація відстані, уникнення зіткнень, оптимізація енерговитрат тощо.

ЦФ для ієрархічного планування руху може бути виражена як:

$$\text{Minimize } J = \sum_{i=1}^{n} w_i \cdot f_i(x), \quad (28.1)$$

де J – загальна ЦФ, $f_i(x)$ – окремі компоненти цільової функції, що відповідають за різні аспекти задачі (наприклад, відстань, енерговитрати, уникнення зіткнень), w_i – вагові коефіцієнти, що визначають важливість кожного компонента, x – набір змінних, що визначають стан системи або траєкторію.

До компонентів цільової функції відносяться:

28.1. Мінімізація відстані:

$$f_1(x) = \int_0^T \|\dot{x}(t)\| dt. \quad (28.2)$$

28.2. Уникнення зіткнень:

$$f_2(x) = \sum_{j=1}^{m} \phi\left(d_j(x)\right). \quad (28.3)$$

де $\phi\left(d_j(x)\right)$ – функція штрафу за наближення до перешкод, $d_j(x)$ – відстань до j-ї перешкоди.

28.3. Оптимізація енерговитрат:

$$f_3(x) = \int_0^T P\big(x(t), \dot{x}(t)\big) dt, \quad (28.4)$$

де $P\big(x(t), \dot{x}(t)\big)$ – потужність, що витрачається на рух у момент часу t.

Об'єднавши всі компоненти, отримаємо повну цільову функцію:

$$\text{Minimize } J = w_1 \int_0^T \|\dot{x}(t)\| dt + w_2 \sum_{j=1}^{m} \phi\left(d_j(x)\right) + \text{w}_3 \int_0^T P\big(x(t), \dot{x}(t)\big) dt, \quad (28.5)$$

де w_1, w_2, w_3 – вагові коефіцієнти, що визначають важливість кожного компонента.

Таким чином**,** ЦФ (28.5) для алгоритму ієрархічного планування руху може бути виражена як лінійна комбінація окремих цільових функцій, що дозволяє враховувати різні аспекти задачі та забезпечує гнучкість і адаптивність алгоритму. При цьому функція є багатокомпонентною і враховує різні аспекти задачі, такі як мінімізація відстані, уникнення зіткнень та оптимізація енерговитрат.

29. *Двошаровий підцільовий алгоритм* (Two-Layered Subgoal) використовує два рівні для планування шляху, для розв'язання складних задач шляхом розбиття їх на підзадачі або підцілі. Основні переваги включають зменшення обчислювальної складності, але алгоритм складний у реалізації та має високі вимоги до обчислювальних ресурсів [62, 63].

ЦФ для такого алгоритму може бути виражена як математична формула, яка визначає мету оптимізації на кожному рівні ієрархії.

ЦФ для двошарового підцільового алгоритму може бути виражена як сукупність цільових функцій для кожного шару. Основна ЦФ може бути представлена як:

$$\text{Minimize } J = \sum_{i=1}^{n} w_i \cdot f_i(x), \quad (29.1)$$

де J – загальна ЦФ, n – кількість підцілей або підзадач, $f_i(x)$ – ЦФ для кожної підцілі або підзадачі, w_i – ваговий коефіцієнт для кожної підцілі або підзадачі, x – набір змінних, що визначають стан системи або рішення задачі.

У двошаровому підході ЦФ може бути розділена на два основні рівні:

29.1. *Верхній рівень* (High-Level Goals):

ЦФ для верхнього рівня може включати глобальні цілі, такі як мінімізація загального часу виконання завдання або мінімізація витрат ресурсів. Має вираз:

$$J_{high} = \sum_{j=1}^{m} w_j \cdot g_j(y), \tag{29.2}$$

де J_{high} – ЦФ верхнього рівня, m – кількість глобальних цілей, w_j – ваговий коефіцієнт для кожної глобальної цілі, $g_j(y)$ – ЦФ для кожної глобальної цілі, y – набір змінних для верхнього рівня.

29.2. *Нижній рівень* (Low-Level Subgoals):

ЦФ для нижнього рівня може включати локальні цілі, такі як уникнення перешкод або оптимізація траєкторії. Формула для нижнього рівня має вираз:

$$J_{low} = \sum_{k=1}^{p} v_k \cdot h_k(z), \tag{29.3}$$

де J_{low} – ЦФ нижнього рівня, p – кількість локальних цілей, v_k – ваговий коефіцієнт для кожної локальної цілі, $h_k(z)$ – ЦФ для кожної локальної цілі, z – набір змінних для нижнього рівня.

Загальна ЦФ для двошарового підцільового алгоритму може бути виражена формулою (29.4) як комбінація цільових функцій, з урахуванням обох рівнів

$$J = J_{high} + J_{low}. \tag{29.4}$$

Застосувавши (29.2) і (29.3) до (29.4) отримаємо розгорнуту цільову функцію:

$$J = \sum_{j=1}^{m} w_j \cdot g_j(y) + \sum_{k=1}^{p} v_k \cdot h_k(z). \tag{29.5}$$

Таким чином, ЦФ (29.5) для двошарового підцільового алгоритму включає цільові функції для кожного рівня, які можуть бути виражені як сума вагових компонентів, що мінімізують або максимізують певні параметри. Це забезпечує гнучкість і ефективність у вирішенні складних задач оптимізації.

30. Алгоритм *RRT with Local Trees* є варіацією класичного RRT, що використовує кілька локальних дерев для покращення ефективності пошуку в складних середовищах та зменшення обчислювальних витрат. Це зменшує кількість перевірок колізій, але алгоритм складний у реалізації та потребує налаштування параметрів [64, 65].

ЦФ для алгоритму RRT з локальними деревами визначає мету оптимізації руху робота, і має формалізований вигляд як:

$$\text{Minimize } J = \sum_{i=1}^{n} w_i \cdot f_i(x), \tag{30.1}$$

де J – загальна ЦФ, n – кількість локальних дерев або підзадач у алгоритмі, $f_i(x)$ – ЦФ для кожного локального дерева або підзадачі, w_i – ваговий коефіцієнт для кожного локального дерева або підзадачі, x – набір змінних, що визначають стан системи або рішення задачі

ЦФ може включати такі компоненти, як мінімізація відстані до цілі, уникнення зіткнень, мінімізація часу виконання завдання тощо.

$$J = w_1 \cdot D(x) + w_2 \cdot C(x) + w_3 \cdot T(x), \tag{30.2}$$

де $D(x)$ – функція відстані до цілі, $C(x)$ – функція уникнення зіткнень, $T(x)$ – функція часу виконання завдання, $w1, w2, w3$ – вагові коефіцієнти для відповідних функцій.

Виконання алгоритму складається з компонентів виконання цільової функції:

1. Мінімізація відстані. Основна мета алгоритму RRT з локальними деревами полягає в мінімізації загальної відстані між початковою та кінцевою точками. Це досягається шляхом додавання відстаней між послідовними точками на шляху:

$$D(x) = \sum_{i=1}^{n} d(x_i, x_{i+1}). \tag{30.3}$$

2. Уникнення перешкод. Для уникнення перешкод вводиться штрафна функція $c(x_j)$, яка додає додатковий штраф до цільової функції, якщо точка x_j знаходиться в зоні перешкод. Ваговий коефіцієнт λ визначає важливість уникнення перешкод відносно мінімізації відстані:

$$C(x) = \lambda \cdot \sum_{j=1}^{m} c(x_j). \quad (30.4)$$

3. Баланс між відстанню та безпекою. Ваговий коефіцієнт λ дозволяє налаштувати баланс між мінімізацією відстані та уникненням перешкод. Вищі значення λ призводять до більшого акценту на безпеку, тоді як нижчі значення λ зосереджуються на мінімізації відстані.

З урахуванням формул (30.2), (30.3) загальна ЦФ отримає вигляд (30.5).

$$\text{Minimize } J = \sum_{i=1}^{n}(w_1 \cdot \sum_{i=1}^{n} d(x_i, x_{i+1}) + w_2 \cdot \lambda \cdot \sum_{j=1}^{m} c(x_j) + w_3 \cdot T(x)) \ . \quad (30.5)$$

Таким чином, ЦФ (30.5) для алгоритму RRT з локальними деревами, включає мінімізацію загальної відстані між початковою та кінцевою точками, а також уникнення перешкод шляхом введення штрафної функції. Ваговий коефіцієнт λ дозволяє налаштувати баланс між цими двома цілями, забезпечуючи ефективне та безпечне планування руху МР.

31. Алгоритм *Obstacle-based RRT* використовується для планування траєкторій у середовищах з перешкодами. Алгоритм використовує перешкоди для керування зразкуванням, що дозволяє краще обходити перешкоди. Це підвищує ефективність у складних середовищах, але алгоритм складний у реалізації та потребує налаштування параметрів [66–68].

ЦФ для алгоритму Obstacle-based RRT спрямована на мінімізацію відстані до цілі, одночасно уникаючи зіткнень з перешкодами , має формалізований вигляд:

$$\text{Minimize J} = \mathrm{d}(\mathrm{x_{start}}, \mathrm{x_{goal}}) + \ \lambda \cdot \sum_{i=1}^{n} CollisionCost\ (x_i) + \mathrm{C}(x_i), \quad (31.1)$$

де J – загальна ЦФ, $d(x_{start}, x_{goal})$ – відстань між початковою точкою x_{start} та цільовою точкою x_{goal}, λ – ваговий коефіцієнт, що визначає важливість уникнення зіткнень, $CollisionCost(x_i)$ – функція вартості зіткнення для кожної точки хі на траєкторії, n – кількість точок на траєкторії.

Компоненті цільової функції алгоритму:

1. Відстань до цілі $d(x_{start}, x_{goal})$ відповідає за мінімізацію відстані між початковою та цільовою точками.

2. Вартість зіткнення $\sum_{i=1}^{n} ColissionCost(x_i)$ враховує вартість зіткнень з перешкодами на траєкторії.

3. Функція вартості зіткнення $(x_i) = \begin{cases} \infty, \text{ якщо } x_i \text{ знаходиться в зоні зіткнення} \\ 0, \text{ інакше} \end{cases}$

або більш детально:

$$\mathrm{C}(x_i) = \begin{cases} \alpha \cdot d(x_i, O), \text{ якщо } x_i \text{ знаходиться поблизу перешкоди} \\ 0, \text{ інакше} \end{cases}, \quad (31.2)$$

де α – коефіцієнт, що визначає вплив відстані до перешкоди на вартість, а $d(x_i, O)$ – відстань від вузла x_i до найближчої перешкоди О.

Таким чином, ЦФ (31.1) для алгоритму Obstacle-based RRT спрямована на мінімізацію відстані до цілі, одночасно уникаючи зіткнень з перешкодами. Вона включає дві основні компоненти: відстань між початковою та цільовою точками та вартість зіткнень на траєкторії. Ваговий коефіцієнт λ дозволяє налаштувати важливість уникнення зіткнень відносно мінімізації відстані. Такий підхід забезпечує ефективне планування траєкторій у складних середовищах з перешкодами.

32. Алгоритм *RRT-Connect* (Rapidly-exploring Random Tree Connect) використовує два дерева, які ростуть від старту та цілі, намагаючись з'єднатися між собою. Це дозволяє швидко

знаходити шлях, але можливі проблеми з масштабованістю та необхідність налаштування параметрів [69, 70]. Використовується для планування траєкторій АМР у робототехніці.

ЦФ для алгоритму RRT-Connect спрямована на мінімізацію відстані між конфігураціями та уникнення зіткнень, може бути виражена як мінімізація довжини шляху між початковою та кінцевою точками. Формально це можна записати так:

$$\text{Minimize } L(q_{start}, q_{goal}), \tag{32.1}$$

де $L(q_{start}, q_{goal})$ – довжина шляху між початковою конфігурацією q_{start} та кінцевою конфігурацією q_{goal}.

З урахуванням функції відстані між конфігураціями x_i та x_{i+1}, ЦФ для алгоритму RRT-Connect отримає наступний вираз:

$$Minimize\ J = \sum_{i=1}^{n} d(x_i, x_{i+1}), \tag{32.2}$$

де J – загальна ЦФ, n – кількість кроків або сегментів траєкторії, $d(x_i, x_{i+1})$ – функція відстані між конфігураціями x_i та x_{i+1}.

Компоненти цільової функції

1. Відстань між конфігураціями:

$$d(x_i, x_{i+1}) = \|x_{i+1} - x_i\|, \tag{32.3}$$

де $\|\ \ \|$ – евклідова відстань або інша метрика, що використовується для вимірювання відстані між конфігураціями.

2. Уникнення зіткнень:

Для забезпечення безпеки траєкторії, необхідно додати обмеження на уникнення зіткнень:

$$subject\ to\ \ x_i \in C_{free}, \tag{32.4}$$

де C_{tree} – допустима область конфігурацій, вільна від перешкод.

Застосувавши (32.3, 32.4) до (32.2), ЦФ для алгоритму RRT-Connect отримає вигляд:

$$Minimize\ J = \sum_{i=1}^{n} \|x_{i+1} - x_i\|\ \ subject\ to\ \ x_i \in C_{free}. \tag{32.5}$$

Таким чином, ЦФ (32.5) алгоритму RRT-Connect включає суму відстаней між послідовними конфігураціями та обмеження на допустимі області конфігурацій. Це дозволяє алгоритму знаходити оптимальні та безпечні траєкторії для МР у складних середовищах.

33. Алгоритм *двонаправленого швидко-зростаючого випадкового дерева* (Bidirectional Rapidly-exploring Random Tree, Bi-RRT) є розширенням класичного алгоритму RRT, який використовує два дерева, що ростуть одночасно від початкової та кінцевої точок, поки вони не з'єднаються. Це підвищує ефективність у складних середовищах, але алгоритм складний у реалізації та потребує налаштування параметрів [71]. Алгоритм використовується для планування траєкторій у просторі станів.

ЦФ для алгоритму Bi-RRT може бути виражена як математична формула, що мінімізує відстань між початковою та кінцевою точками, а також враховує уникнення зіткнень з перешкодами. Формально, ЦФ може бути записана як:

$$\text{Minimize } J = \sum_{i=1}^{n} d(x_i, x_{i+1}), \tag{33.1}$$

де J – загальна ЦФ, n – кількість вузлів у траєкторії, $d(x_i, x_{i+1})$ – відстань між сусідніми вузлами x_i та x_{i+1}.

Для забезпечення безпеки та ефективності траєкторії, ЦФ також може включати *додаткові умови*, такі як уникнення зіткнень:

$$subject\ to\ x_i \in X_{free}, \forall i, \tag{33.2}$$

де X_{free} – допустима область без перешкод.

З урахуванням додаткових умов (33.2), ЦФ може бути записана як:

$$\text{Minimize } J = \sum_{i=1}^{n} d(x_i, X_{i+1}) \;\; subject\ to\ x_i \in X_{free}, \forall i. \tag{33.3}$$

Таким чином, ЦФ (33.3) алгоритму Bi-RRT зазвичай спрямована на мінімізацію відстані між початковою та кінцевою точками, враховуючи обмеження середовища забезпечуючи при цьому уникнення перешкод і дотримання кінематичних обмежень. Формально, ЦФ може бути виражена як сума відстаней між сусідніми вузлами траєкторії з додатковими умовами на допустимість станів.

34. Алгоритм *RRT** (Rapidly-exploring Random Tree Star) є вдосконаленою версією алгоритму RRT, яка забезпечує асимптотичну оптимальність. Алгоритм використовує випадкове зразкування для побудови дерева, яке поступово розширюється до цільової точки. Це означає, що з часом алгоритм знаходить шлях, який наближається до оптимального. Основні переваги включають простоту реалізації та гарантовану оптимальність шляху, але алгоритм має високі вимоги до обчислювальних ресурсів і можливі проблеми з масштабованістю [72, 73].

ЦФ для алгоритму RRT* зазвичай пов'язана з мінімізацією вартості шляху від початкової точки до цільової точки.

Розширене рішення цільової функції для алгоритму RRT* можна виразити як:

$$\text{Minimize } C\left(x_{start}, x_{goal}\right), \tag{34.1}$$

де $C\left(x_{start}, x_{goal}\right)$ – це загальна вартість шляху від початкової точки x_{start} до цільової точки x_{goal}.

Ця вартість може бути визначена як сума вартостей окремих сегментів шляху:

$$C\left(x_{start}, x_{goal}\right) = \sum_{i=1}^{n-1} c(x_i, x_{i+1}), \tag{34.2}$$

де x_i – це точка на шляху, а $c(x_i, x_{i+1})$ – це вартість переходу між точками x_i й x_{i+1}.

Компоненти цільової функції:

1. Вартість переходу $c(x_i, x_{i+1})$ може включати різні метрики.

2. Довжина шляху: $c(x_i, x_{i+1}) = \|x_{i+1} - x_i\|$.

3. Енергоспоживання: вартість може враховувати енергетичні витрати на переміщення між вузлами.

4. Час виконання: вартість може враховувати час, необхідний для переміщення між вузлами.

З урахуванням компонентів, ЦФ для алгоритму RRT* отримає наступний вигляд:

$$\text{Minimize } C\left(x_{start}, x_{goal}\right) = \sum_{i=1}^{n-1} \|x_{i+1} - x_i\|, \tag{34.3}$$

де $\|x_{i+1} - x_i\|$ – евклідова відстань між вузлами x_i й x_{i+1}.

Рівняння (34.3) мінімізує загальну довжину шляху від початкової до цільової точки, що є основною метою алгоритму RRT*.

Таким чином, ЦФ алгоритму RRT* може бути виражена як сума вартостей переходів між послідовними вузлами траєкторії, де вартість може враховувати різні метрики, такі як довжина шляху, енергоспоживання або час виконання , а також забезпечує асимптотично оптимальне рішення для задачі планування траєкторії шляхом мінімізації цільової функції,. Це дозволяє алгоритму знаходити оптимальні траєкторії в складних середовищах.

35. Алгоритм Informed-RRT* є вдосконаленням алгоритму RRT*, який спрямований на оптимізацію процесу планування шляхів шляхом фокусування вибірки на підмножині простору, яка може покращити поточне рішення. Алгоритм швидше знаходить оптимальний шлях, але складніший у реалізації та потребує налаштування параметрів [73, 74].

ЦФ для Informed-RRT* зазвичай спрямована на мінімізацію довжини шляху або іншого критерію вартості.

ЦФ для Informed-RRT* як мінімізація вартості шляху від початкової точки x_{start} до кінцевої точки x_{goal}:

$$\text{Minimize } J(\tau) = \int_0^T c\big(\tau(t)\big)dt, \tag{35.1}$$

де τ – шлях від точки x_{start} до точки x_{goal}, T – час, необхідний для проходження шляхуτ, $c\big(\tau(t)\big)$ – функція вартості, яка може включати довжину шляху, енергію, час або інші критерії.

Алгоритм Informed-RRT* використовує інформоване вибіркове простір для підвищення ефективності пошуку. Це досягається шляхом обмеження вибіркового простору до еліпсоїда, який містить всі можливі покращення поточного рішення. Формально, це можна виразити як:

$$\mathcal{E} = \{x \in \mathbb{R}^n | \, \|x - x_{mid}\|_{A^{-1}} \leq 1\}, \tag{35.2}$$

де $\mathcal{E}$ – еліпсоїд вибіркового простору, x_{mid} – середня точка між початковою та цільовою точками, A – матриця, що визначає форму та розмір еліпсоїда.

Алгоритм Informed-RRT* використовує евристичну функцію для фокусування вибірки на підмножині простору, яка може покращити поточне рішення. Це досягається шляхом вибірки точок всередині пролатного гіперсфероїда, який визначається початковою та кінцевою точками, а також поточним найкращим шляхом.

Пролатний гіперсфероїд визначається як множина точок x, що задовольняють наступну умову:

$$(x - x_{center})^2 \cdot A(x - x_{center}) \leq 1, \tag{35.3}$$

де x_{center} – центр гіперсфероїда, який знаходиться на середині відрізка між x_{start} та x_{goal}, A – матриця, яка визначає форму та розміри гіперсфероїда.

З урахуванням евристики, *ЦФ* може бути переписана як:

$$\text{Minimize } J(\tau) = \int_0^T c\big(\tau(t)\big)dt + h(x_{goal}, x), \tag{35.4}$$

де $h\big(x_{goal}, x\big)$ – евристична функція, яка оцінює вартість досягнення кінцевої точки x_{goal} з поточної точки x.

Таким чином, ЦФ (35.4) для алгоритму Informed-RRT* спрямована на мінімізацію вартості шляху з урахуванням евристики, яка фокусує вибірку на підмножині простору, що може покращити поточне рішення. Використання еліпсоїда для обмеження вибіркового простору дозволяє значно зменшити кількість непотрібних вибірок і прискорити процес пошуку оптимального шляху. Це дозволяє алгоритму швидше знаходити оптимальні або близькі до оптимальних шляхи.

36. Алгоритм *MBD-RRT*FFT* (Multi-Bidirectional Rapidly-exploring Random Tree with Fast Fourier Transform) є складним алгоритмом для планування шляху, який використовує багатонаправлене розширення дерев, багатопотокові обчислення та алгоритм Fitch для оптимізації. Основні переваги включають високу ефективність та зменшення часу виконання завдяки паралельній обробці даних. Недоліками є складність реалізації та необхідність налаштування параметрів [75].

ЦФ цього алгоритму спрямована на мінімізацію вартості шляху з урахуванням різних критеріїв, таких як відстань, час, енергія та уникнення перешкод.

ЦФ для алгоритму MBD-RRT*FFT може бути виражена як:

$$\text{Minimize } J(x) = \sum_{i=1}^{n-1} c(x_i, x_{i+1}), \tag{36.1}$$

де $J(x)$ – загальна вартість шляху, x_i – точки шляху, $c(x_i, x_{i+1})$ – функція вартості переходу між точками x_i та x_{i+1}.

Для алгоритму MBD-RRT*FFT ЦФ може включати додаткові критерії, такі як уникнення перешкод, дотримання динамічних обмежень та оптимізація за допомогою швидкого перетворення Фур'є. Тому розширене рішення цільової функції може бути виражене як:

$$\text{Minimize } J(x) = \sum_{i=1}^{n-1} |c(x_i, x_{i+1}) + \lambda \cdot h(x_i, x_{i+1}) + \mu \cdot f(x_i, x_{i+1})|, \quad (36.2)$$

де $h(x_i, x_{i+1})$ – штрафна функція за порушення обмежень (наприклад, зіткнення з перешкодами), $f(x_i, x_{i+1})$ – функція оптимізації за допомогою швидкого перетворення Фур'є, λ й μ – коефіцієнт штрафу, що визначає важливість уникнення перешкод відносно основної вартості шляху.

ЦФ включає компоненти:

1. Функція вартості переходу визначається як евклідова відстань між точками x_i та x_{i+1}.:

$$c(x_i, x_{i+1}) = \| x_{i+1} - x_i \|. \quad (36.3)$$

2. Штрафна функція $h(x_i, x_{i+1})$ враховує різні обмеження, такі як зіткнення з перешкодами або порушення динамічних обмежень. Вона визначається як:

$$h(x_i, x_{i+1}) = \begin{cases} 0, & \text{якщо перехід не порушує обмежень} \\ f(x_i, x_{i+1}), & \text{якщо перехід порушує обмеження} \end{cases}, \quad (36.4)$$

де $f(x_i, x_{i+1})$ – функція, що визначає величину штрафу за порушення обмежень. Ця функція може бути різною залежно від обмежень [75].

3. Функція оптимізації за допомогою швидкого перетворення Фур'є $f(x_i, x_{i+1})$:

$$f(x_i, x_{i+1}) = FFT(x_i, x_{i+1}). \quad (36.5)$$

Застосовуючи формули (36.3),(36.4) і (36.5) до (36.2) отримаємо загальний вигляд цільової функції:

$$\text{Minimize } J(x) = \sum_{i=1}^{n-1} \left| \| x_{i+1} - x_i \| + \lambda \cdot h(x_i, x_{i+1}) = \begin{cases} 0, & f_{collision}(x_i, x_{i+1}) = \infty \\ f(x_i, x_{i+1}), & f_{dynamic}(x_i, x_{i+1}) = \alpha \cdot violation_{degree(x_i, x_{i+1})} \end{cases} + \mu \cdot FFT(x_i, x_{i+1}) \right|. \quad (36.6)$$

Багатопотоковість дозволяє паралельно обробляти різні частини дерева, що значно прискорює процес пошуку. Після завершення обчислень кожним потоком, результати порівнюються для отримання загального оптимального шляху.

Таким чином, ЦФ (36.2) алгоритму MBD-RRT*FFT спрямована на мінімізацію загальної вартості шляху, враховуючи відстань між точками, штрафи за порушення обмежень та оптимізацію за допомогою швидкого перетворення Фур'є з урахуванням багатопотокової обробки, що дозволяє ефективно планувати шляхи в динамічних середовищах. Це забезпечує уникнення перешкод та дотримання інших важливих критеріїв, таких як динамічні обмеження та швидкість обчислень А також дозволяє алгоритму ефективно планувати шляхи в складних середовищах, забезпечуючи уникнення перешкод та дотримання інших важливих критерії

37. *Динамічні ігри*, це теоретичний підхід для моделювання стратегій, що дозволяє моделювати складні взаємодії. Основні переваги включають можливість моделювання складних взаємодій та застосування в різних галузях, але цей підхід вимагає глибоких знань теорії ігор і складних математичних моделей [76, 77, 78].

Динамічні ігри часто моделюються за допомогою динамічного програмування, де використовується рівняння Беллмана для визначення оптимальної стратегії.

Одним з підходів до вирішення проблеми пошуку шляху АМР є використання динамічних ігор, де ЦФ визначає оптимальний шлях для МР [79, 80].

ЦФ в контексті динамічних ігор для пошуку шляху може бути визначена як функція, яка мінімізує або максимізує певний критерій, наприклад, відстань, час або витрати енергії. Формально, ЦФ може бути записана як:

$$J(u) = \int_{t_0}^{t_f} L(x(t), u)t), t)dt + \Phi(x(t_f)), \quad (37.1)$$

де $J(u)$ – ЦФ, яку потрібно мінімізувати або максимізувати, $L(x(t), u)t)$, t – функція витрат, яка залежить від стану $x(t)$, керування $u(t)$ та часу t, $\Phi(x(t_f)$ – кінцеві витрати, які залежать від стану в кінцевий момент часу t_f, t_0 і t_f – час початку і закінчення в динамічній гри.

Таким чином, ЦФ (37.1) для методу динамічних ігор визначається як максимізація очікуваної суми винагород, враховуючи ймовірності переходів між станами та коефіцієнт дисконтування.

38. *Метод розв'язуючих функцій Чикрія* – це теоретичний підхід для розв'язання задач керування в умовах конфлікту, який базується на використанні обернених функціоналів. Цей метод дозволяє знаходити теоретично обґрунтовані рішення для задач керування в умовах конфлікту, що робить його корисним у різних галузях, таких як робототехніка, економіка та військова справа. Основні переваги включають можливість застосування в різних галузях та теоретично обґрунтовані рішення, але метод має високі вимоги до знань теорії керування та складний у реалізації [81–84].

Метод розв'язуючих функцій А. О. Чикрія є одним із фундаментальних методів, що застосовуються для розв'язання диференціальних ігор з переслідуванням [85]. Цей метод може бути адаптований для задач пошуку шляху МР.

Розглянемо АМР, який має знайти оптимальний шлях з початкової точки A до цільової точки B в середовищі з перешкодами. Нехай $x(t)$ – це стан робота в момент часу t, а $u(t)$ – керування роботом.

ЦФ в цьому контексті визначає витрати на рух МР від початкової точки до цільової точки, враховуючи перешкоди та інші фактори. Тоді ЦФ J може бути визначена як:

$$J = \int_0^T L(x(t), u)t), t)dt + \Phi(x(T)), \tag{38.1}$$

де $L(x(t), u)t)$, t – функція витрат, яка залежить від стану $x(t)$, керування $u(t)$, $\Phi(x(T))$ – кінцева вартість, яка залежать від кінцевого стану T, T – час досягнення точки цільовою функцією.

Метод розв'язуючих функцій передбачає побудову функції $V(x)$, яка задовольняє рівнянню Гамільтона-Якобі-Беллмана (ГЯБ):

$$\frac{\partial V}{\partial x} + \min_u \left[L(x, u) + \frac{\partial V}{\partial x} f(x, u)\right] - 0, \tag{38.2}$$

де $f(x, u)$ – динаміка системи.

Кроки виконання алгоритму включають:

1. Ініціалізація. Встановити початкові умови для функції $V(x)$ на кінцевому стані $x(T)$:

$$V\big(x(T)\big) = \Phi\big(x(T)\big). \tag{38.3}$$

2. Розв'язання рівняння ГЯБ. Використовуючи методи чисельного розв'язання, знайти функцію $V(x)$ для всіх станів x та моментів часу t.

3. Визначення оптимального керування. Для кожного стану x та моменту часу t, знайти оптимальне керування $u^*(t)$, яке мінімізує вираз:

$$u^*(t) = \arg\min_u \left[L(x, u) + \frac{\partial V}{\partial x} f(x, u)\right]. \tag{38.4}$$

Побудова траєкторії: Використовуючи знайдене оптимальне керування $u^*(t)$, будується траєкторія робота від початкової точки A до цільової точки B.

Таким чином, метод розв'язуючих функцій А. О. Чикрія, дозволяє знайти оптимальний шлях АМР, мінімізуючи витрати на рух та враховуючи динаміку системи. ЦФ (38.1) в цьому контексті визначає критерій, за яким оцінюється якість знайденого шляху. Використання часткових похідних дозволяє ефективно досліджувати унімодальні функції та знаходити оптимальні рішення, що забезпечує ефективний та безпечний рух МР в складних середовищах.

Висновки

В роботі розглянуто і проаналізовано 38 сучасних алгоритмів і методів планування шляху для автономних мобільних роботів та їх цільові функції.

Узагальнені результати зведені до єдиної порівняльної таблиці 1, яка надає вид формалізованої основної функції алгоритмів, розкриває основну ідею, переваги/недоліки, сферу застосування і приклад використання. Порівняльна таблиця 1, представлена в формі узагальненого допоміжного довідкового елемента дослідження.

Дослідження підтверджує, що відокремлювати роль цільової функції при дослідженні алгоритмів планування шляху мобільним роботом неможливо, оскільки вона є фундаментальним елементом, який визначає мету оптимізації, оцінює ефективність рішень, забезпечує адаптивність до умов середовища, гарантує безпеку та підвищує ефективність обчислень. Без цільової функції алгоритми планування шляху втрачають свою цілеспрямованість та ефективність, що робить їх непридатними для практичного застосування.

Розуміння цільової функції є критично важливим для алгоритмів будови шляху автономних мобільних роботів з кількох причин, а саме:

1. *Оптимізація маршруту* – ЦФ визначає, що саме алгоритм намагається оптимізувати. Це може бути мінімізація відстані, часу, енергії або уникнення перешкод. Наприклад, для безпілотних наземних засобів (БпНЗ) ЦФ може враховувати динаміку апарата, обмеження рельєфу та ентропію простору переміщення.

2. *Безпека та уникнення перешкод* – ЦФ часто включає параметри, які допомагають уникати зіткнень з перешкодами. Це особливо важливо для автономних мобільних роботів, що працюють у динамічних середовищах з рухомими об’єктами.

3. *Ефективність обчислень* – добре визначена ЦФ дозволяє алгоритму працювати більш ефективно, зменшуючи кількість необхідних обчислень для досягнення оптимального рішення. Це важливо для реального часу, коли МР повинен швидко реагувати на зміни в середовищі.

4. *Адаптивність до змін* – ЦФ може бути налаштована таким чином, щоб алгоритм міг адаптуватися до змін у середовищі або умовах завдання. Наприклад, у випадку з БпЛА, ЦФ може враховувати зміну вітрових умов або обмеження по заряду батареї.

Дослідження показало, що розуміння та правильне визначення цільової функції є ключовим для успішної реалізації алгоритмів будови шляху автономних мобільних роботів.

Отримані висновки підтверджують, що кожен з розглянутих алгоритмів має свої переваги та недоліки, що робить їх придатними для різних застосувань у робототехніці та автономних транспортних засобах. А розуміння цільової функції надає правильного вектору застосування при виборі конкретного алгоритму залежить від специфічних вимог до планування шляху, таких як складність середовища в якому працює АМР, й вимог до ефективності, точності, необхідність оптимізації та обчислювальних ресурсів [1, 2, 4, 16, 64, 75, 82, 85].

Напрями подальших досліджень

Враховуючи отримані результати дослідження, в подальшому планується поглиблене дослідження методу розв’язуючих функцій А. О. Чикрія, яке на думку автора, має великий потенціал для покращення автономних систем у різних аспектах, включаючи оптимізацію, уникнення конфліктів, адаптивність та координацію в мультиагентних системах [84].

Таблиця 1. **Порівняння сучасних алгоритмів планування шляху з урахуванням їх цільових функцій**

№ з/п	Алгоритм	Тип алгоритму	Основна ідея	Цільова функція алгоритму	Переваги	Недоліки	Застосування	Приклади використання
1	2	3	4	5	6	7	8	9
1	**VCD** (Vertical Cellular Decomposition)	Точне розбиття	Вертикальне розбиття простору на клітини	**Мінімізація загальної довжини шляху** Minimize $\sum_{i=1}^{n} A_i$	– Простота реалізації; – Висока точність	– Можливі проблеми з масштабованістю – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
2	**BCD** (Boustrophedon Cellular Decomposition)	Точне розбиття	Розбиття простору на клітини для покриття	**Мінімізація загальної довжини шляху** Minimize $\sum_{i=1}^{n}(L_i + T_i)$	– Простота реалізації – Ефективне покриття простору	– Можливі проблеми з масштабованістю – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
3	**Morse Decomposition**	Точне розбиття	Використання теорії Морса для розбиття простору	**Мінімізація загальної довжини шляху** Minimize $\sum_{i=1}^{n} \int_{M_i} \| \dot{x} - f(x)^2 \| \, dx$	– Глибокий математичний підхід – Можливість аналізу топології	– Складність реалізації – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
4	**Exhaustive Path Planning with Exact Cell Decomposition**	Точне розбиття	Вичерпне планування шляху з точним розбиттям простору	**Мінімізація загальної довжини шляху:** Minimize $\sum_{i=1}^{n} d(C_i, C_{i+1})$ **Мінімізація часу проходження:** Minimize $\sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i}$	– Висока точність – Гарантована точність планування	– Високі вимоги до обчислювальних ресурсів – Складність реалізації	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
5	**Approximate Cell Decomposition**	Приблизне розбиття	Приблизне розбиття простору на регулярні клітини	**Мінімізація загальної довжини шляху:** $OCB_j[k^u] = \bigcup_{t=1}^{k_u} \{ CB_j[[x_k, x'_k] \cdot [y_k, y'_k] \cdot (\gamma_k + l \triangle \theta)]\}$	– Простота реалізації – Швидкість обчислень	– Менша точність порівняно з точними методами – Можливі помилки через наближення	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
6	**Sensor path planning with approximate cell decomposition**	Глобальне планування	Декомпозиція простору на клітини	**Мінімізація загальної довжину шляху:** Minimize $\sum_{i=1}^{n} d(C_i, C_{i+1})$ **Мінімізація часу проходження:** Minimize $\sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i}$	– Ефективність у складних середовищах – Можливість роботи з різними типами перешкод	– Високі вимоги до обчислювальних ресурсів – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
7	**Quadtree–based decomposition**	Глобальне планування	Декомпозиція простору на квадрати	**Мінімізація неоднорідності даних у квадрантах:** Minimize $\sum_{i=1}^{n} Var(Q_i)$	– Простота реалізації – Ефективність у високовимірних просторах	– Можливі проблеми з масштабованістю – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
8	**Framed–quadtree decomposition**	Глобальне планування	Декомпозиція простору на квадрати з рамками	**Мінімізація загальної довжини шляху:** Minimize $\sum_{i=1}^{n} d(C_i, C_{i+1})$ **Мінімізація часу проходження:** Minimize $\sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i}$	– Зменшення кількості вузлів – Підвищена ефективність порівняно з класичним quadtree	– Складність реалізації – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці

Продовження таблиці 1

1	2	3	4	5	6	7	8	9
9	**K–Framed quadtrees decomposition**	Глобальне планування	Комбінація квадратно–рамкової декомпозиції	**Мінімізація загальної довжини шляху:** $\text{Minimize } \sum_{i=1}^{n} d(C_i, C_{i+1})$	– Зменшення кількості вузлів та підвищення точності – Підвищена ефективність та точність порівняно з framed-quadtree	– Складність реалізації – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
10	**Adaptive decomposition**	Глобальне планування	Адаптивна декомпозиція	**Мінімізація похибки реконструкції сигналу:** $\text{Minimize } \sum_{i=1}^{n} \left\lvert x(t) - \sum_{j=1}^{m} C_j(t) \right\rvert^2$	– Висока гнучкість та адаптивність – Можливість адаптації до різних умов	– Складність реалізації – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
11	**Probabilistic cell decomposition**	Глобальне планування	Розбиття простору на ймовірнісні комірки	**Мінімізація ймовірності зіткнення:** $\text{Minimize } \sum_{i=1}^{n} P(C_i)$ **Мінімізація загальної довжини шляху з урахуванням ймовірностей:** $\text{Minimize } \sum_{i=1}^{n} d(C_i, C_{i+1}) \cdot P(C_i)$ **Мінімізація часу проходження з урахуванням ймовірностей:** $\text{Minimize } \sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i} \cdot P(C_i)$	– Ефективність у високовимірних просторах – Можливість роботи у складних середовищах	– Високі вимоги до обчислювальних ресурсів – Складність реалізації	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
12	**Probabilistic cell decomposition with harmonic functions**	Глобальне планування	Розбиття простору на ймовірнісні комірки з гармонічними функціями	**Мінімізація ймовірності зіткнення з урахуванням гармонічних функцій:** $\text{Minimize } \sum_{i=1}^{n} P(C_i) \cdot H(C_i)$ **Мінімізація загальної довжини шляху з урахуванням гармонічних функцій:** $\text{Minimize } \sum_{i=1}^{n} d(C_i, C_{i+1}) \cdot H(C_i)$ **Мінімізація часу проходження з урахуванням гармонічних функцій:** $\text{Minimize } \sum_{i=1}^{n} \frac{d(C_i, C_{i+1})}{v_i} \cdot H(C_i)$	– Покращена точність завдяки гармонічним функціям – Ефективність у складних середовищах	– Високі вимоги до обчислювальних ресурсів – Складність реалізації	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
13	**Ariadne's clew**	Глобальне планування	Побудова дерева, що досліджує нові області простору	**Загальна цільова функція:** $\text{Minimize } f(q) = \sum_{i=1}^{n} \left(d(q_i, q_{goal}) + \lambda \cdot \sum_{j=1}^{m} \left(\frac{1}{\lVert q - q_{obs_j} \rVert} \right) \right)$	– Ефективне дослідження нових областей – Підходить для високовимірних просторів	– Високі вимоги до обчислювальних ресурсів – Складність реалізації	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
14	**ECS** (Expansive configuration spaces)	Глобальне планування	Використання випадкового зразкування для дослідження конфігураційн ого простору	**Загальна цільова функція:** $\text{Minimize } U_{total}(q) = -\alpha \cdot boundary_{measure}(q) + + \beta \cdot \sum_{i=1}^{n} distance\,(q, q_i)$	– Ефективність у складних просторах – Можливість роботи у високовимірних просторах	– Високі вимоги до обчислювальних ресурсів – Складність реалізації	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
15	**PRM** (Probabilistic Roadmap)	Глобальне планування	Використання випадкового зразкування для побудови графа	**Загальна цільова функція:** $\text{Minimize } d_{\text{total}} = \sum_{(q_i, q_j) \in P} d(q_i, q_j)$	– Можливість роботи у високовимірних просторах – Ефективність у складних просторах	– Високі вимоги до обчислювальних ресурсів – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці

Продовження таблиці 1

1	2	3	4	5	6	7	8	9
16	**RRM** (Randomized roadmap method)	Глобальне планування	Використання випадкового зразкування для побудови графа	**Загальна цільова функція:** Minimize $C_{total}(q_{start}, q_{goal}) = \sum_{(q_i,q_j)\in P} c \parallel q_i - q_j \parallel$	– Можливість роботи у високовимірних просторах – Ефективність у складних просторах	– Високі вимоги до обчислювальних ресурсів – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
17	**Lazy PRM**	Глобальне планування	Відкладення перевірок колізій до моменту запиту	**Загальна цільова функція:** Minimize $C_{\text{total}}(q) = \sum_{(q_i,q_j)\in P} \left(d(q_i,q_j) + \lambda \cdot c(q_i,q_j)\right)$	– Зменшення кількості перевірок колізій – Зменшення часу виконання	– Можливі проблеми з масштабованістю – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
18	**Gaussian sampling for PRM**	Глобальне планування	Використання гауссового розподілу для зразкування	**Загальна цільова функція:** $C_r = \{p \in C_{free} \mid \|p-q\| < d \wedge q \in \mathcal{IB} \cup \mathcal{OB}\}$	– Краще покриття складних областей – Зменшення кількості зразків	– Необхідність налаштування параметрів – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
19	**Halton sampling for PRM**	Глобальне планування	Використання послідовності Халтона для зразкування	**Загальна цільова функція:** Minimize $C_{total}(q_{start}, q_{goal}) = \sum_{(q_i,q_j)\in P} c \parallel q_i - q_j \parallel$	– Рівномірний розподіл зразків – Зменшення кількості зразків	– Складність реалізації – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
20	**D*** (Dynamic A*)	Інкрементальний пошук	Інкрементальний пошук з використанням евристик	**Загальна цільова функція:** Minimize $C_{total}(q_{start}, q_{goal}) = = \sum_{(q_i,q_j)\in P}(\parallel q_i - q_j \parallel + \parallel q_j - q_{goal} \parallel) h(q_i, q_{goal})$	– Ефективність у динамічних середовищах – Підходить для частково відомих та змінних середовищ	– Високі вимоги до обчислювальних ресурсів – Складність реалізації	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
21	**Goal-directed and randomized search**	Глобальне планування	Поєднання цілеспрямованого та випадкового пошуку	**Цілеспрямований пошук** Strong (Minimize ∨ Maximize $f(x)$) **Випадковий пошук** Rand (Minimize ∨ Maximize $f(x)$)	- Ефективність у великих просторах – Поєднання переваг цілеспрямованого та випадкового пошуку	– Складність реалізації – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
22	**SANDROS**	Динамічний графовий пошук	Ієрархічний, нерівномірний багаторівневий пошук	**Загальна цільова функція:** Minimize $\sum_{i=1}^{n} \lvert P_i - P_{target} \rvert$	– Ефективність у складних середовищах – Висока точність	– Складність реалізації – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
23	**APF** (Artificial potential field method)	Локальне планування	Використання потенційних полів	**Загальна цільова функція** Minimize $U_{total}(q) = = \frac{1}{2} k_{att} \|q - q_{goal}\|^2 + \sum_{i=1}^{m} \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\|q-q_{obs_i}\|} - \frac{1}{d_0}\right)^2 & if \ \|q - q_{obs_i}\| \le d_0, \\ 0 & if \ \|q - q_{obs_i}\| > d_0. \end{cases}$	– Простота реалізації – Швидкість обчислень	– Проблеми з локальними мінімумами – Не підходить для складних середовищ	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
24	**DAPF** (Dynamic artificial potential field method)	Локальне планування	Використання динамічних потенційних полів	**Загальна цільова функція:** Minimize $U_{total}(q,t) = = \frac{1}{2} k_{att} \|q - q_{goal}\|^2 + \begin{cases} \frac{1}{2} k_{rep} \left(\frac{1}{\|q-q_{obs}\|} - \frac{1}{d_0}\right)^2 & if \ \|q - q_{obs}\| \le d_0, \\ 0 & if \ \|q - q_{obs}\| > d_0. \end{cases} + \alpha \|\dot{q}_{obs}(t)\|$	– Простота реалізації – Швидкість обчислень	– Проблеми з локальними мінімумами – Не підходить для складних середовищ	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці

Продовження таблиці 1

1	2	3	4	5	6	7	8	9
25	**IAPF** (Improved artificial potential field)	Локальне планування	Використання потенційних полів з покращеннями	**Загальна цільова функція:** Minimize $U_{total}(q) =$ $= \frac{1}{2}k_{att}\|q - q_{goal}\|^2 + \sum_{i=1}^{m}\begin{cases}\frac{1}{2}k_{rep}\left(\frac{1}{\|q-q_{obs_i}\|}-\frac{1}{d_0}\right)^2 & if\ \|q-q_{obs_i}\| \le d_0,\\ 0 & if\ \|q-q_{obs_i}\| > d_0.\end{cases} + \sum_{i=1}^{n}\frac{1}{2}k_{virt}\|q - q_{virt,i}\|^2$	– Покращена ефективність уникнення перешкод – Зменшення проблем з локальними мінімумами	– Можливі проблеми з масштабованістю – Не підходить для дуже складних середовищ	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
26	**Artificial potential field based subgoal network**	Потенційні поля з підцілями	Використання потенційних полів для створення мережі підцілей	**Загальна цільова функція:** $U(x) = \frac{1}{2}k_{att}\left\|x - x_{goal}\right\|^2 + + \sum_{i=1}^{n}\frac{1}{2}k_{subgoal}\left\|x - x_{subgoal_i}\right\|^2 + + \sum_{j=1}^{m}\begin{cases}\frac{1}{2}k_{rep}\left(\frac{1}{\left\|x-x_{obs_j}\right\|}-\frac{1}{d_0}\right)^2 & if\ \left\|x - x_{obs_j}\right\| \le d_0,\\ 0 & if\ \left\|x - x_{obs_j}\right\| > d_0.\end{cases}$	– Простота реалізації – Швидкість обчислень	– Проблеми з локальними мінімумами – Не підходить для складних середовищ	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
27	**Dynamic subgoal path planner**	Динамічне планування з підцілями	Генерація підцілей для обходу перешкод	**Загальна цільова функція:** Minimize $J(x) = \alpha \cdot \sum_{i=1}^{n-1}\|x_{i+1} - x_i\| + +\beta \cdot \sum_{i=1}^{n} cost\,(x_i) + \gamma \cdot \sum_{i=2}^{n-1}\|x_{i-1} - 2x_i + x_{i+1}\|$	– Швидке ухилення від локальних мінімумів – Висока ефективність у динамічних середовищах	– Складність реалізації – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
28	**Hierarchical motion planner**	Ієрархічне планування руху	Ієрархічна структура для планування руху	**Загальна цільова функція:** Minimize $J = w_1\int_0^T\|\dot{x}(t)\|dt + w_2\sum_{j=1}^{m}\phi\left(d_j(x)\right) + +\mathrm{w}_3\int_0^T P\left(x(t),\dot{x}(t)\right)dt$	– Зменшення обчислювальної складності – Можливість роботи у високовимірних просторах	– Високі вимоги до обчислювальних ресурсів – Складність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
29	**Two-layered subgoal algorithm**	Дворівневий алгоритм з підцілями	Використання двох рівнів для планування шляху	**Загальна цільова функція:** $J = \sum_{j=1}^{m} w_j \cdot g_j(y) + \sum_{k=1}^{p} v_k \cdot h_k(z)$	– Ефективність у складних середовищах – Зменшення обчислювальної складності	– Складність реалізації – Високі вимоги до обчислювальних ресурсів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
30	**RRT with local trees**	Глобальне планування	Використання локальних дерев для покращення пошуку	**Загальна цільова функція:** Minimize $J =$ $= \sum_{i=1}^{n}(w_1 \cdot \sum_{i=1}^{n} d(x_i, x_{i+1}) + w_2 \cdot \lambda \cdot \sum_{j=1}^{m} c\left(x_j\right) + w_3 \cdot T(x))$	– Покращена ефективність у складних середовищах – Зменшення кількості перевірок колізій	– Складність реалізації – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
31	**Obstacle-based RRT**	Глобальне планування	Використання перешкод для керування зразкуванням	**Загальна цільова функція:** Minimize $\mathrm{J} = \mathrm{d}\left(\mathrm{x}_{\mathrm{start}}, \mathrm{x}_{\mathrm{goal}}\right) + \lambda \cdot \sum_{i=1}^{n} CollisionCost\,(x_i) + \mathrm{C}(x_i)$	– Краще обходження перешкод – Підвищена ефективність у складних середовищах	– Складність реалізації – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
32	**RRT-connect**	Глобальне планування	Бінаправлений пошук з використанням двох дерев	**Загальна цільова функція:** $Minimize\ J = \sum_{i=1}^{n}\|x_{i+1} - x_i\|\ \ subject\ to\ \ x_i \in C_{free}$	– Швидке з'єднання старту та цілі – Простота реалізації	– Можливі проблеми з масштабованістю – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці

Закінчення таблиці 1

1	2	3	4	5	6	7	8	9
33	**Bidirectional RRT**	Глобальне планування	Використання двох дерев для зменшення часу пошуку	**Загальна цільова функція:** $\text{Minimize } J = \sum_{i=1}^{n} d(x_i, X_{i+1}) \;\; subject\ to\ x_i \in X_{free}, \forall i$	– Зменшення часу пошуку – Підвищена ефективність у складних середовищах	– Складність реалізації – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів – Оптимізація маршрутів у логістиці
34	**RRT***	Глобальне планування	Використання випадкового зразкування для побудови оптимального шляху	**Загальна цільова функція:** $\text{Minimize } C(x_{start}, x_{goal}) = \sum_{i=1}^{n-1} \|x_{i+1} - x_i\|$	– Гарантована оптимальність шляху – Простота реалізації	– Високі вимоги до обчислювальних ресурсів – Можливі проблеми з масштабованістю	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
35	**Informed-RRT***	Глобальне планування	Оптимізація RRT* з використанням евристики	**Загальна цільова функція:** $\text{Minimize } J(\tau) = \int_0^T c(\tau(t))dt + h(x_{goal}, x)$	– Швидша конвергенція до оптимального рішення – Покращена якість кінцевого рішення	– Складність реалізації – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для дронів – Оптимізація маршрутів у логістиці
36	**MBD-RRT*FFT** (Multi–threaded Bidirectional RRT with FFT)	Глобальне планування	Використання багатопотоків их обчислень та алгоритму Fitch для оптимізації	**Загальна цільова функція:** $\text{Minimize } J(x) = \sum_{i=1}^{n-1} \left\| \| x_{i+1} - x_i \| + \lambda \cdot \begin{cases} 0, & f_{collision}(x_i, x_{i+1}) = \infty \\ f(x_i, x_{i+1}), & f_{dynamic}(x_i, x_{i+1}) = \alpha \cdot violation_{degree(x_i, x_{i+1})} \end{cases} + + \mu \cdot FFT(x_i, x_{i+1}) \right\|$	– Висока ефективність завдяки багатопотоковим обчисленням – Зменшення часу виконання завдяки паралельній обробці даних	– Складність реалізації багатопотокових обчислень – Необхідність налаштування параметрів	– Робототехніка – Автономні транспортні засоби	– Планування шляху для мобільних роботів у динаміч-них середовищах – Оптимізація маршрутів у логістиці
37	**Динамічні ігри**	Теоретичний підхід для моделю-вання стратегічної взаємодії між агентами	Використання математичних моделей для аналізу стратегій у динамічних середовищах	**Загальна цільова функція:** $J(u) = \int_{t_0}^{t_f} L(x(t), u)t), t)dt + \Phi(x(t_f))$	– Можливість моделювання складних взаємодій – Використання в різних галузях (економіка, військова справа тощо)	– Складність математичних моделей – Високі вимоги до знань теорії ігор	– Економіка, військова справа, соціальні науки – Моделювання стратегічних взаємодій	– Аналіз ринкових стратегій – Військові стратегії
38	**Метод розв'язуючих функцій Чикрія**	Теоретичний підхід для розв'язання задач керування в умовах конфлікту	Використання обернених функціоналів для розв'язання задач керування	**Загальна цільова функція:** $J = \int_0^T L(x(t), u)t), t)dt + \Phi(x(T))$ **Оптимальне керування u* (t)** $u^*(t) = \arg\min_u \left[L(x,u) + \frac{\partial V}{\partial x} f(x,u) \right]$	– Можливість застосування в різних галузях – Теоретично обґрунтовані рішення	– Високі вимоги до знань теорії керування – Складність реалізації	– Робототехніка, економіка, військова справа – Задачі керування в умовах конфлікту	– Оптимізація маршрутів у логістиці – Військові стратегії

СПИСОК ЛІТЕРАТУРИ ТА ВИКОРИСТАНІ ДЖЕРЕЛА

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

2. Ладієва Л. Р. Методи оптимізації та пошуку оптимальних рішень. Електронне мережне навчальне видання / У. Л. Р.Ладієва. Київ: КПІ ім. Ігоря Сікорського, 2023. 73 с.

3. Shi Wei Li. Verification and Analysis of Two-dimensional Path Planning Objective Function Optimization Based on Classical Particle Swarm Optimization Algorithm / 2021 4th International Conference on Intelligent Robotics and Control Engineering (IRCE), 18-20 September 2021. URL: https://doi.org/10.1109/IRCE53649.2021.9570874.

4. Sidhu. Performance Evaluation of Pathfinding Algorithms [Electronic resource] / Sidhu, H. Kaur // Scholarship at UWindsor. 2020. Mode of access: https://scholar.uwindsor.ca/etd/8178.

5. Samridh Garg; Bhanu Devi Shortest Path Finding using Modified Dijkstra's algorithm with Adaptive Penalty Function/ 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). 06-08 July 2023. Mode of access: https://doi.org/10.1109/ICCCNT56998.2023.10308130.

6. Stephan Weiser, Hans Wulf, Jörn Ihlemann Application of a deepest-path algorithm to study the objective function landscape during fitting for the Yeoh and Ogden model / PAMM Proc. Appl. Math. Mech. 2021. Mode of access: https://doi.org/10.1002/pamm.202100086.

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

8. Проценко А. А., Іванов В. Г. Класичні методи планування шляху для мобільних роботів / Системи управління навігації та зв'язку. 3(55) June 2019. С. 143–151. URL: https://doi.org/10.26906/SUNZ.2019.3.143.

9. Pankaj K. Agarwal, Esther Ezra, Micha Sharir Vertical Decomposition in 3D and 4D with Applications to Line Nearest-Neighbor Searching in 3D / arXiv:2311.01597v1 [cs.CG] 2 Nov 2023. Mode of access: https://doi.org/10.48550/arXiv.2311.01597.

10. Sleumer, Nora; Tschichold-Gürmann, Nadine Exact cell decomposition of arrangements used for path planning in robotics/Technical Report / ETH Zurich, Department of Computer Science 329. 1999. Mode of access: https://doi.org/10.3929/ethz-a-006653440.

11. Choset H. Coverage Path Planning: The Boustrophedon Cellular Decomposition / H. Choset, P.Pignon Field and Service Robotics Springer-Verlag London Limited 1998 pp 203–209. Mode of access: https://doi.org/10.1007/978-1-4471-1273-0_32.

12. Bott, Raoul. Morse Theory Indomitable / Bott, Raoul., - Publications Mathématiques de l'IHÉS. 68: 1988., pp. 99–114. Mode of access: DOI:10.1007/bf02698544.

13. Dłotko P. Computing homology and persistent homology using iterated Morse decomposition / P. Dłotko, H. Wagne: arXiv:1210.1429v2 [math.AT] 25 Oct 2012. Mode of access: https://doi.org/10.48550/arXiv.1210.1429.

14. Rasolzadah K. Morse Theory and Handle Decomposition / K. Rasolzadah. Department of Mathematics Uppsala University, Februari 2018.

15. R. Bahnemann, Revisiting Boustrophedon Coverage Path Planning as a Generalized Traveling Salesman Problem / R. Bahnemann, N. Lawrance arXiv:1907.09224v1 [cs.RO] 22 Jul 2019. URL: https://doi.org/10.1007/978-981-15-9460-1_20.

16. Laumond, J.-P. (Ed.) Robot Motion Planning and Control. London: Spring-Verlag Limited. 1998.

17. Chenghui Cai, Silvia Ferrari Information-Driven Sensor Path Planning by Approximate Cell Decomposition / IEEE transactions on systems, man, and cybernetics, vol. 39, No. 3, June 2009. URL: https://doi.org/10.1109/TSMCB.2008.2008561.

18. Chenghui Cai, Silvia Ferrari Information-driven sensor path planning and the treasure hunt problem / Dissertation Duke University 2008. 112 p.

19. Ramon Gonzalez; Marius Kloetzer; Cristian Mahulea Comparative study of trajectories resulted from cell decomposition path planning approaches / 2017 21st International Conference on System Theory, Control and Computing (ICSTCC). URL: https://doi.org/10.1109/ICSTCC.2017.8107010.

20. Prabhakar Reddy G.V.S., Hubert J. Montas, Hanan Samet, Adel Shirmohammadi Quadtree-Based Triangular Mesh Generation for Finite Element Analysis of Heterogeneous Spatial Data / 2001 ASAE Annual International Meeting Sacramento, California, USA, July 30-August 1, 2001. 25 p.

21. Huiwei Wang; Yaqian Huang; Huaqing Li Quadtree-Based Adaptive Spatial Decomposition for Range Queries Under Local Differential Privacy / IEEE Transactions on Emerging Topics in Computing (Volume: 11, Issue: 4, Oct.-Dec. 2023). pp 1045-1056. URL: https://doi.org/10.1109/TETC.2023.3317393.

22. José Lima The K-Framed Quadtrees Approach for Path Planning Through a Known Environment / ROBOT 2017: Third Iberian Robotics Conference. 2017.

23. Zhou Yijun, Xi Jiadong, Xi Jiadong, Luo Chen A Fast Bi-Directional A* Algorithm Based on Quad-Tree Decomposition and Hierarchical Map / Preparation of Papers for IEEE Access (February 2017). URL: http://dx.doi.org/10.1109/ACCESS.2021.3094854.

24. Ana Rodrigues, Pedro Costa, José Lima The K-Framed Quadtrees Approach for Path Planning Through a Known Environment / November 2018 Advances in Intelligent Systems and Computing 2018. URL: http://dx.doi.org/10.1007/978-3-319-70833-1_5.

25. Ana Rodrigues, Pedro Costa, José Lima The K-framed quadtrees approach for path planning through a known environment / Advances in Intelligent Systems and Computing Search for Book Publications. 2018., pp 49–59. URL: http://doi.org/10.1007/978-3-319-70833-1_5.

26. J. W. Burns; N. S. Subotic; D. Pandelis Adaptive decomposition in electromagnetics / IEEE Antennas and Propagation Society International Symposium. 1997. URL: https://doi.org/10.1109/APS.1997.631726.

27. Xiaomei Zhang, Xiangyu Yun, Zhe Wang, Mohan Li, Jinming Hu, Chengmin Wang, Cunfeng Wei An adaptive decomposition algorithm for quantitative spectral CT imaging / X-RAY Spectrometry Vol.53, Iss.4., August 2024., pp. 282–293. URL: https://doi.org/10.1002/xrs.3365.

28. Tao Liu, Zhijun Luo, Jiahong Huang, Shaoze Yan, A Comparative Study of Four Kinds of Adaptive Decomposition Algorithms and Their Applications / PMC PubMed Central 2018 Jul; 18(7): 2120. URL: https://doi.org/10.3390 s18072120.

29. Sabudin E. N, Omar. R and Che Ku Melor C. Potential Field Methods And Their Inherent Approaches For Path Planning / ARPN Journal of Engineering and Applied Sciences Vol. 11, No. 18, Sept. 2016., pp. 10801-10805.

30. Jan Rosell, Pedro Iñiguez Path planning using Harmonic Functions and Probabilistic Cell Decomposition / IEEE Xplore, Conference: Robotics and Automation, ICRA 2005. URL: http://dx.doi.org/10.1109/ROBOT.2005.1570375.

31. Emmanuel f Mazer, Juan-Manuel Ahuactzin, Pierre Bessiere The Ariadne's Clew Algorithm / Journal of Artificial Intelligence Research. May 1998., pp. 295–316. URL: http://dx.doi.org/10.1613/jair.468.

32. J. M. Ahuactzin, P. Bessiere, E. Mazer The Ariadne's Clew Algorithm / Journal of Artificial Intelligence Research 1998. pp. 295–316. URL: https://doi.org/10.48550/arXiv.1105.5440.

33. David Hsu, Jean-claude Latombe, Rajeev Motwani Path Planning in Expansive Configuration Spaces / International Journal of Computational Geometry & Applications 09(04n05) March 1997. URL: http://dx.doi.org/10.1142/S0218195999000285.

34. Arushi Khokhar Probabilistic Roadmap (PRM) for Path Planning in Robotics / Medium., Feb 12, 2021.

35. Lijun Qiao, Xiao Luo, Qingsheng Luo An Optimized Probabilistic Roadmap Algorithm for Path Planning of Mobile Robots in Complex Environments with Narrow Channels / Sensors 2022, 22(22), 8983. URL: https://doi.org/10.3390/s22228983.

36. S. Carpin Algorithmic Motion Planning: The Randomized Approach/ General Theory of Information Transfer and Combinatorics. 2006. pp. 740–768.

37. Jinbao Chen, Yimin Zhou; Jin Gong; Yu Deng An Improved Probabilistic Roadmap Algorithm with Potential Field Function for Path Planning of Quadrotor / 2019 Chinese Control Conference (CCC). July 2019. URL: https://doi.org/10.23919/ChiCC.2019.8865585.

38. Nancy M. Amato, Yan Wu Randomized roadmap method for path and manipulation planning / IEEE International Conference on Robotics and Automation vol. 1., May 1996. pp. 113–120. URL: http://dx.doi.org/10.1109/ROBOT.1996.503582.

39. Robert Bohlin, Lidia E. Kavraki Path Planning Using Lazy / IEEE International Conference on Robotics & Automation, San Francisco, CA., April 2000. pp. 521–528. URL: https://doi.org/10.1109/ROBOT.2000.844107.

40. Jory Denny; Kensen Shi; Nancy M. Amato Lazy Toggle PRM: A single-query approach to motion planning / 2013 IEEE International Conference on Robotics and Automation., Karlsruhe, Germany. 2013. URL: https://doi.org/10.1109/ICRA.2013.6630904.

41. Boor, V., Overmars, M.H., Van Der Stappen, A.F.: The Gaussian sampling strategyfor probabilistic roadmap planners. In: RSS. vol. 2, pp. 1018–1023. IEEE (1999). URL: https://doi.org/10.1109/ROBOT.1999.772447.

42. Steven M. LaValle, Michael S. Branicky On the Relationship Between Classical Grid Search and Probabilistic Roadmaps / The International Journal of Robotics Research Vol.23, Iss. 7-8 2004. URL: https://doi.org/10.1177/0278364904045481.

43. Huageng Zhong, Ming Cong, Minghao Wang, Yu Du, Dong Liu HB-RRT:A path planning algorithm for mobile robots using Halton sequence-based rapidly-exploring random tree / Engineering Applications of Artificial Intelligence., Vol. 133, Part E., July 2024. URL: https://doi.org/10.1016/j.engappai.2024.108362.

44. Anthony Stentz The D* Algorithm for Real-Time Planning of Optimal Traverses / The Robotics Institute Carnegie Mellon University Pittsburgh, Pennsylvania 15213, September 1994.

45. Firas A. Raheema, Umniah I. Hameed Path Planning Algorithm using D* Heuristic Method Based on PSO in Dynamic Environment / American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS) (2018) Volume 49, No 1, pp. 257–271.

46. Dibyendu Biswas D*, D* Lite & LPA* / Medium Jun 27, 2021.

47. Reinhard Bauer, Daniel Delling, Peter Sanders, Dennis Schieferdecker, Dominik, Schultes, Dorothea Wagner Combining Hierarchical and Goal-Directed Speed-Up Techniques for Dijkstra's Algorithm / Experimental Algorithms (WEA 2008). pp.303–318.

48. Akash Lai, Shaz Qadeer A program transformation for faster goal-directed search / 2014 Formal Methods in Computer-Aided Design (FMCAD) October 2014. URL: https://doi.org/10.1109/FMCAD.2014.6987607.

49. Akash Lal, Shaz Qadeer A Program Transformation for Faster Goal-Directed Search / FMCAD '14: Proceedings of the 14th Conference on Formal Methods in Computer-Aided Design 2014, pp. 147–154.

50. Pang C. Chen, Y. Hwang SANDROS: a motion planner with performance proportional to task difficulty/ IEEE Transactions on Robotics and Automation (Vol: 14, Iss. 3, June 1998) pp. 390–403. URL: https://doi.org/10.1109/70.678449.

51. Iswanto, Alfian Ma'arif, Oyas Wahyunggoro, Adha Imam Cahyadi Artificial Potential Field Algorithm Implementation for Quadrotor Path Planning / (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 8, 2019. URL: https://dx.doi.org/10.14569/IJACSA.2019.0100876.

52. Eryi Zhang Path planning algorithm based on Improved Artificial Potential Field method / Applied and Computational Engineering September 2023. pp. 167–174. URL: http://dx.doi.org/10.54254/2755-2721/10/20230170.

53. Wenrui Wang, Mingchao Zhu, Zhenbang Xu An improved artificial potential field method of trajectory planning and obstacle avoidance for redundant manipulators / International Journal of Advanced Robotic Systems, September 2018. URL: https://doi.org/10.1177/1729881418799562.

54. Hu Hongyu, Zhang Chi, Sheng Yuhuan, Zhou Bin, Gao Fei An Improved Artificial Potential Field Model Considering Vehicle Velocity for Autonomous Driving / IFAC-PapersOnLine Vol. 51, Iss. 31., 2018. pp. 863–867. URL: https://doi.org/10.1016/j.ifacol.2018.10.095.

55. Kaddour Messaoudi, Noureddine Chaib A survey of UAV-based data collection: Challenges, solutions and future perspectives / Journal of Network and Computer Applications Vol. 216, July 2023. URL: https://doi.org/10.1016/j.jnca.2023.103670.

56. Lijuan Xie, Huanwen Chen, Guangrong Xie Artificial Potential Field Based Path Planning for Mobile Robots Using Virtual Water-Flow Method / Advanced Intelligent Computing Theories and Applications. With Aspects of Contemporary Intelligent Computing Techniques (ICIC 2007). Pp. 588–595. URL: http://dx.doi.org/10.1007/978-3-540-74282-1_66.

57. Jixue Mo, Gao Changqing, Fei Liu, Qingkai Yang A Modified Artificial Potential Field Method Based on Subgoal Points for Mobile Robot / ICIRA2023-The 16th international conference on intelligent robotics and applications., July 2023. URL: http://dx.doi.org/10.1007/978-981-99-6483-3_26.

58. Hong Liu; Weiwei Wan; Hongbin Zha A dynamic subgoal path planner for unpredictable environments / 2010 IEEE International Conference on Robotics and Automation., Anchorage, AK, USA., May 2010. URL: https://doi.org/10.1109/ROBOT.2010.5509324.

59. David J. Grymin, Charles B. Neas, Mazen Farhood A hierarchical approach for primitive-based motion planning and control of autonomous vehicles / Robotics and Autonomous Systems., Vol. 62, Iss. 2, Feb. 2014, pp. 214–228. URL: https://doi.org/10.1016/j.robot.2013.10.003.

60. Hanlin Chen, Xizhe Zang, Yubin Liu, Xuehe Zhang, Jie Zhao A Hierarchical Motion Planning Method for Mobile Manipulator / Sensors 2023, 23(15), 6952. URL: https://doi.org/10.3390/s23156952.

61. Yao Qi, Binbing He, Rendong Wang, Le Wang, Youchun Xu Hierarchical Motion Planning for Autonomous Vehicles in Unstructured Dynamic Environments / IEEE Robotics and Automation Letters (Volume: 8, Issue: 2, February 2023). pp. 496–503. URL: https://doi.org/10.1109/LRA.2022.3228159.

62. Amitava Chatterjee, Anjan Rakshit, N. Nirmal Singh Vision-Based Mobile Robot Navigation Using Subgoals/ Vision Based Autonomous Robot Navigation., vol. 44, issue 4, May 2011. pp. 620–641.

63. Nirmal Singh, Avishek Chatterjee, Amitava Chatterjee, Anjan Rakshit A two-layered subgoal based mobile robot navigation algorithm with vision system and IR sensors / May Measurement 44(4) 2011. pp. 620–641. URL: http://dx.doi.org/10.1016/j.measurement.2010.12.002.

64. LaValle, Steven M. Rapidly-exploring random trees: A new tool for path planning / Technical Report (TR 98–11). Computer Science Department, Iowa State University. October 1998.

65. J. J. Kuffner; S. M. LaValle RRT-connect: An efficient approach to single-query path planning / Millennium Conference. IEEE International Conference on Robotics and Automation. April 2000. https://doi.org/10.1109/ROBOT.2000.844730

66. Fan Yang, Xi Fang, Fei Gao, Xianjin Zhou, Hao Li, Hongbin Jin, Yu Song Obstacle Avoidance Path Planning for UAV Based on Improved RRT Algorithm / Discrete Dynamics in Nature and Society, Iss. 1., 2022. URL: https://doi.org/10.1155/2022/4544499.

67. Xiong Yin, Wentao Dong, Xiaoming Wang, Yongxiang Yu, Daojin Yao Route planning of mobile robot based on improved RRT star and TEB algorithm / Scientific reports 8942. 2024. URL: https://doi.org/10.1038/s41598-024-59413-9.

68. Xinyu Tang, Jyh-Ming Lien, Nancy Amato OBRRT: Obstacle-Based RRT/ IEEE International Conference on Robotics and Automation. 2006. pp. 895–900. URL: http://dx.doi.org/10.1109/ROBOT.2006.1641823.

69. Xin Cheng, Jingmei Zhou, Zhou Zhou, Xiangmo Zhao An improved RRT-Connect path planning algorithm of robotic arm for automatic sampling of exhaust emission detection in Industry 4.0 / Journal of Industrial Information Integration Vol. 33., June 2023. URL: https://doi.org/10.1016/j.jii.2023.100436.

70. J. J. Kuffner and S. M. LaValle RRT-Connect path solving/ CRA. Millennium Conference. IEEE International Conference on Robotics and Automation. Symposia Proceedings (Cat. No.00CH37065). URL: https://doi.org/10.1109/ROBOT.2000.844730.

71. Rui Zhang, He Guo, Darius Andriukaitis, Yongbo Li Intelligent path planning by an improved RRT algorithm with dual grid map / Alexandria Engineering Journal Vol. 88., February 2024, pp. 91–104. URL: https://doi.org/10.1016/j.aej.2023.12.044.

72. Jun Ding,Yinxuan Zhou, Xia Huang An improved RRT* algorithm for robot path planning based on path expansion heuristic sampling / Journal of Computational Science Vol. 67, March 2023. URL: https://doi.org/10.1016/j.jocs.2022.101937.

73. James J. Kuffner, Jr. Steven M. LaValle RRT-Connect: An Efficient Approach to Single-Query Path Planning / In Proc. 2000 IEEE Int’l Conf. on Robotics and Automation (ICRA 2000) pp. 995–1001. URL: http://dx.doi.org/10.1109/ROBOT.2000.844730.

74. Zhe Huang, Hongyu Chen, John Pohovey, Katherine Driggs-Campbe Neural Informed RRT*: Learning-based Path Planning with Point Cloud State Representations under Admissible Ellipsoidal Constraints / arXiv:2309.14595v2 [cs.RO] 07 Mar 2024. URL: http://dx.doi.org/10.1109/ICRA57147.2024.10611099.

75. Бернацький А. П. Вдосконалений метод планування шляху автономного наземного робота з використанням алгоритму MBD-RRT*FFT / Системи і технології зв’язку, інформатизації та кібербезпеки. Випуск № 5, 2024. URL: https://doi.org/10.58254/viti.5.2024.03.37.

76. Anita Garhwal, Partha Pratim A Survey on Dynamic Spectrum Access Techniques for Cognitive Radio / International Journal of NextGeneration Networks (IJNGN). Vol. 3, No. 4, 2012. URL: http://dx.doi.org/10.5121/ijngn.2011.3402.

77. P. Taylor, L. Jonker, Evolutionary stable strategies and game dynamics /Mathematical Biosciences 40 (1–2) (1978). pp.145–156.

78. Чикрій А. О. Вимірні багатозначні відображення та їх селектори в динамічних іграх переслідування / А. А. Чикрій, І. С. Раппопорт // Пробл. упр. та інформатики. № 1-2. 2006. С. 60–70.

79. Shaobo Zhang, Qinxiang Xia, Mingxing Chen, Sizhu Cheng Multi-Objective Optimal Trajectory Planning for Robotic Arms Using Deep Reinforcement Learning / Sensors 2023, 23(13), 5974. URL: https://doi.org/10.3390/s23135974.

80. Masoud Fetanat; Sajjad Haghzad; Saeed Bagheri Shouraki Optimization of dynamic mobile robot path planning based on evolutionary methods / AI & Robotics (IRANOPEN). 2015. URL: https://doi.org/10.1109/RIOS.2015.7270743.

81. Альбус Дж. Аналітичний метод вирішення ігрового завдання про "М’яку посадку" для рухомих об’єктів / Дж. Альбус, А. Мейстел, А. О. Чикрій, А. А. Білоусов, А. І. Козлов // Кібернетика та систем. аналіз. № 1. 2001. С. 97–115

82. Чикрій А. О Квазилінійні конфліктно керовані процеси зі змінною структурою / А. А. Чикрій, І. І. Матичин // Пробл. упр. та інформатики. № 6. 1998. С. 31–41.

83. Чикрій А. О. Квазилінійні позиційні інтегральні ігри зближення / А. О. Чикрій, Г. Ц. Чикрій, К. Ю. Волянський // Пробл. упр. та інформатики. № 6. 2001. С. 5–28.

84. Chikrii, A. Conflict-Controlled Processes / Springer Science &Business Media. 2013.

85. Барановська Л. В., Гирявець Д. М., Барановська Г. Г. Візуалізація групової гри переслідування на площині / Conference: Information Technologies and Security (ITS-2020). 2021.

DOI: 10.58254/viti.6.2024.03.59

УДК 623

канд. техн. наук Борисов І. В. ORCID: 0000-0003-2276-9913 (НДІ ВР)
канд. техн. наук Волков О. В. ORCID: 0000-0003-3777-6195 (ВА ім. Євгенія Березняка)

КІБЕРБЕЗПЕКА БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ ТА ОСОБЛИВОСТІ ЗАХИСТУ ВІД ПЕРЕХОПЛЕННЯ

У статті розглядаються ключові аспекти кібербезпеки безпілотних авіаційних комплексів (БпАК) в умовах сучасних військових конфліктів і технологічного прогресу, безпілотні системи стали важливими інструментами для збору інформації, ведення розвідки та виконання бойових завдань. Однак їх широке використання супроводжується новими кіберзагрозами, що потребують спеціалізованих заходів для забезпечення безпеки. Стаття аналізує основні види кіберзагроз, які можуть вплинути на БпАК, включаючи перехоплення комунікацій, несанкціонований доступ до управлінських систем і злом криптографічних захистів.

У статті також розглядаються сучасні методи і технології захисту, такі як криптографічні алгоритми, механізми аутентифікації та шифрування даних. Окрім того, аналізуються існуючі стандарти і практичні рішення для забезпечення захисту комунікаційних каналів. Остання частина статті присвячена новітнім трендам у сфері кібербезпеки БпАК та прогнозуванню майбутніх загроз. Розглядаються можливі рішення і підходи для покращення захисту безпілотних систем в умовах швидкої зміни кіберсередовища, а також, надаються рекомендації для вдосконалення систем безпеки БпАК, що включають інтеграцію нових технологій і адаптацію до нових загроз.

Ключові слова: *кібербезпека, безпілотні авіаційні комплекси, перехоплення, дистанційне управління, криптографічний захист, шифрування, аутентифікація.*

I. Borysov, O. Volkov Cyber security of unmanned aviation complexes and features of protection against interception.

The article considers the key aspects of cyber security of unmanned aerial systems (UAS) in the conditions of modern military conflicts and technological progress, unmanned systems have become important tools for gathering information, conducting intelligence and performing combat missions. However, their widespread use is accompanied by new cyber threats that require specialized measures to ensure security. The article analyzes the main types of cyberthreats that can affect UAS, including the interception of communications, unauthorized access to management systems and the breaking of cryptographic protections.

The article also discusses modern protection methods and technologies, such as cryptographic algorithms, authentication mechanisms and data encryption. In addition, existing standards and practical solutions to ensure the protection of communication channels are analyzed. The last part of the article is devoted to the latest trends in the field of cyber security of UAS and forecasting future threats. Possible solutions and approaches for improving the protection of unmanned systems in the rapidly changing cyber environment are considered, as well as recommendations are provided for improving the security systems of UAS, which include the integration of new technologies and adaptation to new threats.

Keywords: *cybersecurity, unmanned aerial systems, interception, remote control, cryptographic protection, encryption, authentication.*

Постановка проблеми. При відбитті широкомасштабної агресії рф проти України безпілотні авіаційні комплекси (БпАК) мають ключове значення в розвідці, спостереженні та веденні бойових операцій. Однак з розвитком технологій зростає і кількість кіберзагроз, які можуть значно вплинути на ефективність і безпеку застосування цих комплексів. Перехоплення сигналів управління і несанкціоноване дистанційне керування БпАК представляють серйозну загрозу, що може призвести до втрати контролю над апаратом, компрометації місії та небезпеки для виконання завдань військовими підрозділами.

Проблематика забезпечення кібербезпеки БпАК охоплює ряд критичних аспектів [1–3]:

уразливість до кіберзагроз. Атакуючі можуть перехоплювати сигнали управління БпАК, що дозволяє їм контролювати або змінювати поведінку дронів, а також, можуть намагатися інфікувати БпАК шкідливим програмним забезпеченням, яке може порушити роботу або викрасти дані;

недостатній рівень шифрування і аутентифікації. Якщо канали зв’язку не захищені належним чином, це створює можливість для прослуховування і перехоплення даних. Відсутність ефективних механізмів аутентифікації може дозволити неавторизованим особам отримати доступ до системи управління БпАК;

вразливе до атак програмне забезпечення може бути використане для здійснення атак або витоку даних. Якщо процес оновлення програмного забезпечення не є безпечним, зловмисники можуть запровадити шкідливий код;

у міру збільшення кількості БпАК зростає ймовірність проведення атак на великі групи дронів, що в подальшому ускладнює їх відновлення та подальшу експлуатацію;

взаємодія БпАК з іншими програмними сервісами (системами) може створювати додаткові канали впровадження вразливостей.

Отже, ці проблеми підкреслюють необхідність розробки і впровадження комплексних заходів для забезпечення кібербезпеки БпАК, включаючи новітні технології захисту, постійний моніторинг та удосконалення протоколів безпеки.

Аналіз досліджень. Результати аналізу бойового застосування БпАК та останні дослідження в області кібербезпеки БпАК [1–4] показують необхідність їх захисту від різноманітних загроз. Зокрема, слід звернути увагу на зростання кількості атак, спрямованих на перехоплення і маніпулювання сигналами управління БпАК, що може мати критичні наслідки для ефективності їх бойового застосування.

Метою статті є аналіз актуальних кіберзагроз для безпілотних військових апаратів, а також розробка та оцінка методів захисту від них.

Виклад основного матеріалу. У сучасних військових конфліктах БпАК відіграють критично важливу роль, забезпечуючи розвідку, спостереження та виконання різноманітних бойових завдань. Однак їх широке використання робить їх вразливими для кіберзагроз. Основними видами загроз та атак є [4–6]:

перехоплення сигналів управління. Зловмисники можуть перехоплювати і декодувати сигнали управління між оператором і БпАК та можуть генерувати фальшиві сигнали управління, щоб взяти контроль над БпАК;

атаки на програмне забезпечення (ПЗ). Зловмисники можуть впроваджувати віруси, трояни або інше шкідливе ПЗ для порушення функціональності або викрадення даних, а також, можуть використовувати відомі уразливості в програмному забезпеченні для отримання несанкціонованого доступу;

атаки на апаратне забезпечення. Атакуючі можуть намагатися фізично пошкодити апаратне забезпечення БпАК для його нейтралізації;

атаки на комунікаційні системи. Атакуючі можуть прослуховувати та аналізувати дані, що передаються між БпАК і його базовою станцією, а також, можуть створювати фальшиві точки доступу або мережі для спроби отримання даних або впливу на систему управління;

атаки на систему навігації. Зловмисники можуть підробляти сигнали GPS, щоб ввести БпАК в оману щодо його місцезнаходження або взагалі глушити сигнали GPS для перешкоджання навігації БпАК;

атаки на інфраструктуру управління. Атакуючі можуть намагатися зламати сервери або бази даних, які використовуються для управління БпАК, щоб викрасти або змінити інформацію, проводити збої у командуванні або порушення обробки даних;

використання методів соціальної інженерії для отримання доступу до облікових записів або систем управління БпАК.

Ці види загроз вимагають комплексного підходу до забезпечення кібербезпеки БпАК, включаючи використання сучасних технологій захисту, постійний моніторинг систем та регулярні оновлення програмного забезпечення.

Механізми перехоплення і впливу на управлінські системи БпАК можуть включати різноманітні техніки та методи [2, 4–6]. Ось деякі з них.

1. Перехоплення сигналів управління:

зловмисники можуть використовувати радіоапаратуру для перехоплення радіочастотних сигналів управління між оператором і БпАК. Це може включати як управлінські команди, так і дані з сенсорів;

після перехоплення сигналів, зловмисники можуть декодувати їх для розуміння протоколів комунікації і подальшого впливу на систему.

2. Атаки на канали зв’язку:

атакуючі можуть генерувати фальшиві сигнали (Spoofing) для управління БпАК або підробляти інформацію, яку БАК отримує від базової станції;

зловмисники можуть створювати електромагнітні перешкоди (Jamming) для блокування або спотворення комунікацій між БпАК і його контролером.

3. Атаки на протоколи зв’язку:

зловмисники можуть спробувати зламати або обійти механізми аутентифікації, що використовуються для підключення до БпАК;

якщо передача даних зашифрована, атакуючі можуть спробувати знайти вразливості в криптографічних алгоритмах для дешифрування інформації.

4. Внесення шкідливого коду:

атакуючі можуть використовувати вразливості в програмному забезпеченні БпАК для внесення шкідливого ПЗ або вірусів, які можуть змінити його поведінку або знищити дані;

атакуючі можуть підмінити оновлення програмного забезпечення БпАК на шкідливі версії для контролю над системою.

5. Злом системи навігації:

атакуючі можуть підробляти сигнали GPS (GPS-спуфінг), щоб ввести БпАК в оману щодо його реального місцезнаходження;

включення пристроїв для глушіння сигналів GPS (GPS-джаммінг), що призводить до втрати навігаційних даних і можливих аварійних ситуацій.

6. Компрометація комунікаційної інфраструктури:

зловмисники можуть зламати або впливати на базові станції, які управляють БпАК, щоб отримати контроль або порушити їхню роботу;

атакуючі можуть намагатися зламати сервери або системи управління для отримання доступу до інформації або контролю над БпАК.

7. Маніпуляція даними та командами:

атакуючі можуть маніпулювати або змінювати команди, які надходять до БпАК, щоб вплинути на його поведінку;

надання неправдивих або шкідливих даних БпАК, які можуть призвести до некоректних рішень або дій.

Ці механізми демонструють широкий спектр можливих атак на управлінські системи БпАК і підкреслюють важливість впровадження комплексних заходів для захисту від таких загроз.

Ось кілька реальних випадків атак на БпАК, які демонструють різноманітні способи, якими зловмисники можуть вплинути на ці системи:

1. Атака на дрони у конфліктних зонах. У 2018 році в Венесуелі відбулася спроба замаху на президента Мадуро за допомогою безпілотних літальних апаратів. Дрони, які були оснащені вибуховими пристроями, вибухнули під час виступу президента. Зловмисники використовували дрони для доставки вибухових пристроїв, це свідчить про можливість використання БпАК для атак на високопрофільні цілі.

2. GPS-спуфінг у Дубаї. У 2016 році в Дубаї дрони, які проводили геодезичні дослідження, були піддані GPS-спуфінгу. Це призвело до помилкових даних про їхнє

місцезнаходження. Зловмисники підробили сигнали GPS, щоб ввести дрони в оману і змусити їх працювати не в тому місці, де їх було заплановано.

3. Атака на комерційний дрон в США. У 2020 році дрон компанії Amazon був зламаний з метою отримання несанкціонованого доступу до комерційних даних. Зловмисники змогли використовувати уразливості в програмному забезпеченні дрона та перехоплювати його комунікаційні канали для отримання конфіденційної інформації.

4. Використання дронів для нагляду. У 2017 році в Китаї дрони, що використовувалися для нагляду, були захоплені і перепрограмовані для збору інформації та шпигунства. Атакуючі отримали доступ до системи управління дронами і перепрограмували їх для збору конфіденційної інформації.

Широкомасштабне вторгнення рф в Україну показало, що БпАК відіграють важливу роль у збройному протистоянні і стали мішенню для різних кіберзагроз і атак. Ось кілька прикладів.

1. Атаки на системи управління БпАК. Під час конфлікту на Донбасі неодноразово відзначено випадки перехоплення сигналів управління БпАК. Атакуючі використовували спеціальне обладнання для перехоплення і декодування радіочастотних сигналів. Зловмисники змогли змінити або вплинути на команди, що надходять до дронів, це дозволило їм контролювати або порушити роботу безпілотників.

2. Атаки на GPS-системи. Неодноразово повідомлялися випадки GPS-спуфінгу, коли російські сили намагалися підробляти сигнали GPS, що призводило до неправильної навігації дронів і спотворення даних розвідки.

3. Кібернетичні атаки на інфраструктуру БпАК. Це включало в себе спроби зламу систем управління дронами або проникнення у сервери для отримання доступу до даних. Атакуючі використовували різні методи, включаючи шкідливе ПЗ, фішинг або експлойти для отримання доступу до управлінських систем і даних.

4. Неодноразово зафіксовані випадки, коли обидві сторони використовують засоби радіоелектронної боротьби для перехоплення, глушіння сигналів або знищення дронів.

Ці випадки підкреслюють важливість забезпечення кібербезпеки та захисту дронів від різноманітних загроз. Вони також вказують на різні способи, якими БпАК можуть бути використані як інструменти для атак.

Таким чином, захист БпАК від перехоплення сигналів і комунікацій є критично важливим для забезпечення їхньої безпеки та ефективності. Основними ключовими особливостями і методами захисту від перехоплення є:

використання сучасних криптографічних алгоритмів для шифрування сигналів управління та даних, що передаються між БпАК і контролером;

аутентифікація і авторизація (впровадження багаторівневої аутентифікації, наприклад, паролі, біометричні дані та токени, для доступу до системи управління БпАК, включаючи перевірку прав користувачів);

зміна частот радіозв’язку за певним алгоритмом для ускладнення перехоплення і декодування сигналів (Frequency Hopping) та використання адаптивних алгоритмів для вибору частот і швидкої зміни частот для підвищення стійкості до перехоплення;

впровадження технологій для протидії глушінню сигналів, таких як автоматичне виявлення і переключення на вільні частоти та використання технологій для виявлення і протидії спуфінговим атакам, таких як перевірка автентичності сигналів;

встановлення систем для постійного моніторингу сигналів і виявлення аномалій або спроб перехоплення;

використання аналізу трафіку для виявлення підозрілих або ненормальних комунікаційних патернів;

впровадження захищених мікросхем і плат, які мають вбудовані механізми захисту від несанкціонованого доступу;

постійне оновлення програмного забезпечення БпАК для усунення вразливостей і захисту від нових загроз;

застосування безпечних протоколів для обміну даними, таких як SSL/TLS;

регулярне тестування систем на стійкість до різних типів атак, включаючи перехоплення, проведення незалежних аудитів і перевірок для виявлення можливих вразливостей.

Ці методи та технології забезпечують всебічний підхід до захисту БпАК від перехоплення сигналів і контролюють рівень їхньої безпеки в умовах сучасних кіберзагроз.

Крім того, технічні засоби захисту є критично важливими для забезпечення безпеки БпАК [3–6]. Ось основні компоненти та принципи використання криптографії, аутентифікації та шифрування даних.

1. Криптографія:

симетричне шифрування. Використовується один ключ для шифрування і дешифрування даних. Наприклад, AES (Advanced Encryption Standard). Переваги: швидкість і ефективність при великих обсягах даних. Недоліки: проблема безпечної передачі ключа;

асиметричне шифрування. Використовуються пари ключів: публічний і приватний. Публічний ключ для шифрування, приватний для дешифрування. Наприклад, RSA (Rivest-Shamir-Adleman). Переваги: безпека при передачі ключів, можливість підпису даних. Недоліки: повільніше порівняно із симетричним шифруванням;

гібридне шифрування. Поєднує симетричне і асиметричне шифрування для забезпечення високого рівня безпеки і швидкості. Наприклад, використання RSA для передачі симетричного ключа AES;

хеш-функції. Використовуються для забезпечення цілісності даних, перетворюючи інформацію в унікальний хеш-код. Наприклад, SHA-256, MD5. Переваги: легкість перевірки цілісності даних. Недоліки: не забезпечує конфіденційність даних.

2. Аутентифікація:

паролі. Стандартний метод аутентифікації, який включає в себе використання паролів або PIN-кодів. Переваги: простота впровадження. Недоліки: слабка захищеність, якщо паролі не є складними і змінюються не регулярно;

багатофакторна аутентифікація (MFA). Включає в себе два або більше факторів для підтвердження особи. Може бути комбінацією пароля, біометричних даних або одноразових кодів. Переваги: підвищена безпека. Недоліки: може бути більш складним у впровадженні і використанні;

біометричні дані. Використовують унікальні фізичні характеристики для аутентифікації, такі як відбитки пальців або сітківка ока. Переваги: високий рівень безпеки та зручність. Недоліки: може бути схильним до зловживань або помилок;

сертифікати цифрового підпису. Використовують пари ключів і сертифікати для підтвердження особи. Сертифікати видаються на основі довірених центрів сертифікації. Переваги: безпека і можливість перевірки автентичності даних. Недоліки: необхідність управління сертифікатами.

3. Шифрування даних:

шифрування даних при передачі. Забезпечує захист даних під час їх передачі каналами зв’язку. Використовуються такі протоколи, як TLS/SSL (Transport Layer Security/Secure Sockets Layer). Переваги: захист даних від перехоплення під час передачі. Недоліки: необхідність належного управління сертифікатами та ключами;

шифрування даних на диску. Забезпечує захист даних, що зберігаються на пристроях. Наприклад, AES може бути використано для шифрування файлів і баз даних. Переваги: захист

даних у випадку втрати або крадіжки пристроїв. Недоліки: необхідність управління ключами і можливість впливу на продуктивність;

шифрування метаданих. Захищає не тільки самі дані, але і метадані, такі як інформація про файли та їх структуру. Переваги: додатковий рівень захисту. Недоліки: може бути складним у реалізації та управлінні.

Критично важливим для забезпечення безпеки передачі даних є захист каналів зв’язку, особливо у випадку БпАК та інших критичних систем. Ось основні методи і технології захисту каналу зв’язку.

1. Шифрування каналу зв’язку:

SSL/TLS (Secure Sockets Layer/Transport Layer Security). Забезпечує шифрування даних, що передаються мережею і аутентифікацію сторін зв’язку. Широко використовуються в Інтернеті для захисту вебтрафіку. Переваги: високий рівень захисту даних від перехоплення і маніпуляцій. Недоліки: може впливати на продуктивність через додаткове навантаження на обробку даних;

IPsec (Internet Protocol Security). Протокол для захисту даних на рівні мережі, який забезпечує шифрування і аутентифікацію пакетів IP-трафіку. Переваги: широка підтримка і можливість захисту всього IP-трафіку. Недоліки: може бути складним в налаштуванні та управлінні;

VPN (Virtual Private Network). Створює зашифроване з’єднання через публічні мережі для забезпечення приватності і захисту даних. Переваги: захист даних від перехоплення в публічних мережах. Недоліки: може знижувати швидкість зв’язку.

2. Аутентифікація і авторизація:

багатофакторна аутентифікація (MFA). Включає кілька рівнів перевірки (наприклад, пароль плюс одноразовий код), щоб підтвердити особу користувача. Переваги: підвищує безпеку доступу до каналу зв’язку. Недоліки: може бути складним у впровадженні та використанні;

цифрові сертифікати. Використовуються для підтвердження ідентичності та встановлення зашифрованих з’єднань між двома сторонами. Переваги: забезпечує верифікацію і безпеку підключення. Недоліки: необхідність управління сертифікатами і довіреними центрами сертифікації.

3. Технології захисту від глушіння та перешкод:

частотна стрибкоподібність (Frequency Hopping). Зміна частот радіозв’язку за певним алгоритмом для ускладнення перехоплення і глушіння сигналів. Переваги: підвищує стійкість до перехоплення і глушіння. Недоліки: може ускладнити налаштування і синхронізацію;

антиджаммінг (Anti-jamming). Технології для виявлення і протидії глушінню сигналів, такі як автоматичне перемикання на чисті частоти. Переваги: підвищує надійність зв’язку в умовах електромагнітних перешкод. Недоліки: вимагає спеціалізованого обладнання та налаштування.

4. Контроль доступу і моніторинг:

системи контролю доступу. Впровадження засобів для обмеження доступу до каналу зв’язку на основі прав користувачів або груп. Переваги: захист від несанкціонованого доступу. Недоліки: потребує постійного моніторингу і управління правами доступу;

моніторинг трафіку. Використання інструментів для постійного моніторингу мережевого трафіку і виявлення аномалій або спроб перехоплення. Переваги: швидке виявлення і реагування на загрози. Недоліки: може бути ресурсоємним і вимагати спеціалізованого обладнання.

5. Інші методи:

захист від атак типу “Man-in-the-Middle” (MITM). Використання криптографії для забезпечення цілісності і конфіденційності даних, що передаються, щоб унеможливити

підробку або прослуховування з боку третьої сторони. Переваги: захищає від перехоплення і підробки даних. Недоліки: може вимагати складних алгоритмів і налаштувань;

сегментація мережі. Розділення мережі на сегменти для обмеження можливості доступу до критичних систем і даних. Переваги: знижує ризики при компрометації одного сегмента. Недоліки: може ускладнити управління і налаштування мережі.

Використання цих методів і технологій забезпечує багаторівневий підхід до захисту каналу зв’язку, знижуючи ризики перехоплення, глушіння і несанкціонованого доступу.

Аналіз сучасних рішень і стандартів захисту для БпАК включає в себе огляд існуючих технологій та підходів до забезпечення безпеки. Основні аспекти таких рішень і стандартів охоплюють захист комунікацій, захист даних, управління доступом, а також адаптацію до нових загроз.

Стандарти захисту від кіберзагроз:

NIST Cybersecurity Framework. Рамка для управління кіберзахистом, включаючи ідентифікацію, захист, виявлення, реагування і відновлення. Дозволяє організаціям розробити комплексний план кіберзахисту. Широко використовується в США і міжнародній практиці;

ISO/IEC 27001. Стандарт для системи управління інформаційною безпекою. Визначає вимоги для впровадження та підтримки системи управління безпекою інформації. Забезпечує структурований підхід до захисту інформації;

Zero Trust Security Model. Модель безпеки, яка припускає, що жоден користувач або пристрій не є довіреним, поки не буде перевірено. Підходить для сучасних розподілених і хмарних середовищ. Фокусується на постійній перевірці і контролі доступу;

Blockchain для безпеки даних. Використання технології блокчейн для забезпечення цілісності та автентичності даних. Може використовуватися для захисту транзакцій і даних у реальному часі. Забезпечує додатковий рівень захисту завдяки незмінності записів;

AI і Machine Learning для кіберзахисту. Використання штучного інтелекту та машинного навчання для виявлення аномалій і загроз у реальному часі. Збільшує ефективність моніторингу та реагування на кіберзагрози. Допомагає автоматизувати процеси виявлення та реагування на загрози.

Аналіз цих рішень і стандартів допомагає забезпечити комплексний підхід до захисту БпАК і інших критичних систем від різних типів загроз. Ось кілька прикладів реалізації таких рішень.

1. Шифрування та захист даних:

військові дрони США, такі як MQ-9 Reaper, використовують шифрування AES для захисту комунікацій між дронами і командними центрами. Це забезпечує захист передачі відео та інших даних від перехоплення і прослуховування. Як результат підвищення рівня безпеки даних і команд, що передаються через різні канали зв’язку;

інфраструктура критичних об’єктів. Для захисту комунікацій і даних в інфраструктурі критичних об’єктів, таких як енергетичні станції, використовуються протоколи TLS для шифрування інформації, що передається між контролерами і серверами. Як результат, зменшення ризику несанкціонованого доступу до критичних даних і контролю.

2. Аутентифікація та управління доступом:

компанія DJI використовує багатофакторну аутентифікацію для доступу до своїх систем управління дронами DJI. Користувачі повинні підтвердити свою особу через мобільний додаток і ввести пароль для доступу до функцій дрона. Як результат, збільшення рівня безпеки доступу до дронів і запобігання несанкціонованому управлінню;

системи управління доступом у хмарних середовищах. Хмарні платформи для управління БпАК часто використовують OAuth 2.0 і OpenID Connect для забезпечення безпечного доступу до даних і ресурсів. Це дозволяє інтегрувати сторонні сервіси і

забезпечити контроль доступу на основі токенів. Як результат, гнучке управління доступом і інтеграція з іншими сервісами при забезпеченні високого рівня безпеки.

3. Захист комунікацій:

військові дрони використовують технології частотної стрибкоподібності (FHSS) для захисту від глушіння і перехоплення сигналів. Це дозволяє змінювати частоти радіозв’язку у часі, ускладнюючи виявлення і перешкоджання;

впровадження адаптивних систем частотного стрибка (AFH) в безпроводових комунікаціях для безпілотних транспортних систем, що автоматично змінюють частоти залежно від наявних перешкод.

Критично важливим для забезпечення безпеки БпАК в умовах швидкого розвитку технологій є прогнозування нових типів загроз. Ось кілька потенційних загроз і можливих рішень для зниження їх рівня [5–7]:

1. Загрози на основі штучного інтелекту для атак на БАК, включаючи автоматизовані атаки, адаптивні алгоритми для обходу захисту і дезінформаційні кампанії. Можливими рішеннями є розробка систем AI, які здатні виявляти аномалії і небезпечні поведінки, базуючись на машинному навчанні та комбінація традиційних і AI-орієнтованих методів для посилення кіберзахисту.

2. Квантові комп’ютери можуть потенційно розшифровувати дані, які захищені сучасними криптографічними алгоритмами. Можливими рішеннями є розробка і впровадження нових криптографічних алгоритмів, стійких до атак квантових комп’ютерів та використання квантових ключів для забезпечення високого рівня безпеки.

3. Використання автономних дронів або роботизованих систем для атак на інші БпАК або критичні об’єкти. Можливими рішеннями є розробка і впровадження рішень для захисту від автономних атак, таких як виявлення і нейтралізація загроз.

4. Злом і маніпуляція компонентами Інтернету речей (IoT), які інтегруються з БпАК. розробка і впровадження спеціалізованих рішень для захисту компонентів IoT, таких як шифрування даних і аутентифікація пристроїв та впровадження строгих політик контролю доступу до IoT-компонентів і регулярне оновлення програмного забезпечення.

5. Злом або маніпуляції в динамічних мережах ad-hoc, де БпАК спілкуються між собою без фіксованої інфраструктури. Можливими рішеннями є розробка і впровадження протоколів комунікації, які забезпечують безпеку в ad-hoc мережах, використання криптографії для забезпечення захищеного зв’язку між пристроями в ad-hoc мережах.

Таким чином, ці рекомендації допоможуть у створенні більш стійкої та ефективної системи безпеки для безпілотних авіаційних комплексів, що забезпечить їхню захищеність від нових і існуючих загроз.

Висновки та перспективи подальшого дослідження

Дослідження виявило, БпАК стикаються з серйозними кіберзагрозами, такими як перехоплення сигналів управління, дистанційне захоплення контролю, вразливості ПЗ та ін. Найефективнішими методами захисту є криптографічний захист, багаторівнева аутентифікація, інтеграція механізмів безпеки в ПЗ та фізичний захист комунікацій [3–6]. Аналіз показує, що ці рішення значно підвищують захист БпАК від кіберзагроз, їх ефективність підтверджена реальними кейсами.

Попри досягнуті результати, є питання для подальших досліджень, зокрема розробка нових методів шифрування, стійких до майбутніх загроз, таких як квантові обчислення, а також дослідження захисту під час масованих атак. Подальші вдосконалення можуть включати адаптацію аутентифікаційних систем до бойових умов, впровадження машинного навчання для активного виявлення загроз і розробку нових комунікаційних протоколів, а також, розробка інтегрованих систем, що поєднують криптографію, контроль доступу та фізичний захист.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. P.-Y. Kong, A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles," in IEEE Access, vol. 9, pp. 148244–148263, 2021, DOI: 10.1109/ACCESS.2021.3124996.

2. Z. Yu, Z. Wang, J. Yu, D. Liu, H. Herbert Song and Z. Li, "Cybersecurity of Unmanned Aerial Vehicles: A Survey," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 39, no. 9, pp. 182–215, Sept. 2024, DOI: 10.1109/MAES.2023.3318226.

3. R. Alkadi, N. Alnuaimi, C. Y. Yeun and A. Shoufan, "Blockchain Interoperability in Unmanned Aerial Vehicles Networks: State-of-the-Art and Open Issues," in *IEEE Access*, vol. 10, pp. 14463–14479, 2022, DOI: 10.1109/ACCESS.2022.3145199. k

4. R. Guo, M. Huang, J. Li and J. Wang, "Cybersecurity of Unmanned Aerial Vehicles: A Survey," *2021 14th International Conference on Advanced Computer Theory and Engineering (ICACTE)*, Hangzhou, China, 2021, pp. 57–64, DOI: 10.1109/ICACTE53799.2021.00017.

5. L. Li, K. Qu and K.-Y. Lin, "A Survey on Attack Resilient of UAV Motion Planning," *2020 IEEE 16th International Conference on Control & Automation (ICCA)*, Singapore, 2020, pp. 558–563, DOI: 10.1109/ICCA51439.2020.9264513.

6. R. Hamadi, H. Ghazzai and Y. Massoud, "Reinforcement Learning Based Intrusion Detection Systems for Drones: A Brief Survey," *2023 IEEE International Conference on Smart Mobility (SM)*, Thuwal, Saudi Arabia, 2023, pp. 104–109, DOI: 10.1109/SM57895.2023.10112557.

7. M. Adil, M. A. Jan, Y. Liu, H. Abulkasim, A. Farouk and H. Song, "A Systematic Survey: Security Threats to UAV-Aided IoT Applications, Taxonomy, Current Challenges and Requirements With Future Research Directions," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 1437–1455, Feb. 2023, DOI: 10.1109/TITS.2022.3220043.

DOI: 10.58254/viti.6.2024.04.68

УДК 004.051

Волошин В. В. ORCID: 0009-0004-7121-0950 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Данилюк І. А. ORCID: 0000-0003-0955-0108 (ВІТІ ім. Героїв Крут)
Карпенко А. О. ORCID: 0000-0002-8372-6303 (ВІТІ ім. Героїв Крут)
канд. ф.-м. наук Ковальчук Б. П. ORCID: 0000-0001-5219-7624 (ВІТІ ім. Героїв Крут)

ВДОСКОНАЛЕННЯ АЛГОРИТМУ ПОБУДОВИ ОПТИМАЛЬНОГО МАРШРУТУ З ВИКОРИСТАННЯМ «ГАРЯЧИХ ЗОН»

У статті авторами розглянуто вирішення проблеми планування оптимальних маршрутів у динамічному середовищі з використанням географічних даних OpenStreetMap (OSM) для території України. В умовах конфліктних ситуацій та ведення бойових дій виникає необхідність адаптації класичних алгоритмів пошуку маршрутів для врахування специфічних обмежень на місцевості. Основна мета дослідження – розробка адаптивного алгоритму A, який враховує наявність зон підвищеного ризику (“гарячих зон”), які можуть значно вплинути на ефективність та безпечність розрахованого маршруту. Для реалізації поставленої мети був проведений аналіз існуючих алгоритмів пошуку найкоротшого шляху з використанням класичного алгоритму A* та його евристичної функції, що враховує відстань між точками маршруту. Розглянута алгоритмічна особливість модифікації алгоритму A*, що включає врахування додаткового коефіцієнта вартості для "гарячих зон". Запропонований підхід базується на додаванні адаптивного множника, який обмежує можливість прокладання маршруту через небезпечні ділянки. Для перевірки запропонованого методу було використано OSM-дані, що містять лише базову інформацію про дороги без врахування воєнних обмежень. Це обмеження підкреслює важливість додаткового аналізу таких факторів, як безпека та ризик при плануванні маршруту. Отримані результати показують ефективність розробленого адаптивного алгоритму A* для задачі побудови маршруту в умовах динамічного середовища, зокрема з можливістю уникнення небезпечних зон ("гарячих зон"). Висновки проведеного дослідження підтверджують, що додатковий коефіцієнт вартості у "гарячих зонах" покращує точність маршруту та підвищує безпеку пересування. Розроблений алгоритм може застосовуватися для автоматизованого планування маршрутів у ситуаціях, де критично важливо враховувати змінні фактори ризику та специфічні умови на місцевості.*

Ключові слова: *алгоритм A*, маршрутизація, "гарячі зони", OpenStreetMap, динамічне середовище, найкоротший шлях, воєнні обмеження.*

V. Voloshyn, I. Danylyuk, A. Karpenko, B. Kovalchuk Development of an optimal route planning algorithm using hot zones

The authors in the article address the problem of planning optimal routes in a dynamic environment using OpenStreetMap (OSM) geographic data for the territory of Ukraine. Amid conflict situations and active hostilities, there is a need to adapt classical route-finding algorithms to account for specific terrain constraints. The main aim of the research is to develop an adaptive A algorithm that considers high-risk areas ("hot zones") which can significantly impact the efficiency and safety of the calculated route. To achieve this goal, the authors conducted an analysis of existing shortest path search algorithms using the classic A* algorithm and its heuristic function, which considers the distance between route points. The study explores a modified version of the A* algorithm that includes an additional cost factor for "hot zones." The proposed approach introduces an adaptive multiplier that restricts route planning through dangerous areas. To validate the proposed method, OSM data containing only basic road information, without military restrictions, was used. This limitation highlights the importance of additional analysis of factors such as safety and risk in route planning. The results demonstrate the effectiveness of the developed adaptive A* algorithm in constructing routes in a dynamic environment, particularly with the ability to avoid dangerous ("hot") zones. The study's conclusions confirm that adding a cost factor in "hot zones" improves route accuracy and enhances travel safety. The developed algorithm can be applied to automated route planning in scenarios where it is crucial to consider variable risk factors and specific terrain conditions.*

Keywords: *A* algorithm, routing, hot zones, OpenStreetMap, dynamic environment, shortest path, military restrictions.*

Постановка завдання

Постановка проблеми у задачі побудови оптимального маршруту полягає у забезпеченні швидкого, безпечного та ефективного планування шляхів у динамічних умовах, які включають різноманітні ризики та обмеження. У мирних умовах алгоритми вибору найкоротшого шляху,

такі як класичний A*, успішно виконують завдання, проте в умовах бойових дій або інших надзвичайних ситуацій виникає потреба в адаптації до специфічних загроз. Однією з ключових перешкод є наявність "гарячих зон" – територій з підвищеним рівнем ризику, яких необхідно уникати або обирати обхідні шляхи. Ця проблема є актуальною для таких наукових і практичних сфер, як військове планування, безпека транспорту та системи управління надзвичайними ситуаціями, оскільки точне врахування ризикованих зон дозволяє підвищити безпеку переміщення і зменшити ресурси, необхідні для реалізації кожного маршруту. Геопросторові дані OpenStreetMap (OSM) [1], які використовуються для побудови маршрутів, надають лише базову інформацію про дорожню інфраструктуру, без урахування факторів підвищеної небезпеки, спричинених бойовими діями чи іншими загрозами. Отже, актуальним є розроблення адаптивного алгоритму, здатного враховувати динамічні обмеження та забезпечувати безпеку при переміщенні через території, які зазнали змін у зв’язку з військовою діяльністю чи іншими небезпечними факторами.

Аналіз останніх публікацій

Останні дослідження в області планування оптимальних маршрутів із врахуванням динамічних умов значною мірою зосереджені на удосконаленні алгоритмів пошуку шляхів [2], таких як A*, Dijkstra та їхніх модифікацій для роботи в середовищах з ризиками та обмеженнями [3]. Зокрема, дослідження в рамках військового планування та інтелектуального управління транспортом спрямовані на розроблення адаптивних алгоритмів, що можуть враховувати часові та географічні змінні. Наприклад, дослідження Кортеза та колег [4] розглядає адаптивний підхід до A* для роботи з динамічними перешкодами. Проте більшість із цих робіт зосереджена на теоретичних моделях і лише частково охоплює проблему інтеграції актуальних даних про ризики в режимі реального часу. Водночас, важливою частиною, що залишається невирішеною, є розроблення практичного підходу до адаптації традиційних алгоритмів найкоротшого шляху з урахуванням специфічних обмежень, пов’язаних із веденням бойових дій, що робить критичним використання "гарячих зон" у маршрутах на основі даних OSM.

Проведений аналіз виявив необхідність вдосконалити алгоритм A*, оскільки його класична реалізація не враховує специфічних аспектів реального часу та зон підвищеного ризику, що особливо важливо в умовах динамічних середовищ, як-от зони бойових дій або інтенсивного транспортного трафіку. Використання так званих "гарячих зон" дозволяє алгоритму більш точно адаптувати маршрути до змінних умов, таких як нові перешкоди, небезпечні ділянки чи блокування, що може значно покращити безпеку та ефективність маршрутизації. Вдосконалений підхід також враховує можливість оновлення інформації про ці зони в режимі реального часу, що розширює можливості алгоритму в контексті військових та інтелектуальних транспортних застосувань.

Метою даної статті є вдосконалення класичного алгоритму A* шляхом інтеграції адаптивного коефіцієнта ризику, що дозволить ефективніше будувати маршрути, уникаючи "гарячих зон" в умовах бойових дій, враховуючи обмеженість доступних геопросторових даних.

Виклад основного матеріалу

У цьому дослідженні проведено комплексний аналіз проблем, пов’язаних з вирішенням задачі маршрутизації в динамічному середовищі, використовуючи географічні дані з OSM для території України. Основним завданням є планування оптимального маршруту між двома точками з урахуванням топографічних, дорожніх, та інших характеристик місцевості. Задача найкоротшого шляху полягає у пошуку мінімальної відстані між вершинами в графі (де граф представлений даними OSM для України), що є абстрактним математичним об’єктом із множинами вершин та ребер [5]. За Парвін Шармою і Неї Курханом, задача найкоротшого шляху визначається як мінімізація довжини (вартості) між вузлами [6], а Карішма Талан та

Г. Р. Бамнот підкреслюють її як пошук найшвидшого маршруту [7]. У загальному вигляді, це пошук шляху з найменшою вартістю між двома вершинами графа [8].

Одним із найпоширеніших алгоритмів для вирішення задач найкоротшого шляху є алгоритм A* (A-star), який використовує евристичні оцінки для зменшення кількості перевірених вузлів у процесі пошуку [9]. Результати застосування алгоритму A* до даних OSM показали його ефективність у генерації маршрутів на основі відкритих геопросторових даних. Однак OSM-дані містять лише інформацію про дороги та маршрути, які придатні для загального використання [10], але не включають специфічних обмежень, зумовлених воєнною обстановкою чи (та) реальними бойовими діями. Хоча алгоритм успішно знаходить найкоротший шлях, він не враховує ризиків, пов'язаних із переміщенням через "гарячі зони". Для повноцінного планування маршруту в умовах військових дій важливо інтегрувати інформацію про такі зони, оскільки вони можуть значно впливати на безпечність та ефективність побудованого маршруту.

Для подолання цієї проблеми було розроблено адаптивний алгоритм на основі A*, що враховує динамічні зміни середовища. Цей підхід доповнює алгоритм A* обробкою "гарячих зон", дозволяючи алгоритму змінювати маршрут відповідно до поточної навколишньої обстановки. Він працює шляхом додавання додаткової вартості для проходження через небезпечні зони, що змушує алгоритм уникати їх у процесі пошуку оптимального шляху. Таким чином, новий адаптивний алгоритм надає пріоритет маршрутам, що мінімізують ризики, пов'язані з пересуванням через небезпечні ділянки. Це робить його більш гнучким та ефективним у випадках, де обставини змінюються динамічно.

Експериментальні результати досліджень свідчать, що адаптивний алгоритм демонструє покращену ефективність у порівнянні з класичним A*, особливо в умовах, де необхідно уникати певних зон. Такий підхід враховує не тільки відстань, але й фактори безпеки, що є вирішальним для складних маршрутів. Це робить його корисним у завданнях планування складних маршрутів, особливо у випадках, коли наявні зовнішні чинники, які впливають на безпечність чи швидкість переміщення.

Алгоритм A* працює з графом, що представляє просторову структуру дороги, де вузли відповідають перехрестям або кінцевим точкам доріг, а ребра – шляхам між ними з певними характеристиками, такими як довжина та обмеження швидкості. Для перевірки ефективності та точності роботи алгоритму A* було використано дані OSM, які конвертувалися у граф для подальшої обробки. Процес конвертації даних з OSM у граф складається з кількох важливих етапів. Спочатку дані OSM завантажуються для обраного регіону за допомогою API або з готових файлів (зазвичай у форматах .osm або .pbf). Потім ці дані проходять фільтрацію: залишаються тільки елементи, пов'язані з транспортними маршрутами, як-от *highway, motorway, secondary, residential.* Інші елементи, які не впливають на планування маршрутів, відкидаються.

На етапі створення вершин, кожен вузол у графі відповідає перехрестю або кінцевій точці дороги. Усі унікальні координати з OSM перетворюються на вершини, де кожна вершина має ідентифікатор, широту та довготу. Набір вершин позначається як

$$V=\{v_1,v_2,\ldots,v_n\}, \quad (1)$$

де кожна вершина v_i представляє певне географічне положення.

Далі відбувається створення ребер. Кожне ребро графа представляє дорогу, що з'єднує вузли. Воно має напрямок, довжину (розраховану за Евклідовою або Манхеттенською метрикою). Граф представлений як

$$G=(V, E), \quad (2)$$

де $E=\{e_1,e_2,\ldots,e_m\}$ – набір ребер.

Для ефективної роботи алгоритму A* на великих картах граф оптимізується. Наприклад, зменшується кількість вершин шляхом об'єднання прямих відрізків в одне ребро. Після

завершення побудови граф зберігається в базі даних або у форматах для швидкого доступу, як-от матриця суміжності або список суміжності.

Класичний алгоритм A* використовує евристичну функцію для оцінки вартості шляху *f(n)*, яка обчислюється як сума двох складових:

$$f(n) = g\,(n) + h(n), \tag{3}$$

де *g(n)* – фактична вартість маршруту від початкової точки до вузла;

h(n) – евристична оцінка вартості маршруту від вузла до кінцевої точки (зазвичай Евклідова або Манхеттенська відстань).

Для адаптації алгоритму до обробки "гарячих зон" вводиться додатковий коефіцієнт вартості *α(n)*, що відображає підвищену вартість проходження через такі зони. Модифікована функція вартості для кожного вузла виглядає наступним чином:

$$f(n) = g\,(n) + h(n) + \alpha\,(n), \tag{4}$$

де $\alpha(n)$ – додаткова вартість для вузлів у "гарячих зонах". Функція евристики *h(n)*, як і в класичному алгоритмі A*, оцінює залишкову відстань до цілі, використовуючи, наприклад, Евклідову відстань:

$$h(n) = \sqrt{(x_{end} - x_n)^2 + (y_{end} - y_n)^2}. \tag{5}$$

Щоб додати динамічне врахування "гарячих зон", вводимо додаткову функцію *α(n)*, яка змінює основну вартість залежно від знаходження вузла в "гарячій зоні":

$$a(n) = \begin{cases} w_{hot}, & \text{якщо } n \text{ знаходиться в "гарячій зоні"} \\ 0, & \text{якщо } n \text{ не належить до "гарячої зони"} \end{cases}. \tag{6}$$

Тут w_{hot} – додаткова вартість проходження через "гарячу зону", залежна від ступеня небажаності або інтенсивності цієї зони.

Адаптивний алгоритм A* функціонує за такою послідовністю кроків, що враховують динамічну зміну вартості шляхів залежно від наявності "гарячих зон".

Алгоритм починає з ініціалізації двох основних структур даних – відкритого списку вузлів *(open list)* та закритого списку вузлів *(closed list)*. Відкритий список включає всі вузли, які будуть розглянуті для подальшої обробки, тоді як закритий список містить вузли, що вже були опрацьовані. Для кожного вузла *n* встановлюється початкове значення функції вартості $g(n)=\infty$ (символізує нескінченну віддаленість, тобто шлях ще не знайдений), а евристична функція *h(n)* розраховується на основі обраного методу, такого як Евклідова відстань. Ця евристика відображає приблизну відстань від вузла *n* до кінцевої точки. Далі для кожного вузла обчислюється значення функції $f(n)=g(n)+h(n)$, яка відображає поточну оцінку вартості проходження через цей вузол.

На кожній ітерації алгоритм обирає вузол із відкритого списку, який має мінімальне значення *f(n).* Цей вузол вважається найбільш перспективним для подальшого пошуку оптимального шляху. Вибір мінімального *f(n)* забезпечує баланс між фактично пройденою відстанню *g(n)* та оцінкою залишкового шляху *h(n)*.

Для кожного обраного вузла *n* алгоритм розглядає його сусідів *m* і обчислює нове значення функції *g(m)*, що включає:

$$g(m)=g(n)+cost(n,m)+\alpha(m), \tag{7}$$

де *cost(n, m)* – вага (або вартість) переходу між вузлами *n* та *m*, а *α(m)* – додатковий коефіцієнт, що враховує підвищену вартість при проходженні через "гарячі зони".

Важливо, що якщо вузол *m* ще не був оброблений або нове значення *g(m)* виявиться меншим за попереднє, значення *g(m)* оновлюється, і вузол додається до відкритого списку. Цей підхід дає змогу алгоритму адаптивно обирати вузли, що уникатимуть зон з високою вартістю, якщо альтернативні шляхи є менш витратними.

Процес продовжується, доки не досягнуто кінцевої точки або відкритий список не стане порожнім. У випадку досягнення цілі, алгоритм повертає оптимальний маршрут; якщо ж

відкритий список порожній і ціль не досягнута, алгоритм сигналізує про відсутність можливого шляху.

Розрахунок вартості проходження через "гарячі зони" проводимо наступним чином. Для кожного ребра *e*, що з'єднує вузли *n* та *m*, якщо відома його вага *w(e)*, загальна вартість шляху через "гарячу зону" визначається як:

$$g(m)=g(n)+w(e)+\alpha(m), \quad (8)$$

де *α(m)* адаптивно змінюється залежно від поточних умов, наприклад, часу або ситуації, що впливає на актуальність уникнення "гарячої зони". У цьому контексті *α(m)* можна розглядати як функцію часу або іншого параметру, що динамічно коригується в ході виконання алгоритму

$$a(m,t)=\begin{cases} w_{hot}(t), & \text{якщо } m \text{ знаходиться в "гарячій зоні" на момент } t \\ 0, & \text{якщо } m \text{ не належить до "гарячої зони"} \end{cases}. \quad (9)$$

Для перевірки роботи даного алгоритму було написано програму мовою програмування C#:

```
// Евристична функція з урахуванням "гарячих зон"
Func<uint, float> heuristic = vertex =>
{
    var vertexLocation = graph.GetVertex(vertex);
    var endLocation = graph.GetVertex(endVertex);
    var dx = vertexLocation.Latitude - endLocation.Latitude;
    var dy = vertexLocation.Longitude - endLocation.Longitude;
    var baseHeuristic = (float)Math.Sqrt(dx * dx + dy * dy);
    return baseHeuristic + GetHeatFactor(vertex);
};
int i = 0;
while (priorityQueue.Count > 0)
{
    i++;
    var (currentDistance, currentVertex) = priorityQueue.Min;
    priorityQueue.Remove(priorityQueue.Min);

    if (currentVertex == endVertex)
        break;

    foreach (var edge in graph.GetEdgeEnumerator(currentVertex))
    {
        var neighbor = edge.To;
        // Додаємо вартість зони до ваги
        var weight = edge.Data.Distance + GetHeatFactor(neighbor);
        var distance = currentDistance + weight;

      if (!distances.ContainsKey(neighbor) || distance < distances[neighbor])
      {
        priorityQueue.Remove((distances.GetValueOrDefault(neighbor, float.MaxValue)
                + heuristic(neighbor), neighbor));
        distances[neighbor] = distance;
        previous[neighbor] = currentVertex;
        priorityQueue.Add((distance + heuristic(neighbor), neighbor));
      }
    }
}
```

Для перевірки роботи реалізації даного стандартного алгоритму А*, маршрут був прокладений через місто Охтирка (рис. 1). На рисунку маршрут зображено зеленим кольором. Адаптивний алгоритм А* при додаванні "гарячої зони" в місті Охтирка при інших однакових даних побудував маршрут іншими дорогами (на рисунку маршрут зображено синім кольором).

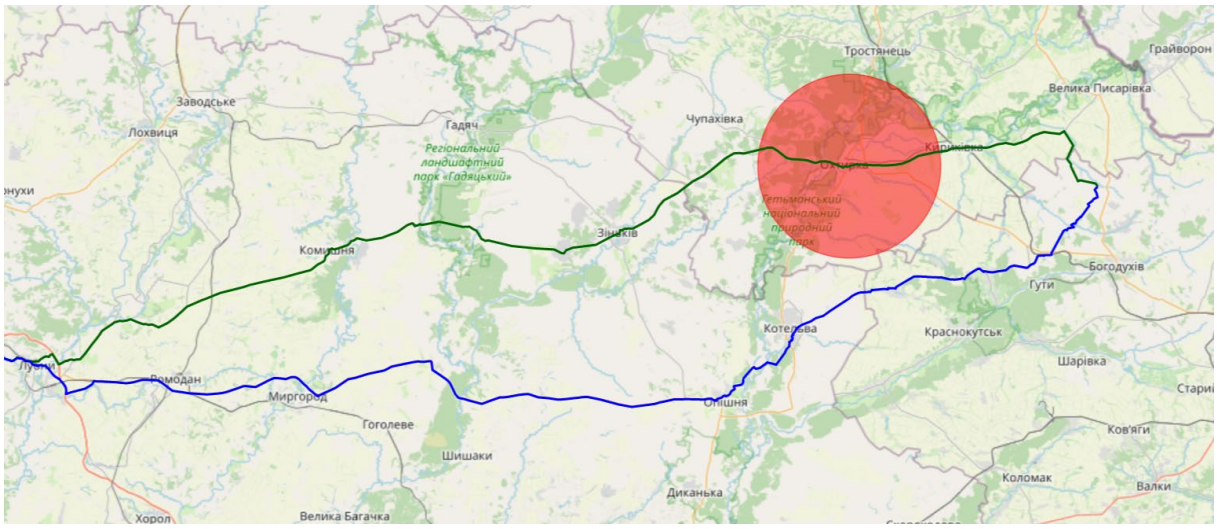


Рисунок 1. Порівняння роботи алгоритмів А* та адаптивного алгоритму А* з врахуванням "гарячих зон"

Був проведений порівняльний аналіз роботи запропонованих двох алгоритмів (класичного алгоритму А* та його адаптацію, яка враховує "гарячі зони"). Результати порівняння представлені в табл. 1.

Таблиця 1

Порівняння алгоритмів А* та адаптивного алгоритму А* з урахуванням "гарячих зон"

Характеристика	**Алгоритм А***	**Адаптивний алгоритм А* з урахуванням "гарячих зон"**
Функція вартості	$f(n)=g(n)+h(n)$	$f(n) = g(n) + h(n) + \alpha(n)$
Метод евристики	Евклідова або Манхеттенська відстань	Евклідова або Манхеттенська відстань
Врахування "гарячих зон"	Не враховує	Враховує
Складність	$O(b^d)$	$O(b'^d)$, де $b' > b$ через додаткові обмеження
Планування в умовах змінної обстановки	Не враховує зміни	Враховує зміни у вигляді додаткової вартості для небезпечних зон
Придатність для реальних карт	Висока	Вища через можливість об’їзду небезпечних ділянок
Обчислювальна вартість	Низька	Трохи вища через додаткові обчислення для "гарячих зон"
Точність маршруту	Висока	Вища через уникнення небезпечних зон

Порівняння адаптивного алгоритму А* з урахуванням "гарячих зон" та класичного алгоритму А* демонструє важливі відмінності в підходах до оптимізації маршрутів у динамічних умовах. Адаптивний алгоритм А*, завдяки функції вартості, доповненій параметром $\alpha(n)$, враховує додаткові обмеження у вигляді ризикових зон, що дає йому перевагу в адаптації до змінної обстановки. У той час як класичний алгоритм А* з базовою функцією вартості $f(n)=g(n)+h(n)$ залишається ефективним для статичних середовищ, його

недолік проявляється у неврахуванні небезпечних зон, що може знижувати точність у складних ситуаціях. Адаптивний алгоритм A* зазвичай має трохи вищу обчислювальну вартість через додаткові розрахунки для "гарячих зон", що, в свою чергу, збільшує складність. Однак така підвищена обчислювальна вартість компенсується більш точною маршрутизацією та можливістю об’їзду ризикових ділянок, що робить адаптивний алгоритм A* кращим вибором для використання на реальних картах з динамічними умовами.

Висновки

Таким чином, в рамках даного дослідження було проведено аналіз проблем, пов’язаних із вирішенням задачі маршрутизації в динамічному середовищі, що допомогло визначити основні виклики для безпечного та ефективного планування маршруту. Було проведене дослідження в цій сфері, проаналізовано роботу класичного алгоритму A* і його вдосконалений адаптивний варіант, який враховує "гарячі зони". Порівняння алгоритмів показало, що адаптивний алгоритм A* забезпечує більшу точність і надійність маршруту завдяки здатності реагувати на динамічні зміни в середовищі, що відкриває нові можливості для його застосування в умовах реальних бойових дій, де важлива оперативність і безпека руху. Запропонований адаптивний алгоритм A* може бути використаний в транспортних системах, де необхідно уникати небажаних ділянок "гарячих зон", або знайти оптимальні альтернативні маршрути. Додатково, адаптивний алгоритм A* здатен працювати з даними в реальному часі, що дозволяє реагувати на зміни в обстановці, оперативно перераховуючи маршрут, відповідно до актуальної інформації. Така адаптивність відкриває нові можливості для застосування алгоритму не лише у цивільних, але й у військових середовищах, де критично важливо забезпечувати швидкість і безпеку руху в складних та небезпечних умовах.

Подальшими можливими науковими дослідженнями автори розглядають підвищення швидкодії роботи запропонованого алгоритму.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. OpenStreetMap // [Електронний ресурс]. 29.10.2024. URL: https://uk.wikipedia.org/wiki/OpenStreetMap.

2. Ваврук Є. Я., Мозіль З. Г. Вибір алгоритму пошуку оптимального шляху передавання даних у розподіленій системі. 2018 URL: https://science.lpnu.ua/sites/default/files/journal-paper/2019/sep/18542/182073vis905ksmzvichniy-42-48.pdf.

3. Бульба С. С., Соловйова О. І., Семеренко Ю. О. Дослідження алгоритмів пошуку оптимального шляху 19.04.2024. URL: https://doi.org/10.26906/SUNZ.2024.2.067.

4. Hybrid A* path search with resource constraints and dynamic obstacles. Secyrity Intelligent Aerospace Systems / Alán Cortez and oth. 25 January 2023. Vol. 1. URL: https://doi.org/10.3389/fpace.2022.1076271.

5. Бартіш М. Я., Дудзяний І. М. Дослідження операцій. Частина 2. Алгоритми оптимізації на графах: Підручник. Львів: Видавничий центр ЛНУ ім. Івана Франка, 2007. 120 с.

6. Comparison of optimal path finding techniques for minimal diagnosis in mapping repair. International Conference on Data and Software Engineering (ICoDSE) / Inne Gartina Husein*, Saiful Akbar, Benhard Sitohang, Fazat Nur Azizah. 2017. URL: http://dx.doi.org/10.1109/ICODSE.2017.8285853.

7. Analysis of Dijkstra’s Algorithm and A* Algorithm in Shortest Path Problem. Journal of Physics: Conference Series / Dian Rachmawati1 and Lysander Gustin. 2019. URL: https://doi.org/10.1088/1742-6596/1566/1/012061.

8. Трохимчук Р. М. Теорія графів. Навчальний посібник для студентів факультету кібернетики / Р. М. Трохимчук. К.: РВЦ «Київський університет», 1998. 43 с.

9. Шевцов М. В., Ніколюк П. К. Порівняння різних евристичних функцій в алгоритмі A* 18.07.2023. URL: https://jait.donnu.edu.ua/article/view/14012.

10. Change Detection from Remote Sensing to Guide OpenStreetMap Labeling / Conrad M. Albrecht and oth. 2020. Journal: ISPRS Int. J. Geo-Inf. Vol. 9. Num. 427. URL: https://doi.org/10.3390/ijgi9070427.

DOI: 10.58254/viti.6.2024.05.75

УДК 004.932.2

канд. техн. наук, доцент Грінько В. О. ORCID: 0000-0002-9574-3792 (ВІТІ ім. Героїв Крут)
Грінькова Г. В. ORCID: 0009-0003-4896-364X (НДІ ВР)
Грінько С. В ORCID: 0009-0009-7350-1360 (ДУ «Відкриті публічні фінанси»)

МЕТОДИКА ОЦІНКИ ТОЧНОСТІ РОЗПІЗНАВАННЯ СИМВОЛІВ І ТЕКСТУ З ЗОБРАЖЕННЯ ДЛЯ АНАЛІЗУ ЯКОСТІ СУЧАСНИХ ІНСТРУМЕНТІВ OCR

Оптичне розпізнавання символів – це потужна технологія, яка перетворює зображення з текстом у редагований і пошуковий формат. Це забезпечує ефективність у роботі з документами, підвищує доступність інформації і сприяє автоматизації багатьох процесів.

Вперше цю технологію почали використовувати на початку 90-х, при оцифруванні історичних газет для створення електронного архіву. За останні роки систему оптичного розпізнавання символів вдалося доопрацювати до «ідеалу»: нинішні системи оптичного розпізнавання символів показують майже ідеальну точність розпізнавання тексту. Але для цього потрібно виконання наступних вимог:

рівність і контрастність символів;

однотипність фону тексту;

контраст між фоном та літерами.

Набагато складніше процес розпізнавання символів і тексту з зображень, коли не виконуються вищеперелічені вимоги, а саме вирішення таких задач є вимогами сьогодення для вирішення практичних завдань у військовій сфері. Розпізнавання тексту з зображень має багато важливих застосувань, що робить його актуальним і необхідним.

В статті, з використанням конкретних типів зображень, проаналізовано декілька найбільш відомих та популярних моделей штучного інтелекту для розпізнавання тексту з зображення, такі як Tesseract OCR, PyTorch, EasyOCR, Keras OCR5, OpenCV, отримані результати розпізнавання тексту і символів з зображень різної складності.

Для оціки результатів точності розпізнавання символів і тексту, розроблена методика оцінки точності розпізнавання на базі спеціальних метрик оцінки, яка основана на порівнянні розпізнаного тексту із еталонним (правильним) текстом. Найбільш поширені метрики включають точність розпізнавання символів (Character Accuracy Rate, CAR) та точність розпізнавання слів (Word Accuracy Rate, WAR).

За допомогою розробленої методики оцінки точності розпізнавання проведено аналіз точності розпізнавання найбільш популярних інструментів технології оптичного розпізнавання тексту і символів з зображень різної складності. Проведений аналіз показав, що найбільшу ефективність і точність розпізнавання демонструє модель EasyOcr, яка навіть в умовах сильної «зашумленості» і неякісної контрастності зображення демонструвала стабільний результат і при умовах подальшого налаштування для потреб користувача, може бути застосована для рішення конкретного завдання.

Ключові слова: *методика оцінки, метрики оцінки, розпізнавання тексту, технології OCR, моделі OCR, точність розпізнавання, аналіз зображень, машинне навчання.*

V. Hrinkov, G. Hrinkova, S. Hrinkov. Analysis of modern optical character recognition tools for character recognition and text from the image

Optical character recognithen is a powerful technology that converts images with text into an editable and searchable format. This ensures efficiency in working with documents, increases the availability of information and contributes to the automation of many processes.

This technology was first used in the early 1990s, when digitizing historical newspapers to create an electronic archive. In recent years, the optical character recognition system has been refined to the "ideal": current optical character recognition systems show almost perfect text recognition accuracy. But for this, the following requirements must be met:

equality and contrast of symbols;

homogeneity of the background of the text;

contrast between background and letters.

The process of recognizing symbols and text from images is much more complicated when the above requirements are not met, and the solution of such problems is the current requirement for solving practical tasks in the military sphere. Text recognition from images has many important applications, which makes it relevant and necessary.

The article, using specific types of images, analyzed several of the most famous and popular models of artificial intelligence for recognizing text from an image, such as Tesseract OCR, PyTorch, EasyOCR, Keras OCR5, OpenCV, and obtained the results of recognizing text and symbols from images of various complexity.

To evaluate the results of character and text recognition accuracy, a recognition accuracy evaluation method has been developed based on special evaluation metrics, which is based on comparing the recognized text with the reference (correct) text. The most common metrics include Character Accuracy Rate (CAR) and Word Accuracy Rate (WAR).

With the help of the developed method of recognition accuracy assessment, an analysis of the recognition accuracy of the most popular tools of the technology of optical recognition of text and symbols from images of different complexity was carried out. The conducted analysis showed that the EasyOcr model demonstrates the highest efficiency and accuracy of recognition, which even in conditions of strong "noise" and low-quality contrast of the image showed a stable result, and under the conditions of further adjustment for the needs of the user, it can be applied to solve a specific task.

Keywords: *evaluation method, evaluation metrics, text recognition, OCR technologies, OCR models, recognition accuracy, image analysis, machine learning.*

Актуальність та постановка завдання в загальному вигляді. Зі збільшенням обсягу цифрових та друкованих даних все більш актуальним стає використання технологій автоматичного розпізнавання тексту. Інструменти *OCR (Optical Character Recognition)* дозволяють перетворювати відскановані документи, фотографії та інші зображення, що містять текст, у редагованому цифровому форматі. Це сприяє підвищенню ефективності обробки інформації в різних сферах. У військовій сфері інформація є ключовим ресурсом для забезпечення оперативного управління та ухвалення тактичних і стратегічних рішень. В умовах бойових дій та військових операцій необхідно швидко обробляти великі обсяги даних із різних джерел. Технології *OCR*, які дозволяють автоматично розпізнавати текст із зображення, залишаються надзвичайно актуальними і необхідними в різних напрямках діяльності Збройних сил України:

1. Розвідка та аналіз даних. *OCR*-технології можуть бути застосовані для автоматичного розпізнавання та аналізу текстової інформації з розвідувальних зображень, таких як фотографії з дронів, супутників та інших розвідувальних платформ. Це допомагає витягувати корисні дані із захоплених у противника документів, написів на транспортних засобах та об’єктах.
2. Підтримка в бойових операціях. Розпізнавання тексту із зображень може використовуватися для оновлення карт і навігаційних систем у реальному часі, що є критично важливим для планування операцій і переміщення військ, виявлення та аналіз написів на зображеннях може допомогти в ідентифікації прихованих загроз, таких як міни або вибухові пристрої, позначені попереджувальними знаками.
3. Автоматизація документації та логістики. *OCR*-технології можуть застосовуватись для автоматизації обробки різних документів та логістичних даних у військовій сфері. Це включає розпізнавання та обробку рахунків, накладних, контрактів та іншої документації, що прискорює процеси та знижує ризик помилок.
4. Кібербезпека. *OCR*-технології можуть застосовуватись для аналізу текстів та кодів у рамках забезпечення кібербезпеки. Це включає розпізнавання шкідливих текстів, сканування документів на наявність прихованих загроз та аналіз логів систем.
5. Забезпечення безпеки та контролю доступу. *OCR*-технології можуть використовуватися для автоматичного розпізнавання текстів на перепустках, посвідченнях особи та інших документах, що сприяє посиленню контролю доступу та забезпечення безпеки на військових об’єктах.
6. Технічна документація та навчання. *OCR*-технології можуть використовуватися для оцифрування та обробки технічної документації, інструкцій та навчальних матеріалів, що сприяє більш ефективному навчанню та підвищенню кваліфікації військовослужбовців.
7. Розпізнавання текстів на транспортних засобах та устаткуванні. *OCR*-технології можуть застосовуватись для розпізнавання текстів, серійних номерів та міток на військовій техніці, обладнанні та транспортних засобах, що допомагає в ідентифікації та відстеження активів.

8. Переклад та локалізація. *OCR*-технології у поєднанні із системами машинного перекладу може допомогти у перекладі текстів різними мовами, що важливо для взаємодії з міжнародними партнерами та коаліційними силами.

9. Зв'язок та координація. Автоматичне вилучення інформації з польових звітів дозволить командирам отримувати актуальну інформацію та приймати рішення в режимі реального часу, розпізнавання тексту може бути інтегроване з іншими системами управління і контролю, що покращує загальну координацію дій.

Таким чином, розпізнавання тексту із зображень є важливим інструментом для підвищення ефективності, точності та швидкості виконання військових завдань. Технологічні досягнення в цій області можуть суттєво підвищити бойову здатність та інформаційну перевагу Збройних сил України.

Зважаючи на вищезазначене, методика оцінки точності розпізнавання, на базі якої здійснюється пошук найбільш ефективного інструменту розпізнавання тексту і символів із зображень є актуальним завданням.

Аналіз попередніх досліджень. Науковим дослідженням щодо використання інструментів *OCR* для розпізнавання символів і тексту присвячено значну кількість робіт [1–12], аналіз деяких з них викладено нижче.

Дослідження [1] присвячено аналізу та дослідженню сучасних підходів до обробки зображення та розпізнавання текстової інформації у технології *OCR*. У ході дослідження виявлено та проаналізовано найбільш популярні методи класифікації (шаблонний, структурний, ознаковий, статистичний, із застосуванням штучних нейронних мереж) та зроблено висновки стосовно ефективних напрямів їх застосування.

В роботі [2] описуються способи використання інструментів *OCR* для перетворення будь-яких надрукованих або відсканованих текстових зображень в цифровий формат.

В роботі [3] наводиться історичний екскурс розвитку технологій *OCR,* поточний стан використання технологій *OCR* для розпізнавання символів і перспективи його розвитку і застосування.

Робота [4] розглядає сучасні підходи до OCR, включаючи методи глибинного навчання. Вона також містить огляд різних інструментів і програм OCR, ілюстрованих прикладами для кращого розуміння технології.

Робота [5] досліджує новітні досягнення у розпізнаванні тексту на основі глибокого навчання. Автори описують моделі для розпізнавання та розпізнавання тексту в складних сценах, таких як вуличні фотографії та відео.

Робота [6] досліджує використання згорткових нейронних мереж (CNN) для розпізнавання тексту в зображеннях із природних сцен (вивіски, вуличні таблички тощо). В роботі представляється наскрізна система для виявлення тексту, локалізації та розпізнавання тексту в природному вигляді і пошук текстових зображень. Система побудована на визнанні і ранжуванні пропозиції, тренуванні великої згортки нейронної мережі для розпізнавання слів у цілому фрагменті зображення одночасно, завдяки систем, заснованих на класифікаторі символів минулого.

З розвитком нейронних мереж і машинного навчання сучасні OCR-системи досягли значних успіхів у точності розпізнавання тексту, однак проблеми зчитування тексту на низькоякісних зображеннях, різноманітність мов, шрифтів та складні макети документів все ще залишаться актуальними. Аналіз наявних інструментів OCR дозволяє розуміти їхні можливості, обмеження та перспективи подальшого вдосконалення.

Метою статті є розробка методики оцінки точності розпізнавання символів і тексту моделями та проведення аналізу і порівняння сучасних інструментів OCR розпізнавання символів і тексту із зображенням різної складності.

Для досягнення цієї мети необхідно провести:

1. Огляд існуючих алгоритмів та технологій, що використовуються в сучасних *OCR*-системах.
2. Вибір найпопулярніших моделей *OCR* для аналізу.
3. Вибір опцій зображень.
4. Розробка методики оцінки точності розпізнавання символів та тексту.
5. Оцінка точності інструментів при розпізнаванні текстів на зображеннях різної якості.
6. Виявлення переваг та обмеження OCR-системи для роботи з різними типами зображень.
7. Розробка рекомендацій щодо вибору та використання OCR-інструментів залежно від вирішення конкретної задачі.

Результати аналізу користувальницьких програм застосовуються з вибором найбільш відповідного інструменту OCR для конкретних потреб та завдань, а також сприяють розвитку нових підходів до вдосконалення системного розпізнавання.

Виклад основного матеріалу. Існує багато моделей і бібліотек, котрі можна використовувати для розпізнавання тексту і символів з зображення. У цій статті буде використовуватись мова програмування Python, як більш популярна мова для штучного інтелекту та машинного навчання та більш лаконічна. Приведемо декілька найбільш відомих і популярних моделей.

1. *TesseractOCR1*. Інструмент оптичного розпізнавання символів, розроблений Google, який підтримує більше 100 мов. Він може працювати з різноманітними форматами зображень та обробляти складні тексти. Для використання *Tesseract OCR* на *Python*, необхідно встановити бібліотеку *pytesseract2*, котра надає простий інтерфейс для роботи з *Tesseract OCR*. Офіційний ресурс моделі *Tesseract OCR: GitHub - tesseract-ocr/tesseract: Tesseract Open Source OCR Engine (main repository).*
2. *EasyOCR3.* Бібліотека, котра використовує нейронні мережі лля розпізнавання тексту з зображення. Вона підтримує більше 80 мов, включаючи кирилицю, може розпізнавати текст у різних орієнтаціях та умовах освітлення. EasyOCR також дозволяє налаштовувати параметри розпізнавання, такі як розмір тексту, колір фону та контраст. Офіційний ресурс моделі EasyOCR: [GitHub - JaidedAI/EasyOCR: Ready-to-use OCR with 80+ supported languages and all popular writing scripts including Latin, Chinese, Arabic, Devanagari, Cyrillic and etc][7]**.**
3. *PyTorch OCR4*. Бібліотека, яка реалізує кілька сучасних моделей для розпізнавання тексту із зображення, таких як *CRNN, STAR-Net, RobustScanner* і *NRTR*. Вона заснована на фреймворці *PyTorch* та підтримує *GPU* –прискорення. *PyTorch OCR* також надає вже обучені моделі для різних мов та сценаріїв, таких як документи, таблиці та рукописний текст. Офіційний ресурс моделі *PyTorch OCR*: [*GitHub - DYJNG/PyTorchOCR: OCR Toolkits based on PyTorch*] [8].
4. *Keras OCR5*. Бібліотека, яка реалізує двоетапний підхід для розпізнання тексту із зображення. Спочатку вона використовує модель *CRAFT* для виявлення областей тексту на зображенні, а потім використовує модель *CRNN* для розпізнавання символів у кожній області. Вона заснована на фреймворці *Keras* та підтримує *GPU*-прискорення. *Keras OCR* також надає вже навчені моделі для англійської та французької мов. Офіційний ресурс моделі *Keras OCR*: [*GitHub - faustomorales/keras-ocr: A packaged and flexible version of the CRAFT text detector and Keras CRNN recognition model*] [9].
5. *OpenCV* – це бібліотека, яка надає велику кількість функцій для роботи із зображеннями та відео, включаючи розпізнавання тексту. Вона підтримує різні алгоритми для

виявлення та вилучення тексту із зображення, такі як MSER, SWT та EAST. Вона також дозволяє використовувати різні двигуни для розпізнання символів, такі як *Tesseract OCR, LSTM* та *CNN*. Офіційний ресурс моделі *OpenCV*: [*OpenCV - Open Computer Vision Library*] [10].

EasyOCR. Встановлюємо модель через *pip install pip install easyocr.* Модель дуже зручна, оскільки має підтримку багатьох мов та автоматично завантажує їх при додаванні абревіатури цих мов, також є можливість одночасно використовувати кілька мов для розпізнавання. Модель постійно оновлюється та покращується.

*Tesseract OCR***.** Встановлюємо її через *pip install pip install pytessereact***.** Для цієї моделі в стартовому наборі існує лише модель для розпізнавання англійської мови, якщо використовується інша мова, необхідно завантажити язикові дані додатково з репозиторію, що є доволі незручним.

PyTorch. Для розпізнавання тексту на зображенні з використанням *PyTorch* використовується *Tesseract* (для розпізнавання тексту) та *PyTorch* для розпізнавання областей зображення з текстом. Встановлюємо ці бібліотеки за допомогою pip install: *pip install pytesseract Pillow torchvision.*

Keras OCR5. Встановлюємо цю бібліотеку за допомогою pip install: *pip install keras-ocr OpenCV.* Встановлюємо цю бібліотеку за допомогою *pip install: pip install pytesseract pip install opencv-python*

Протестуємо вказані моделі на трьох зображеннях різного рівня складності. Для першого зображення з розміром 73 кБ (рис. 1), результати розпізнавання тексту (символів) приведені в таблиці 1.

Рис. 1. Зображення 73 кБ

Таблиця 1

Результати розпізнавання тексту і символів із зображення на рис. 1

EasyOCR	*Tesseract OCR*	*PyTorch*	*Keras OCR5*	*OpenCV*
['ENLII', '[Ч@ПИ', '[EISTRT', 'Б1ош', '89', 'Шрота', 'Допота', 'Скавость', 'Цепь Нет даннымо GPS', 'NSmsLId', 'БПА', '[Нет даШньМЕт GP S', '178', 'Крс']	ВОЛр ор Розраои е ВАг Бтом] @.° ЦИ Ц рота олгота @ Скорость | Ё._ МА еп Негданных т оРУ он _В щ аЁЁЗ›ЁЁЁ.ЁЁН"ЁЬЦ оате оАИЫ Болефк сооащесщес оО в Рар о СОя оь о сооЙ *- ощ сиее аНЕО кО,, оо овосорееоиоНоНН Н УН —° СОИ ТР о ссныньнь чеыЕ Н @т ОЫЕ о КОЧЕ стр ЯОМ ИО р палек оаЫ ооа нааВЬсессв › —чача оо Ь ЬАМ о, с ПИЗВаЕ На ы й ' : ,Ъ:,,_\.\\ ‹ ^ ста РОИ оо аЕН, МЕОар оР Воаео ол ОАар НЕЙ ЛВ ВЕИ ОАА ; *@ ЙОЕ МОНЕа КОЙ ЗЕВ ОН ов с ГА^ оааа н г""г,»"щ Ь"'?@Ё"" В РОИ #'г›і.ъ;?;…\;*_„:т ВМ ,'ч#,›ё.… ж ОкБ` АААНЫ "___- !.:,'__,;@;,:__;_;';,,:э_' Пр аееа –	Для першого зображення модель не розпізнала нічого	['alt', 'es', 'baadi', 'ins', 'start', 'stons', 'for', 'bt', '9', 'gind', '89', 'donteta', 'lmpeta', 'ckopoct', 'kepc', 'het', 'grs', 'nsnotreh', 'lenb', 'sahtae', 'et', 'si', 'het', 'gps', 'ot', 'aahnae', 't8']	Для першого зображення модель не розпізнала нічого

Для другого зображення з розміром 217 кБ (рис. 2) моделі видали наступні результати (таблиця 2):

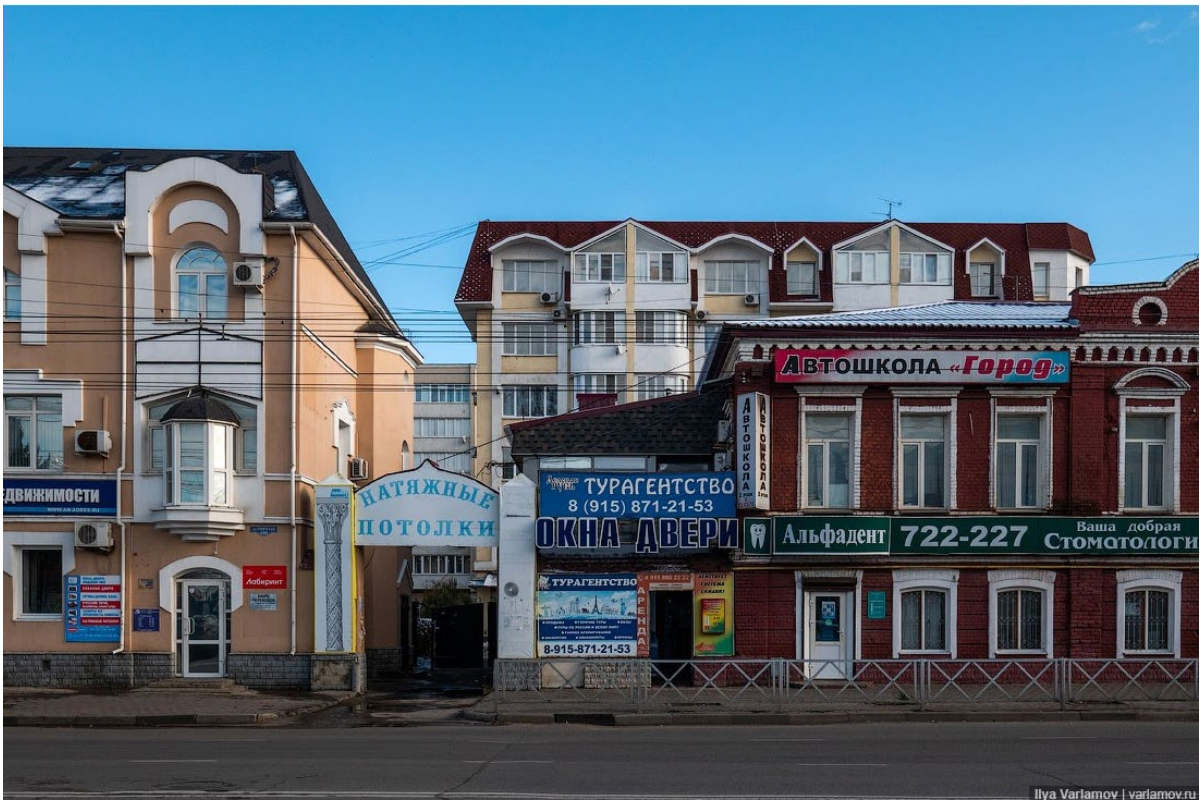


Рис. 2. Зображення 217 кБ

Таблиця 2

Результати розпізнавання тексту (символів) з зображення рис. 2

EasyOCR	*Tesseract OCR*	*PyTorch*	*Keras OCR5*	*OpenCV*
['ДВТошКолА #ро9', 'ДВИЖИМОНИ', 'ХАтяжныд', 'Дан" ТУРАГЕНТСТВО', """, '8 (915) 871-21-53', '[потолки', 'ШШШШ [ВЕРП', 'Альфадент 722-227', 'Стоашатообоги', 'добрая', '~ЛбНЕяиг', 'ТУИГЕНТЕГНО', '1', '8-915-871-21-53', 'Луа Уаашон', '~агашокш', '[']	ста + ‘ во, „Заенащабораеоы в о К СО '@‘Ёі@ Й —° И е шо \ В, - Рі,:."""м;'—\ — Е == Ы ВВ, % ЕА ВТОШКОЛА «Город» - % -5ваа 2° ва р 60 вяниности_| , й Г каа е оее 8 Ы НЕ М _i_' роой) ПБ ТО АН т2227 стообла _ а_'г' Н ЕЕЕ Ё і			с ЗртНе в) — аМСа О == — уа Уапатом \манатоулы	ime ТУРАТЕАТСТВО (1h 8 aie nee 21-53 =3 yOE SX KIS XS ages _ tlya Varlamov | varlamov.ru-	['c', 'abtolwkola', 'ropog', 'i', '', 'iyer', 'typarehtctbo', 'hatakhble', 'abiammocth', '8', '9151', '8712153', 'notojika', 'okha', 'abeph', 'goopaa', 'bawa', 'ajibpaieht', '722227', 'ctomatoiorh', 'tooupat', 'typarehtctbo', 'p', 'e', 'a', '89158112153', 'lya', 'varlamoy', 'varamoviu']	‘wa ТУРАТЕНТСТВО | . 8 (915) 8671-24-53 і UGK (IRIE 2-227 cxbsiensteen OO o _—— nn + Mya Variamov | variamov.ne:

Тут вже більше моделей видали прийнятний результат, хоча текст був не накладений на зображення, тому його виділення було ускладнено.

Для третього зображення з розміром 122 кБ (рис. 3), моделі видали наступні результати (таблиця 3):

	A	B	C	D	E	F
1	Name	Type 1	Type 2	HP	Attack	Defense
2	Abra	Psychic		25	20	15
3	Kadabra	Psychic		40	35	30
4	Alakazam	Psychic		55	50	45
5	Machop	Fighting		70	80	50
6	Machoke	Fighting		80	100	70
7	Machamp	Fighting		90	130	80
8	Bellsprout	Grass	Poison	50	75	35
9	Weepinbell	Grass	Poison	65	90	50
10	Victreebel	Grass	Poison	80	105	65
11	Tentacool	Water	Poison	40	40	35
12	Tentacruel	Water	Poison	80	70	65

Рис. 3. Зображення 122 кБ

Таблиця 3

Результати розпізнавання тексту (символів) з зображення рис. 3

EasyOCR	*Tesseract OCR*	*PyTorch*	*Keras OCR5*	*OpenCV*
[['B', 'D', 'E', '1', 'Name', 'Type 1', 'Type 20', 'HP', 'Attack', 'Defense_', '2', 'Abra', 'Psychic', '25', '20', '15', '3', 'Kadabra', 'Psychic', '40', '35', '30', '4', 'Alakazam', 'Psychic', '55', '50', '45', '5', 'Machop', 'Fighting', '70', '80', '50', '6', 'Machoke', 'Fighting', '80', '100', '70', 'Machamp', 'Fighting', '90', 130', '80', '8', 'Bellsprout', 'Grass', 'Poison', '50', '75', '35', '9', 'Weepinbell', 'Grass', 'Poison', '65', '90', '50', '10', 'Victreebel', 'Grass', 'Poison', '80', '105', '65', '11', 'Tentacool', 'Water', 'Poison', '40', '40', '35', '12', 'Tentacruel', 'Water', 'Poison', '80', '70', '65']	A B ¢C D E F G imName Ed Type1Bd Type 2R7HP (Attack BJ Defense 2 Abra Psychic 25 20 15 3 Kadabra Psychic 40 35 30 4 Alakazam Psychic 55 50 45 5 Machop Fighting 70 80 50 6 Machoke _ Fighting 80 100 70 7 Machamp _ Fighting 90 130 80 8 Bellsprout Grass Poison 50 75 35 9 |Weepinbell Grass Poison 65 90 50 10 Victreebel Grass Poison 80 105 65 11 Tentacool Water Poison 40 40 35 12 Tentacruel Water Poison 80 70 65	A B ¢C D E F Name PJ Type1Bd Type 2B4HP [fq Attack BJ Defense Abra Psychic 25 20 15 Kadabra Psychic 40 35 30 Alakazam __ Psychic 55 50 45 Machop Fighting 70 80 50 Machoke __ Fighting 80 100 70 Machamp _ Fighting 90 130 80 Bellsprout Grass Poison 50 75 35 Weepinbell Grass Poison 65 90 50 Victreebel Grass Poison 80 105 65 Tentacool Water Poison 40 40 35 Tentacruel Water Poison 80 70 65	['c', 'a', 'e', 'f', 'g', 'b', 'd', 'defense', 'type', 'type', 'hp', 'attack', 'name', '1', '2', '1', 'psychic', 'abra', '20', '25', '15', '2', 'kadabra', 'psychic', '40', '35', '30', '3', 'alakazam' , 'psychic', '55', '50', '45', '4', 'machop', 'fighting', '70', '80', '50', '5', 'machoke', 'fighting', '80', '100', '70', '6', 'machamp', 'fighting', '90', '130', '80', '7', 'bellsprout', 'grass', 'poison', '50', '75', '35', '8', 'weepinbell', '90', 'grass', 'po', 'ison', '65', '50', '9', 'victreebel', 'grass', '80', '105', 'po', 'ison', '65', '10', 'tentacool', 'water', 'poison', '40', '40', '35', '11', 'tentacruel', 'water', 'po', '80', '70', '65', '12', 'ison']	wo wWOnN DU BWN BPP RP WNrR OO A Name B Cc a Type 18a Type 2a HP ba Attack a Defenselig Abra Kadabra Alakazam Machop Machoke Machamp Bellsprout Weepinbell Victreebel Tentacool Tentacruel Psychic Psychic Fighting Fighting Fighting Grass Grass Grass Water Water Poison Poison Poison Poison Poison 25 40 55 70 80 90 50 65 80 40 80 20 35 50 80 100 130 75 90 105 40 70 15 30 45 50 70 80 35

Визначення точності розпізнавання тексту чи символів із зображення здійснюємо за допомогою загальновизнаних метрик оцінки, які порівнюють розпізнаний текст із еталонним (правильним) текстом. Найбільш поширені метрики (оцінки точності) включають точність розпізнавання символів (*Character Accuracy Rate, CAR*) та точність розпізнавання слів (*Word Accuracy Rate, WAR*) і описуються формулами (1), (2) [11]:

$$CAR = (1 - \frac{S + D + I}{N}) \times 100\%, \quad (1)$$

де S – кількість замінених символів;

D – кількість віддалених символів;

I – кількість вставлених символів;

N – загальна кількість символів у еталонному тексті.

$$WAR = (1 - \frac{S_W + D_W + I_W}{N_W}) \times 100\%, \quad (2)$$

де S_W – кількість замінених слів;

D_W – кількість віддалених слів;

I_W – кількість вставлених слів;

N_W – загальна кількість слів у еталонному тексті.

Сутність методики оцінки точності розпізнавання символів полягає у порівнянні еталонного зображення з результатами розпізнавання і складається у виконанні наступних кроків (для пояснення будемо використовувати таблицю 4).

Таблиця 4

Пояснення алгоритму методики

Еталонний фрагмент	Результат розпізнавання
	A B ¢C D E F Nime PJ Typa 1Bd Type 2B4HP [fq Attack BJ Defense

Крок 1. Визначаємо загальну кількість символів у еталонному фрагменті. При розрахунку змінної пропуски не враховуються, знак ▫ дорівнює 2 символам $N = 45$.

Крок 2. Визначаємо загальну кількість символів у фрагменті розпізнавання $N^* = 47$.

Крок 3. Визначаємо значення змінних *I, D.* Для цього знаходимо різницю $\Delta = N^* - N$. Якщо $\Delta > 0$, то $I = \Delta$, $D = 0$. Якщо $\Delta < 0$, $I = 0$, $D = |\Delta|$. Якщо $\Delta = 0$, то $I = 0$, $D = 0$. Для нашого прикладу $I = 2$, $D = 0$.

Крок 4. Методом порівняння визначаємо значення змінної *S,* для нашого прикладу $S = 12$.

Крок 5. Значення змінних підставляємо в формулу 1, знаходимо точність розпізнавання символів. Для нашого прикладу $CAR = 69\%$. Якщо відношення $\frac{S + D + I}{N} > 1$, то $CAR = 0$.

Сутність методики оцінки точності розпізнавання слів також полягає у порівнянні еталонного зображення з результатами розпізнавання і складається у виконанні наступних кроків (для пояснення будемо використовувати таблицю 4). Під словом розумітимемо множину символів між пропусками.

Крок 1. Визначаємо загальну кількість слів у еталонному фрагменті $N_W = 16$.

Крок 2. Визначаємо загальну кількість слів у фрагменті розпізнавання $N_W^* = 16$.

Крок 3. Визначаємо значення змінних I_W , D_W. Для цього знаходимо різницю $\Delta_W = N_W^* - N_W$. Якщо $\Delta_W > 0$, то $I_W = \Delta_W$, $D_W = 0$. Якщо $\Delta_W < 0$, $I_W = 0$, $D_W = |\Delta_W|$. Якщо $\Delta_W = 0$, то $I_W = 0$, $D_W = 0$. Для нашого прикладу $I_W = 0$, $D_W = 0$.

Крок 4. Методом порівняння між еталонним і результуючим фрагментами визначаємо значення змінної S_W, для нашого прикладу $S_W = 8$.

Крок 5. Значення змінних підставляємо в формулу 2, знаходимо точність розпізнавання слів. Для нашого прикладу $WAR = 50\%$.

Якщо відношення $\frac{S_W + D_W + I_W}{N_W} > 1$, то $WAR = 0$.

Результати розпізнавання символів і тексту, які отримані за допомогою вищенаведених методик наведено в таблиці 5.

Таблиця 5

Точність розпізнавання символів і тексту із зображення для вибраних моделей OCR в умовах розпізнавання різної складності

Зображення	*EasyOCR, %*		*Tesseract OCR, %*		*PyTorch, %*		*Keras OCR5,%*		*OpenCV, %*	
	CAR	*WAR*	*CAR*	*WAR*	*CAR*	*WAR*	*CAR*	*WAR*	*CAR*	*WAR*
Рисунок 1	54	49	0	0	0	0	22	11	0	0
Рисунок 2	78	72	46	0	18	15	68	47	25	18
Рисунок 3	98	93	98	92	91	71	96	93	85	68

Для розглянутих прикладів краще всього себе показала модель *EasyOcr*. Також вона є найзручнішою та однією з найпопулярніших і частіше оновлених. При використанні налаштувань для зображень, відповідно до конкретних потреб, вона покаже ще кращі результати. На другому місті модель *Keras OCR5*. У моделі є труднощі з встановленням. У моделі всього дві мови доля розпізнавання – англійська та французька, тож у випадку інших мов краще вибрати іншу модель.

Висновки. В результаті аналізу деяких моделей технології *OCR* для розпізнавання тексту і символів із зображень різної складності, які проведені за допомогою розроблених методик, найбільшу ефективність і точність розпізнавання продемонструвала модель *EasyOcr,* яка навіть в умовах сильної «зашумленості» і неякісної контрастності зображення (рис. 1) показала непоганий результат і при умовах подальшого налаштування для потреб користувача, може бути застосована для рішення конкретного завдання.

Майбутні напрями досліджень. Таким чином, отримані результати є підґрунтям для подальших наукових досліджень, які полягають в автоматизації процесу підрахунку даних для оцінки точності розпізнавання і продовженню аналізу якості розпізнавання інших моделей OCR, вдосконаленні метрики для оцінки якості розпізнавання, включення нових метрик, таких як семантична точність, що оцінює збереження змісту документа, і структурна точність для складних документів (таблиці, діаграми, формули). Це дозволить глибше аналізувати точність розпізнавання різних типів контенту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Переяславська С., Шевченко В., Смагіна О. Аналіз підходів до розпізнавання текстової інформації у технології OCR. Scientific Collection «InterConf»: SCIENTIFIC RESEARCH IN XXI CENTURY (March 6–8, 2021).

2. Hamad K, Kaya M. A Detailed Analysis of Optical Character Recognition Technology URL: https://dergipark.org.tr/en/download/article-file/236939 (дата звернення: 25.04.2024).

3. Eikvil L. OCR Optical Character Recognition. URL: https://www.nr.no/~eikvil/OCR.pdf (дата звернення: 15.09.2024).

4. Optical Character Recognition: An Illustrated Guide to the Frontier. Georeg Nagy, Stephen V. Rise, Thomas A. Narker. Springer Science&Business Media. 2019 (дата звернення: 25.05.2024).

5. Scene Text Detection and Recognition: The Era of Deep Learning – Baoguan Shi, Xiang Bai, Kong Yao (2017). URL: https://www.researchgate.net/publication/328899907 (дата звернення: 20.10.2024).

6. Reading Text in the Wild with Convolutional Neural Networks. Jaderberg M., Simonyan K., Vedaidi A., Zisserman A. URL: https://www.robots.ox.ac.uk/~vgg/publications/2016/Jaderberg16/jaderberg 16.Pdf (дата звернення: 14.08.202424).

7. URL: https://github.com/JaidedAI/EasyOCR (дата звернення: 16.03.2024).

8. URL: https://github.com/DYJNG/PyTorchOCR (дата звернення: 09.04.2024).

9. URL: https://github.com/faustomorales/keras-ocr (дата звернення: 19.04.2024).

10. *U*RL: https://opencv.org/ (дата звернення: 18.04.2024).

11. ISO/IEC 19757-7:2009. "Information technology – Document Schema Definition Languages (DSDL) – Part 7: Character Repertoire Description Language (CREPDL)".

12. Jurafsky, D., & Martin, J. H. (2009). "Speech and Language Processing". Upper Saddle River, New Jersey 07458.

DOI: 10.58254/viti.6.2024.06.85

УДК.62-23

д-р техн. наук, професор Кузавков В. В. ORCID: 0000-0002-0655-9759 (ВІТІ ім. Героїв Крут)
канд. техн. наук Мацаєнко А. М. ORCID: 0000-0003-1149-7318 (ВІТІ ім. Героїв Крут)
Погребняк С. В. ORCID: 0000-0002-7902-9847 (ВІТІ ім. Героїв Крут)
Бербер І. О. ORCID: 0009-0004-5136-942X (ІСЗЗІ НТУУ "КПІ ім. Ігоря Сікорського")

МЕТОДОЛОГІЯ ВИЗНАЧЕННЯ ТЕХНІЧНОГО СТАНУ ІМПУЛЬСНОГО БЛОКА ЖИВЛЕННЯ В ДИНАМІЧНОМУ РЕЖИМІ

Оскільки блок живлення є складовою частиною будь-якого радіоелектронного пристрою, для забезпечення високої якості та надійності його функціонування необхідна періодична перевірка його експлуатаційних характеристик та застосованих в ньому конструктивних рішень.

Відсутність або несвоєчасність процедур перевірки ставить під загрозу функціонування усього пристрою і робить користувача вразливим перед ймовірним настанням раптових відмов та подальшими потенційно неприємними ситуаціями.

Слід враховувати, що елементна база (якість виготовлення) блоків живлення не відрізняється від якості елементної бази усього пристрою, при цьому цей блок є посередником між мережею електроживлення (параметрами, характеристиками та станом мережі живлення) і основним пристроєм (технічним станом та адекватністю користувача при його застосуванні).

Отже, від ефективності та коректності функціонування блока живлення, стабільності його параметрів залежить довговічність основного обладнання. На випадок критичного стану устаткування саме блок живлення містить в собі запобіжник (систему автоматичного аварійного вимикання), при цьому спрацьовування запобіжника не дозволяє визначити причину (джерело) критичного стану (мережа – блок живлення – основне устаткування – порушення правил експлуатації). Заміна запобіжника, або підміна блока живлення не гарантує кінцевого розв'язання задачі технічного діагностування. З огляду на постійно зростаючу складність та високу вартість сучасних радіоелектронних пристроїв (в тому числі і з елементами штучного інтелекту) критично важливим є питання своєчасного діагностування потенційних несправностей блоків живлення. Тому, розробка науково обґрунтованих підходів до визначення технічного стану саме блоків живлення та локалізації його несправностей є актуальною задачею.

Ключові слова: *імпульсний блок живлення, діагностика, життєвий цикл, тестова послідовність, електролітичний конденсатор, безконтактний індукційний метод.*

V. Kuzavkov, A. Matsayenko, S. Pohrebniak., I. Berber Methodology for determining the technical condition of the pulse power supply unit in dynamic mode

Since the power supply unit is an integral part of any electronic device, to ensure high quality and reliability of its operation, it is necessary to periodically check its operational characteristics and the structural solutions used in it.

The lack or untimely verification procedures jeopardizes the functioning of the entire device and leaves the user vulnerable to the likely onset of sudden failures and subsequent potentially unpleasant situations.

It should be borne in mind that the element base (workmanship) of the power supply units does not differ from the quality of the element base of the entire device, while this unit is an intermediary between the power supply network (parameters of the characteristics and state of the power supply network) and the main device (technical condition and adequacy of the user when using it).

Therefore, the durability of the main equipment depends on the efficiency and correctness of the functioning of the power supply, the stability of its parameters. In case of a critical state of the equipment, the power supply unit itself contains a fuse (automatic emergency shutdown system), while the operation of the fuse does not allow to determine the cause (source) of the critical state (network - power supply unit - main equipment - violation of operating rules). Replacing the fuse, or replacing the power supply does not guarantee the final solution to the problem of technical diagnostics. Given the ever-increasing complexity and high cost of modern electronic devices (including those with elements of artificial intelligence), the issue of timely diagnosis of potential power supply malfunctions is critically important. Therefore, the development of scientifically sound approaches to determining the technical condition of power supplies and localizing its faults is an urgent task.

Keywords: *pulsed power supply, diagnostics, life cycle, test sequence, electrolytic capacitor, non-contact induction method.*

Постановка задачі в загальному вигляді. Незалежно від конструктивного виконання блока живлення (зовнішній або вбудований) необхідно передбачити засоби перевірки його технічного стану. Це дозволить переконатися, що джерело живлення працює належним чином, а параметри вихідної напруги відповідають заявленим вимогам.

Вимоги для перевірки імпульсного блока живлення (ІБЖ) складаються, виходячи з параметрів пристрою і умов його застосування. На підставі цих вимог складається загальна стратегія тестування і тест-план. У такому тестовому плані повинні бути відображені всі допустимі експлуатаційні межі, температурні умови експлуатації, параметри вхідної та вихідної напруги, які вважаються нормальними і пристрій повинен працювати без збоїв і що всі необхідні запаси відповідають вимогам**.**

Аналіз публікацій за темою дослідження. Сучасна радіоелектронна апаратура характеризуються багатофункціональністю і складністю, яка обумовлена обсягом і характером розв'язуваних ними завдань. Дане обладнання містить у своєму складі один із найважливіших елементів – вторинні джерела живлення.

Аналіз розвитку радіоелектронного обладнання (РЕО) показує, що поліпшення тактико-технічних та експлуатаційних характеристик супроводжується схемним та конструктивним ускладненням основного обладнання з одночасним зниженням його надійності [1, 2].

Поліпшення ремонтопридатності та підвищення ефективності діагностичного забезпечення (під яким слід розуміти комплекс взаємозалежних правил, методів, алгоритмів та засобів, необхідних для здійснення діагностування РЕО на всіх етапах життєвого циклу) дозволяє досягти необхідних показників надійності [3, 4].

Метою статті є висвітлення складових розробленої методології визначення технічного стану елементів ІБЖ, в основу якої покладено безконтактний індукційний метод контролю технічного стану (ТС) радіоелектронних об'єктів (одним з яких є імпульсні вторинні джерела живлення (ІБЖ)). Складовими методології також виступають: алгоритм реалізації метода, алгоритм функціонування діагностичного пристрою, варіант практичної реалізації апаратної та програмної складової пристрою діагностування (контролю).

Актуальність завдань технічного діагностування ІБЖ може підтверджуватись наступними чисельними показниками:

відсоток ІБЖ від функціонального складу основного устаткування в сучасному РЕО становить до 10 % [5, 6];

значний час діагностування (до 70% від загального часу контролю ТЗ);

допустиме значення економічних витрат 10–15 % вартості основного устаткування РЕО і фактична вартість відновлювальних робіт з урахуванням доставки комплектуючих імпортного виробництва до 50 % вартості життєвого циклу виробу [7].

Виклад основного матеріалу. Сутність запропонованого підходу (методології) контролю технічного стану вторинних джерел живлення полягає у автоматичному (автоматизованому) аналізі діагностичного параметра, отриманого безконтактним методом. При чому, аналізу піддається реакція ІБЖ як САУ зі зворотнім зв'язком на динамічну зміну навантаження у вихідних колах чотириполюсника.

Аналіз існуючих методів контролю технічного стану ІБЖ показує, що якість визначення технічного стану (ТС) цих виробів безпосередньо на об'єктах РЕО досить низька [8], внаслідок чого знижується коефіцієнт готовності РЕО. У процесі експлуатації ІБЖ функціонують за умов непередбачено динамічної зміни навантаження. При цьому контроль ТС здійснюється в статичному режимі, і позитивні результати контролю ТС в цьому випадку не гарантують працездатного стану ОК під час реальної роботи.

Безконтактний індукційний метод має високу чутливість і інформативність, оскільки умови для роботи складових елементів ІБЖ (САУ) у цьому випадку виявляються жорсткішими за звичайний режим функціонування (але в допустимих межах). У цьому випадку елементи,

які не піддаються контролю без вилучення зі схеми, спотворюють вид (параметри) перехідного процесу та змінюють його показники.

Динамічний контроль обраного об'єкта контролю можливо здійснювати у часовій та частотній області, а також із застосуванням статистичних методів обробки інформації. На практиці частотний метод контролю застосовується на етапі проєктування ІБЖ, а застосування статистичного методу в місцях експлуатації неможливе через відсутність репрезентативної статистичної вибірки подібних зразків.

Використання часового контролю передбачає реєстрацію та аналіз параметрів ОК у часі, у тому числі із застосуванням засобів відображення первинної інформації.

Для того, щоб отримати задану достовірність контролю (особливо у місцях експлуатації), необхідно чітко визначити ознаки, які характеризують справний та несправний стан; вибрати узагальнені параметри, що однозначно визначають ці ознаки; знайти співвідношення між точністю вимірювань контрольованих параметрів (КП) та допусками на ці КП. Вирішення цих завдань можливе лише при використанні автоматизованих вимірювальних систем.

Широко відома практика використання ступінчастої функції (теорія автоматичного керування), яка подається на вхід об'єкта контролю. Результатом впливу такої функції на об'єкт є перехідний процес, в якому відображається інформація про реакцію системи на весь спектр частот. Сам перехідний процес визначається показниками якості (ПК), основними з яких є: час перехідного процесу τ1 та τ2; помилка в режимі $\alpha = 0{,}05U_{вст}$; N – число коливань протягом перехідного процесу, $\Delta U_{ст.}$ – коефіцієнт перерегулювання (20%–30% $U_{вст.}$), $t_{вст.}$ – час встановлення, T_o – період коливань (рис. 1).

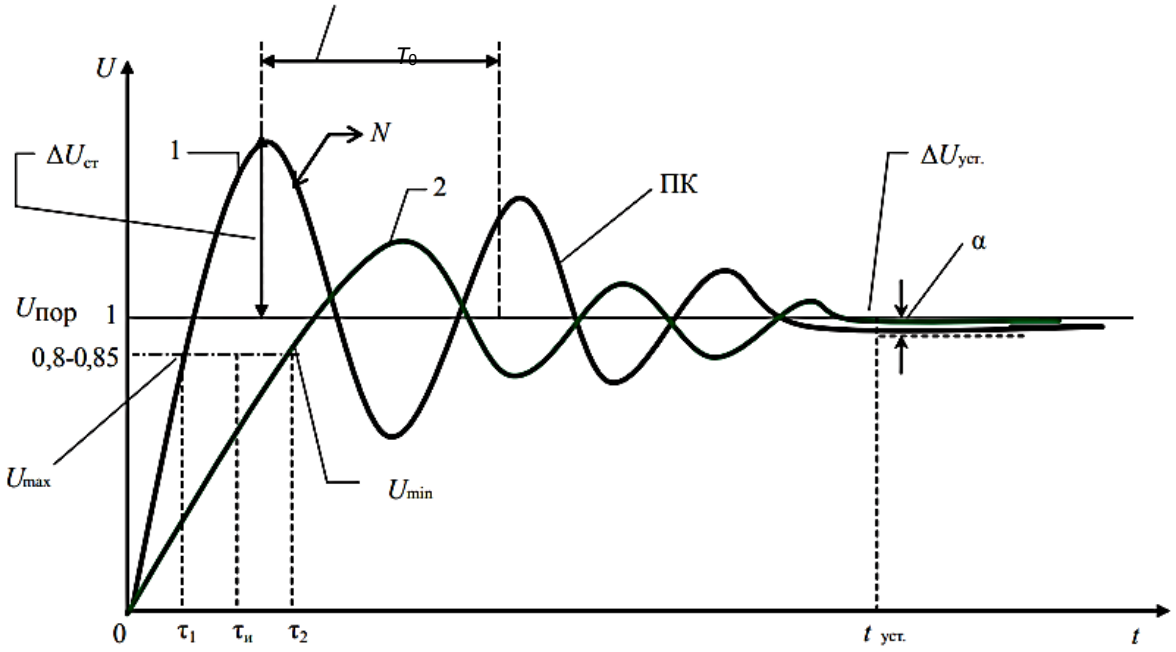


Рис. 1. Перехідний процес та його параметри

Оцінку стану ОК за одним із перелічених вище показників (чи його композиції) можна назвати прямими динамічними оцінками, оскільки вони характеризують динаміку безпосередньо за кривою перехідного процесу [9].

Однак, при контролі ТС сучасних ІБЖ слід враховувати низку особливостей їх побудови:

джерело живлення є первинним елементом технічної системи та не повною мірою відповідає класичному чотириполюснику (відсутні вхідні кола);

сучасне вторинне джерело живлення є автоматичною системою управління (АСУ) замкнутого типу із зворотним зв’язком; у цій системі здійснюється автоматичний контроль основного параметра ІБЖ ($U_{вих}$). Відхилення цього параметра від норми призводить до необхідності внутрішнього регулювання.

Як зазначено у [2], перерегулювання вихідного значення напруги в 20–30 % може призвести до виходу з ладу основного обладнання та вихідних кіл самого ІБЖ (така напруга виходить за межі допустимих рівнів для радіоелектронного комплексу (РЕК) вихідних кіл ІБЖ, тому цього принципово не можна допустити.

Особлива увага на включення сучасних джерел живлення без навантаження ($P_н$=0), що є неприпустимим; інакше кажучи, при включенні джерела, $P_н$ має бути у певних межах ($P_{мін}$ … $P_{макс}$).

Використання первинної інформації для прийняття рішення про технічний стан ОК без попередньої обробки практично неможливо.

При використанні запропонованого методу вдається значно скоротити час, який витрачається на контроль ІБЖ. Це досягається, в першу чергу, використанням єдиного фізичного параметра діагностування.

Крім того, використання методу дозволяє оцінити ТС ОК без розриву зворотних зв’язків (використання особливостей функціонування ОК).

Мінімальна кількість контрольованих параметрів та уніфікація вхідних впливів у представленій методології дозволяє автоматизувати процес контролю технічного стану та процес прийняття рішення.

З практичної точки, постає задача створення пристрою (підсистему контролю ТС обраного ОК) який би задовольняв наступним вимогам:

функціональність – здатність забезпечити необхідний рівень виконання передбачених завдань;

точність – чисельні значення діагностичних параметрів повинні вимірюватись з похибками, які не перевищують задані граничні показники;

надійність – здатність пристрою до безвідмовної роботи протягом заданого часу, обумовленого часом виконання поставленого завдання;

економічна доцільність створення такого пристрою передбачає використання відносно дешевих комплектуючих та їх невелику кількість.

Належний рівень надійності пристрою контролю в цілому забезпечується застосуванням комплектуючих компонентів високого класу точності (з мінімальними допусками), кратним резервуванням експлуатаційних номіналів (за температурою, потужністю та ін.) в сукупності з мінімальною кількістю РЕК.

Функціонування пристрою визначення ТС, обраного ОК, забезпечується апаратною та програмною складовою. До складу апаратної частини входить пристрій формування тестової послідовності, блок керування, засоби отримання та обробки діагностичної інформації.

Структурна схема блоку формування тестової послідовності наведена на рисунку 2, на якому позначено: блок керованого навантаження (БлКН), датчик діагностичної інформації (ДДІ), об’єкт контролю (ОК), блок керування (БлКр), автономна автоматизована система діагностування (ААСД).

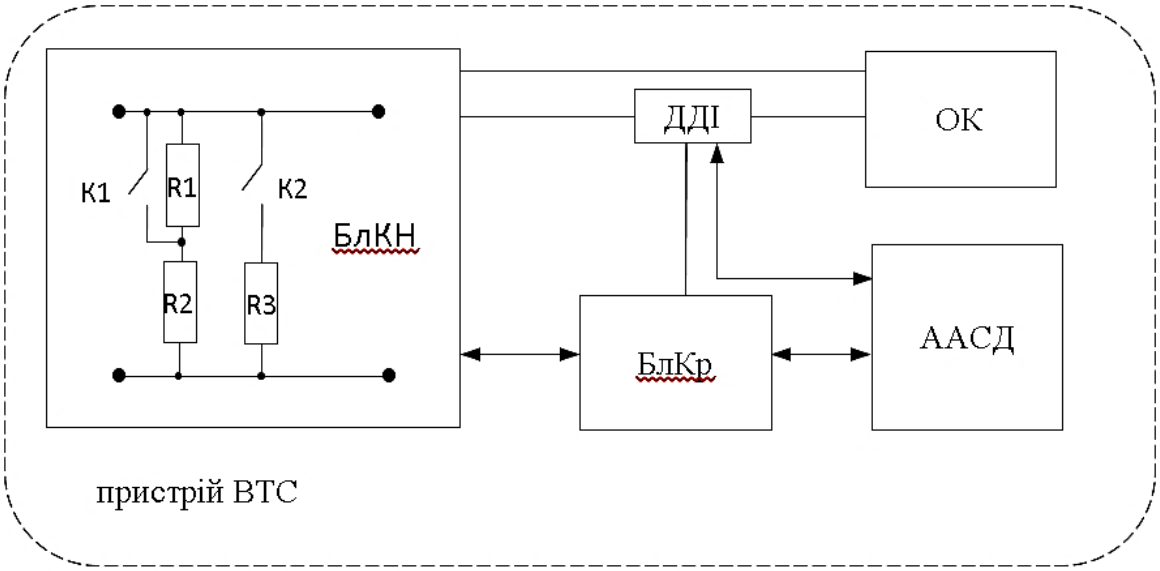


Рис. 2. Структурна схема підсистеми визначення технічного стану

Номінальні значення елементів $R1$ – $R3$, отримані виходячи з технічних характеристик ІБЖ, який підлягає перевірці. Оскільки вмикання обраного ОК без навантаження неприпустимо, то первинне вмикання (вихід імпульсного блоку живлення на робочий режим) здійснюється при номінальному значенні навантаження (вихідного струму). Подальше перемикання навантаження відповідно до обраної форми тестового впливу відбувається шляхом комутації електронними ключами (елементами $K1$, $K2$).

Значення часових параметрів тестового сигналу (управління ключовими елементами) здійснюється мікроконтролером зі складу блоку керування. Початок та завершення тестової послідовності (інтервал часу реєстрації діагностичного параметра) здійснюється автоматично.

Відповідно до представленої методології (частиною якої є безконтактний індукційний метод) отримання діагностичної інформації, в пристрої використано безконтактний індукційний датчик (вторинна обмотка спеціалізованого трансформатора струму). Інформативність (адекватність) отриманих діагностичних даних забезпечується відомим співвідношенням (1):

$$\tau = 3RC, \tag{1}$$

де τ – тривалість перехідного процесу, яка визначається параметрами RC кола;

R – опір ділянки кола**;**

C – сумарна ємність цієї ділянки.

Вважаючи, що величина R є незмінною, можливо стверджувати, що зміна параметрів перехідного процесу обумовлена зміною параметрів складових РЕК ОК.

Проведений аналіз будови ІБЖ, дозволяє стверджувати, що параметри перехідного процесу під впливом навантаження, в першу чергу, визначаються технічним станом електролітичного конденсатора у вихідному фільтрі. За результатами проведеного аналізу цей радіоелектронний компонент визнано низьконадійним.

Таким чином, після обробки діагностичного сигналу (перетворення в цифрову форму та статистичну обробку) отримуємо енергетичний паспорт об’єкта контролю на момент перевірки (з урахуванням часу експлуатації). Прийняття рішення про фактичний технічний стан ОК здійснюється в режимі реального часу системою АСД (автоматична система діагностики) шляхом порівняння інформації (представленої у вигляді гістограми) з еталонним паспортом ОК.

Практична реалізація блоку керування (БлКр) виконана на мікроконтролері *ATMega328* корпорації *MICROCHIP*, що задовольняє вимоги за швидкодією та енергоспоживанням. Мікроконтролери *AVR* мають розвинену систему команд (до 133 інструкцій), високу продуктивність (до 1 *MIPS*/МГц), можливість внутрішньосхемного програмування.

На рис. 3 представлена принципова схема тестової установки. За формування часових інтервалів та керуючих імпульсів (згідно з алгоритмом) відповідає мікроконтролер ATmega328.

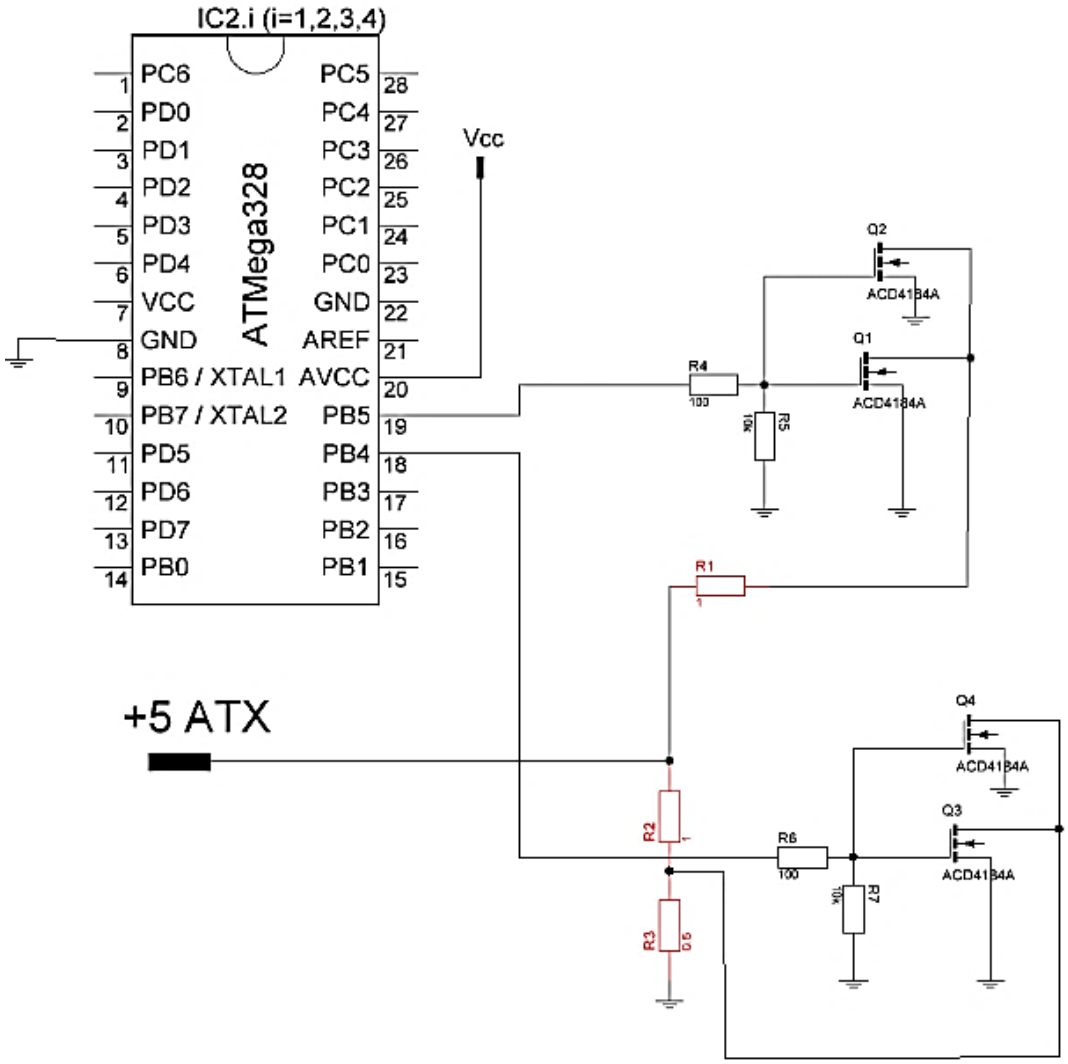


Рис. 3. Принципова схема тестової установки підсистеми визначення технічного стану на базі мікроконтролера ATmega328

В якості силових ключів використані пари MOSFET транзисторів *Q*1, *Q*2 і *Q*3, *Q*4 типу ACD4184A.

Резистори *R*1, *R*2, *R*3 забезпечують потрібні для експерименту значення струму (навантаження блока живлення, що підлягає дослідженню). Потужність розсіювання цих резисторів обрана 10 Вт. Під час експерименту температура їх нагрівання не перевищувала 40 °С.

Значення резисторів R4, R6 забезпечують надійне «відкриття» MOSFET транзисторів. Резистори R5, R7 застосовано для уникнення впливу завад на роботу ключів. Живлення мікроконтролера здійснюється від окремого стабілізованого джерела живлення (напруга 5В).

Програмна складова пристрою визначення технічного стану створена за допомогою інтегрованого середовища розробки *AVR Studio.*

На рис. 4 представлено алгоритм роботи мікроконтролера, завдання якого полягає в формуванні керуючих імпульсів на пари силових транзисторів (типу *ACD4184A*).

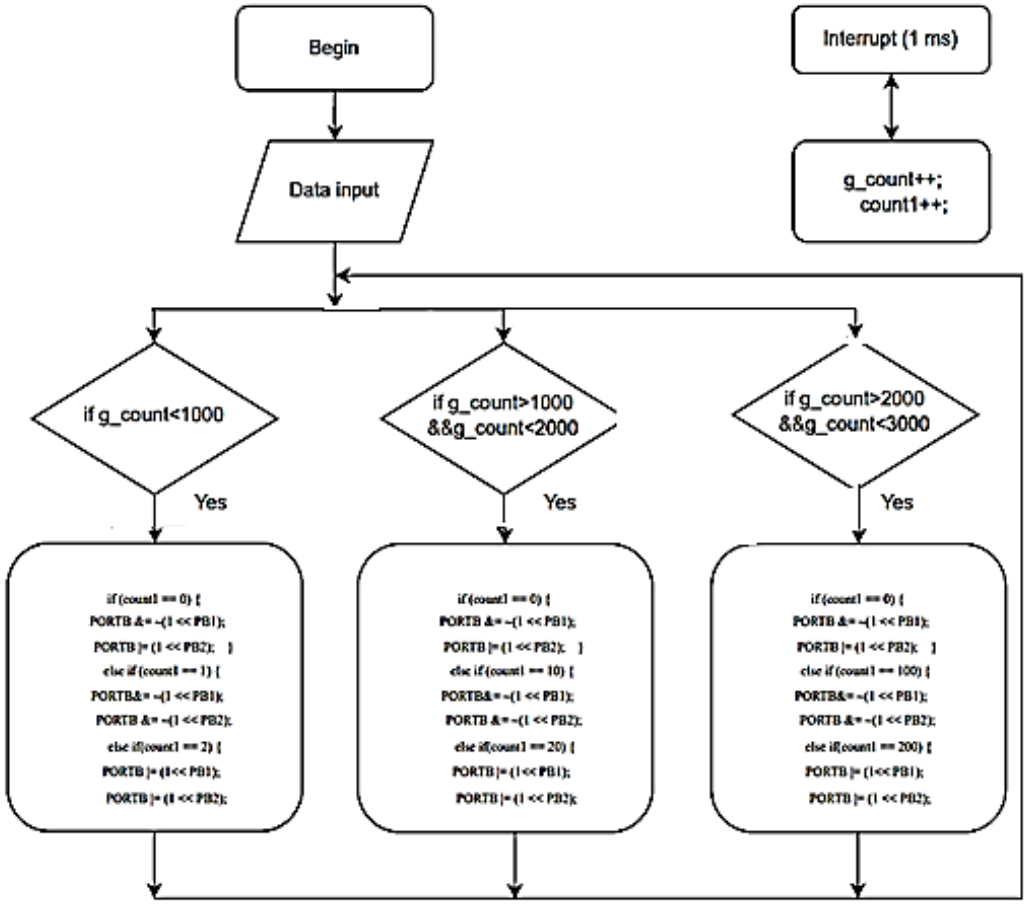


Рис. 4. Блок схема алгоритму функціонування мікроконтролера *ATMega328*

Саме алгоритм формування керуючих сигналів забезпечує необхідну тривалість тестової послідовності та час між перемиканнями.

Під час проведення досліджень довжина тестової послідовності становила 3 секунди. При цьому, всередині тестової послідовності інтервал комутації складав 1 мс, 10 мс та 100 мс відповідно. Зміна часу перемикання дозволила виявити умови отримання діагностичного сигналу з більшою інформативністю (10 мс).

Забезпечення необхідних часових інтервалів виконано з застосуванням переривання мікроконтролера за часом на таймері Т1, в обробнику переривань якого, встановлюються значення змінних g_count, count1.

В основному циклі здійснюється аналіз поточних значень цих змінних, а в заданий момент часу (згідно з алгоритмом) видаються сигнали комутації на виводи мікроконтролера PB5 і PB4, та відповідні затвори пар силових транзисторів.

Практично виготовлений пристрій за схемою на рис. 3 (та алгоритмом функціонування рис. 4) дозволяє виявити технічний стан електролітичних конденсаторів блока живлення у вхідних та вихідних колах фільтрації.

Висновки

Запропонований у рамках методології підхід до діагностування низьконадійних елементів зі складу імпульсних джерел живлення може бути використано для визначення

стану будь яких блоків живлення сучасного РЕО, які містять в собі елементи кіл зворотного зв’язку. Розроблена схема пристрою контролю (алгоритм функціонування, програмна та апаратна складова) дозволяє оцінити технічний стан електролітичних конденсаторів зі складу ІБЖ без їх демонтажу, що принципово відрізняє її від існуючих на сьогодні систем контролю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коренівська О. Л., Бенедицький Б. В. Надійність експлуатація та ремонт радіоелектронної та телекомунікаційної техніки: навч. посіб. Житомирська політехніка, 2020. 181 с.

2. Бобало Ю. Я. Аналіз методів оцінювання безвідмовності систем сумісно працюючих компонентів електронних пристроїв / Ю. Я. Бобало, Л. А. Недоступ, О. В. Лазько // Радіоелектронні і комп’ютерні системи. 2007. № 7 (26). С. 212–214.

3. ДСТУ IEC 60706-2:2008 (IEC 60706-2:2006, IDT) Ремонтопридатність устаткування. Частина 2. Вимоги до ремонтопридатності та дослідження на етапі проектування та конструювання. 45 с.

4. Єманов В. В. Досвід функціонування системи технічного забезпечення силових структур провідних країн світу в умовах кризових ситуацій: Честь і закон. № 2 (85). 2023. С. 80–85.

5. Піддубний В. О., Товкач І. О. Елементна база радіоелектронної апаратури: Пасивні радіокомпоненти. В 4 ч. Ч. 1.: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2021. 98 с.

6. Панфілов І. П., Савицька М. П., Флейта Ю. В. Компонентна база радіоелектронної апаратури: навч. посіб. Модуль 1. Одеса: ОНАЗ ім. О. С. Попова, 2013. 180 с.

7. Толстова А. В., Огненна Х. В. Теоретичні аспекти формування механізму інноваційного розвитку промислового підприємства. Науковий вісник Міжнародного гуманітарного університету. 2016. Вип. 21. С. 106–110. URL: http://www.vestnik-econom.mgu.od.ua/journal/2016/21-2016/24.pdf.

8. K. Khan, R. Verma, A. Roy Review of High Voltage Pulsed Power Supplies and Power Electronics in Pulse Power Generation /Power-Research-A-Journal-of-CPRI URL: https://www.researchgate.net/journal/ Power-Research-A-Journal-of-CPRI-0973; http://dx.doi.org/10.33686/pwj.v19i2.1140.

9. Givi H., Farjah E. and Ghanbari T. A comprehensive monitoring system for online fault diagnosis and aging detection of non-isolated dc–dc converters’ components / IEEE Trans. Power Electron. vol. 34, № 7. 2019. Pp. 6858–6875.

DOI: 10.58254/viti.6.2024.07.93

УДК: 004.056

Куцаєв П. В. ORCID: 0000-0002-3235-3316 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Данилюк І. А. ORCID: 0000-0002-7192-9242 (ВІТІ ім. Героїв Крут)
Паламарчук С. А. ORCID: 0000-0001-7483-9165 (ВІТІ ім. Героїв Крут)
Чередниченко О. Ю. ORCID: 0000-0002-0816-8321 (ВІТІ ім. Героїв Крут)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ПОТРЕБ СЕКТОРА БЕЗПЕКИ І ОБОРОНИ

Блокчейн-технології швидко завойовують популярність у різних галузях завдяки своїй здатності забезпечувати надійний захист даних, прозорість та децентралізацію. Особливо важливими вони стають у сфері телекомунікацій, де зберігання, обробка, передача та управління даними має критичне значення, особливо у військовій сфері. Використання технології блокчейн може значно підвищити рівень безпеки, ефективність та надійність в зазначеній галузі, вирішуючи проблеми централізації та вразливості до атак.

Використання блокчейн-технологій, за рахунок їх децентралізації, значно підвищить безпеку інформаційно-комунікаційних систем, завдяки розподіленій архітектурі, де дані зберігаються на численних незалежних вузлах, що ускладнює їхнє масове знищення чи модифікацію. Відсутність єдиної точки відмови знижує ризики зламів, а механізми консенсусу забезпечують перевірку і захист від несанкціонованих змін. В цілому, така технологія дозволяє створювати більш стійкі, надійні та захищені системи, що дозволить значно зменшити втрати особового складу, техніки та майна.

Метою дослідження є аналіз сучасного стану та існуючих проблемних питань, які автори пропонують вирішити за допомогою розробки та впровадження блокчейн-технологій у телекомунікаційній галузі, зокрема білінгових операцій, роумінгу, управління ідентифікацією користувачів та дослідження можливостей автоматизації процесів за допомогою смарт-контрактів, що дозволить підвищити ефективність роботи інформаційно-комунікаційних систем за рахунок підвищення швидкості передачі даних і оптимізації їх роботи.

Подальші наукові дослідження, на думку авторів, можуть бути спрямовані на можливість масштабування та зниження енергоспоживання використання технології блокчейн, а також на його інтеграцію з іншими технологіями, такими як штучний інтелект та квантові технології.

Ключові слова: *блокчейн, телекомунікації, безпека даних, смарт-контракти, автоматизація, білінг, роумінг.*

P. Kutsaiev, I. Danyliuk, S. Palamarchuk, O. Cherednychenko Prospects of using blockchain technology in the field of information protection in state institutions

Blockchain technologies are rapidly gaining popularity in various industries due to their ability to provide reliable data protection, transparency and decentralization. They become especially important in the telecommunications, where the storage, processing, transmission and management of data are of critical importance, especially the military industry. The implementation of blockchain technology can significantly increase the level of security, efficiency and reliability in the mentioned industry, solving the problems of centralization and vulnerability to attacks.

The use of blockchain technologies, due to their decentralization, will significantly increase the security of information and communication systems, due to the distributed architecture, where data is stored on numerous independent nodes, which makes their mass destruction or modification difficult. The absence of a single point of failure reduces the risks of breaches, and consensus mechanisms provide verification and protection against unauthorized changes. In general, this technology allows for the creation of more stable, reliable and protected systems, which will significantly reduce the loss of personnel, equipment and property.

The purpose of this scientific researching is to analyze the current state and existing problematic issues, which the authors propose to solve with the help of the development and implementation of blockchain technologies in the telecommunications industry, in particular, billing operations, roaming, user identity management, and the researching of the possibilities of automating processes using smart contracts, which will allow to increase the efficiency of information and communication systems, due to increasing the speed of data transmission and optimizing their work.

Further scientific research, according to the authors, can be aimed at the possibility of scaling and reducing energy consumption of the using of blockchain technology, as well as its integration with other technologies, such as artificial intelligence and quantum technologies.

Keywords: *blockchain, telecommunications, data security, smart contracts, automation, billing, roaming.*

Постановка проблеми. У сучасному світі, де дані стають одним з основних засобів у сучасних військових конфліктах, питання їхньої захищеності набувають особливої актуальності. Інформаційно-психологічні операції, крадіжки даних і шахрайство стають щоденними викликами для різних сфер. Технологічні рішення, що базуються на централізованих системах зберігання, стають все менш ефективними для протидії цим загрозам.

У традиційних централізованих системах безпеки даних операції часто перевіряються і підтверджуються центральними серверами або адміністраторами, що може стати потенційною вразливістю, особливо в умовах зростання обсягів даних та цифровізації суспільства. Такі галузі, як державні структури, сили оборони, засоби масової інформації, телекомунікації, фінанси та охорона здоров’я, потребують надійних рішень для забезпечення захисту даних та автоматизації процесів.

Аналіз останніх досліджень. Технологія блокчейн, вперше запропонована у 2008 році Сатоші Накамото для використання у криптовалюті Bitcoin, виявила свій потенціал далеко за межами фінансового сектора. В її основі лежить розподілений реєстр, який зберігає дані у вигляді послідовних блоків, що додаються до ланцюжка, утворюючи своєрідну цифрову книгу, де кожна зміна фіксується і доступна для всіх учасників системи. Це робить блокчейн надзвичайно привабливим для галузей, де потрібно забезпечити незмінність і цілісність інформації, а також прозорість транзакцій між різними сторонами [1].

Останні дослідження підтверджують, що використання блокчейн-технологій стає важливим інструментом для підвищення безпеки інформації в різних галузях, включаючи телекомунікації, фінанси та різноманітні процеси в урядових структурах. Наприклад, автори [5] зазначають, що блокчейн-технологія суттєво спрощує процеси автоматизації та забезпечення безпеки у телекомунікаціях, зокрема через впровадження смарт-контрактів. Саме впровадження блокчейн-технологій підвищує автоматизацію білінгових операцій і роумінгу, що значно підвищує прозорість і надійність транзакцій між операторами зв’язку [2].

Дослідження [6] фокусується на викликах та можливостях впровадження блокчейн-технологій у телекомунікаціях. Вони зазначають, що основними перевагами блокчейн є його здатність захищати ідентифікаційні дані користувачів і запобігати шахрайству. Смарт-контракти дозволяють автоматизувати процеси перевірки ідентичності, що суттєво знижує ризики компрометації даних під час обробки транзакцій [3].

Огляд досліджень, проведений авторами [7], зосереджується на інформаційно-комунікаційних системах із застосуванням блокчейн-технологій для захисту транзакцій і передачі даних. Проведене дослідження свідчить про те, що блокчейн-технологія підвищує ефективність управління мережею та здійснює контроль доступом до ресурсів через децентралізовану платформу. Це відкриває можливості для впровадження блокчейн-технологій не лише в галузі телекомунікацій, але й в інших галузях, таких як фінансові послуги, побутова сфера та охорона здоров’я.

Блокчейн-технології також привертають увагу дослідників у сфері кібербезпеки. Автори [8] у своїх дослідженнях підкреслюють, що основними перевагами блокчейн-технології – є захист даних від модифікацій і фальсифікацій. Вони зазначають, що криптографічні алгоритми, такі як хеш-функція, забезпечують незмінність інформації, що робить використання блокчейн-технологій надійним рішенням для зберігання чутливої інформації.

Крім того, автори [9] провели дослідження економічних аспектів щодо використання блокчейн-технологій. Вони дійшли висновку, що блокчейн-технологія дозволяє знизити витрати на зберігання даних та обробку транзакцій завдяки автоматизації операційних процесів. Їхні дослідження свідчать, що компанії, які використовують блокчейн, досягають вищої стабільності та рентабельності.

Таким чином, аналіз досліджень підтверджує значні переваги блокчейн-технологій для безпеки даних, зниження витрат та підвищення ефективності роботи в різних галузях. Проте, як зазначається у дослідженнях, блокчейн-технологія також стикається з викликами, такими як високе енергоспоживання та проблеми масштабування, що потребує подальших досліджень та вдосконалень [2, 3].

Метою даного дослідження є аналіз сучасного стану та існуючих проблемних питань, які автори пропонують вирішити за допомогою розробки та впровадження блокчейн-технологій у телекомунікаційній галузі, зокрема білінгових операцій, роумінгу, управління ідентифікацією користувачів, та дослідження можливостей автоматизації процесів за допомогою смарт-контрактів, що дозволить підвищити ефективність роботи інформаційно-комунікаційних систем, за рахунок підвищення швидкості передачі даних і оптимізації їх роботи.

Виклад основного матеріалу дослідження. Блокчейн – це децентралізована база даних, яка зберігає записи (блоки) інформації у вигляді послідовного ланцюга. Кожен блок містить хеш попереднього блоку, що робить ланцюг незмінним після додавання нових блоків. Головною особливістю блокчейн є його незмінність, завдяки тому, що будь-які спроби змінити дані у вже створеному блоці призводять до того, що всі попередні блоки цього ланцюга мають бути також змінені, що виявляє фальсифікацію при такій спробі. Це можливо завдяки тому, що всі вузли мережі мають копії всіх блоків, що гарантує високий рівень безпеки.

Блокчейн використовує криптографічні алгоритми для забезпечення захисту даних. Одним з основних механізмів є хеш-функція, яка генерує унікальний цифровий підпис для кожного блоку даних. Цей цифровий підпис неможливо відтворити, що робить фальсифікацію практично неможливою. Кожен новий блок додається до ланцюжка з хешем попереднього блоку, і навіть мінімальні зміни у даних призведуть до зміни хеш-функції, що буде негайно виявлено іншими учасниками мережі.

Крім того, блокчейн підтримує розподілене зберігання даних, де інформація зберігається на всіх вузлах мережі одночасно. Це означає, що навіть якщо один вузол мережі виходить з ладу, дані залишаються доступними для всіх інших учасників. Це суттєво підвищує надійність і стійкість мережі, оскільки втрата або знищення даних на одному вузлі не призведе до втрати інформації.

Ще одним ключовим елементом блокчейн є алгоритми консенсусу, які дозволяють учасникам мережі домовлятися про додавання нових блоків без необхідності у централізованому управлінні. Найпоширенішими алгоритмами консенсусу є Proof of Work (PoW) та Proof of Stake (PoS)**.** Алгоритм PoW передбачає вирішення складних математичних задач, що потребує великих обчислювальних ресурсів. PoS, у свою чергу, дозволяє учасникам мережі валідувати нові блоки, базуючись на їхньому вкладі (стейку) у систему, що зменшує енергоспоживання та збільшує швидкість транзакцій [1, 4].

Смарт-контракти – ще один спосіб використання технології блокчейн, який дозволяє автоматизувати виконання зобов'язань між учасниками договору за попередніми домовленостями, які унеможливлюють випадки шахрайства, будь-ким, в тому числі і членів угоди. Це спеціальні програми, на основі блокчейн-технології, які автоматично виконують умови угоди, щойно всі необхідні параметри виконані.

Наприклад, смарт-контракт може визначити, які дані доступні певному підрозділу на основі його рівня доступу або функціональних обов'язків. При цьому всі дії фіксуються в блокчейн, та будь-яка зміна доступу або перегляд інформації записується для подальшої перевірки. На рис. 1 зображена модель смарт-контракту, який визначає чи має право доступу підрозділ оборони А та В до інформації в блоках.

Рис. 1. Спрощена модель опису функціонування смарт-контракту

Смарт-контракти значно підвищують ефективність транзакцій та усувають необхідність у третіх сторонах, що часто є джерелом затримок та додаткових витрат [1].

Використання блокчейн-технологій у сфері телекомунікацій може суттєво підвищити рівень безпеки даних та автоматизації операційних процесів. Запропонований підхід передбачає впровадження систем на основі блокчейн-технологій для управління доступом, білінгом, роумінгом та ідентифікацією користувачів, що допоможе забезпечити вищу прозорість і стійкість до кібератак.

1. Управління доступом: блокчейн-технології можуть використовуватися для управління доступом до інформації між підрозділами сектора безпеки і оборони завдяки своїй децентралізованій архітектурі і криптографічним методам захисту даних. У такій системі всі операції з даними реєструються у блокчейні, і кожен підрозділ отримує доступ тільки до тієї інформації, яка йому необхідна для виконання своїх завдань. Використання смарт-контрактів дозволяє автоматично надавати або обмежувати доступ до певних даних відповідно до рівня доступу кожного підрозділу. Наприклад, рій БпЛА, який функціонує під управлінням одного блокчейн, може безперервно відображати обстановку в заданому секторі, розпізнавати об’єкти та приймати рішення про приналежність об’єкта ворогу, а далі надавати доступ до даних тільки визначеним підрозділам, тим самим підтримуючи ситуаційну обізнаність для всіх учасників бойових дій [15]. На рисунку 2 представлена методика з використанням блокчейн-технології для виявлення ворожих об’єктів на полі бою.

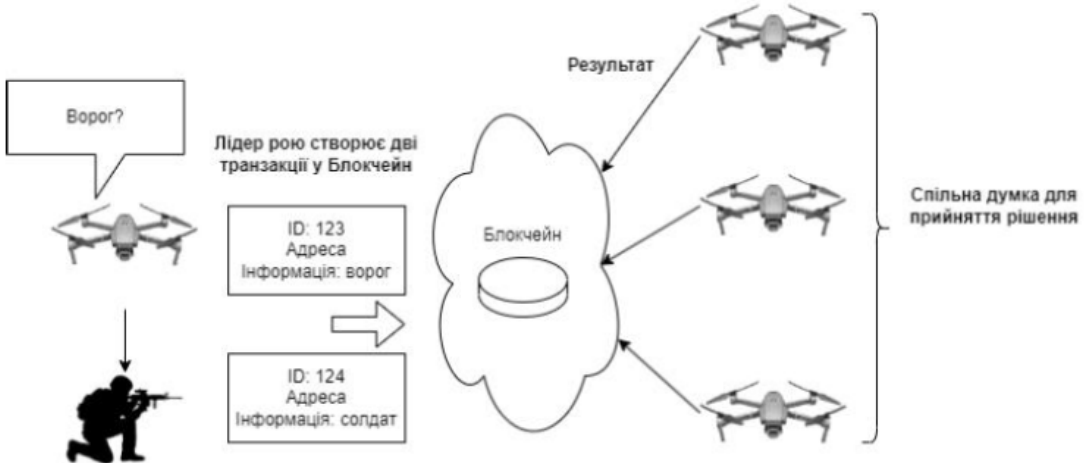


Рис. 2. Методика з використанням блокчейн-технологій для виявлення ворожих об’єктів на полі бою

Децентралізоване зберігання даних: дані зберігаються в розподіленій мережі, що складається з ланцюга блоків, кожен з яких захищений криптографічними алгоритмами. Кожен запит на доступ до інформації записується у блок, і всі вузли ланцюга можуть перевірити легітимність цього запиту. Наприклад, у випадку захоплення ворогом певного пристрою, при спробі підключитись до блокчейну він буде заблокований, оскільки інші учасники будуть попереджені про втрату пристрою. Це запобігає несанкціонованим спробам доступу до інформації.

Шифрування даних: кожен блок у ланцюжку даних шифрується за допомогою криптографічних методів, що дозволяє зберігати дані у незмінному вигляді і забезпечити їхню конфіденційність. Доступ до блоків можливий лише через розшифровку з використанням приватних ключів, що надаються виключно авторизованим користувачам.

Математична модель **контролю за доступом** до інформації між підрозділами базується на розрахунку рівня авторизації доступів до інформації для кожного підрозділу.

Контроль за доступом для підрозділу Ci можна розрахувати як співвідношення кількості успішних доступів до загальної кількості спроб доступу для кожного підрозділу згідно з виразом (1):

$$Ci = \frac{n_{auth}(i)}{n_{total}(i)}, \tag{1}$$

де $n_{auth}(i)$ – кількість авторизованих доступів підрозділу i;

$n_{total}(i)$ – загальна кількість спроб доступу підрозділу i.

Вираз (1) дозволяє оцінити, наскільки успішно підрозділ здійснює доступ до інформації. Якщо $Ci \approx 1$, це означає, що всі спроби доступу були авторизованими, що свідчить про високий рівень контролю за доступом.

Показник Ci може бути оптимізований за допомогою: використання смарт-контрактів для автоматичного управління доступом, додаткового шифрування ідентифікаційних даних користувачів для перевірки їх рівня доступу.

Загальний рівень захищеності військових комунікацій S можна оцінити через сукупність контрольованого доступу до інформації по всіх підрозділах згідно з виразом (2):

$$S = \frac{\sum_{i=1}^{N} C_i A_i}{\sum_{i=1}^{N} A_i}, \tag{2}$$

де N – кількість підрозділів ;

Ci – контроль за доступом для підрозділу i;

Ai – вага або важливість інформації для підрозділу i.

Вираз (2) дозволяє оцінити загальний рівень захищеності мережі, враховуючи як ефективність контролю за доступом до інформації, так і важливість даних, до яких мають доступ підрозділи. Якщо деякі підрозділи мають високий рівень доступу до критично важливих даних, це підвищує загальну вразливість системи, тому слід зосередити ресурси на забезпеченні їх захищеності.

Для підвищення захищеності комунікацій потрібно: збільшити рівень авторизованих доступів $n_{auth}(i)$; впровадити більш ефективні криптографічні механізми для перевірки ідентифікації користувачів; використовувати смарт-контракти для автоматизації процесу контролю доступу.

Оскільки військові комунікації можуть постійно змінюватись (нові підрозділи, змінюється кількість спроб доступу до даних), можна враховувати динаміку зміни рівня захищеності згідно з виразом (3):

$$S(t) = \frac{\sum_{i=1}^{N} C_i(t) A_i}{\sum_{i=1}^{N} A_i}, \tag{3}$$

де t – час надання доступу.

Вираз (3) дозволяє аналізувати, як захищеність змінюється з часом, виявляти підрозділи, які можуть ставати більш вразливими, та швидко реагувати на зміни.

2. Управління білінгом та роумінгом через смарт-контракти: традиційні білінгові системи телекомунікаційних компаній мають певні вразливості, зокрема щодо прозорості розрахунків між операторами. У випадку роумінгу, це може бути досить складний процес, який включає взаємодію різних систем і операторів для правильного розподілу витрат і наданих послуг. Наприклад, під час спільних навчань на території країн-партнерів, потрібно відпрацьовувати розгортання різних типів зв’язку з різними операторами. Застосування блокчейн-технології може стати вирішенням цієї проблеми за рахунок впровадження смарт-контрактів. У випадку з роумінгом, смарт-контракти можуть автоматично розраховувати платежі між операторами на основі фактичного використання послуг (рисунок 3), знижуючи ризик помилок або шахрайства. Це також прискорить процес білінгу, оскільки операції автоматизуються та виконуються майже миттєво [3, 4].

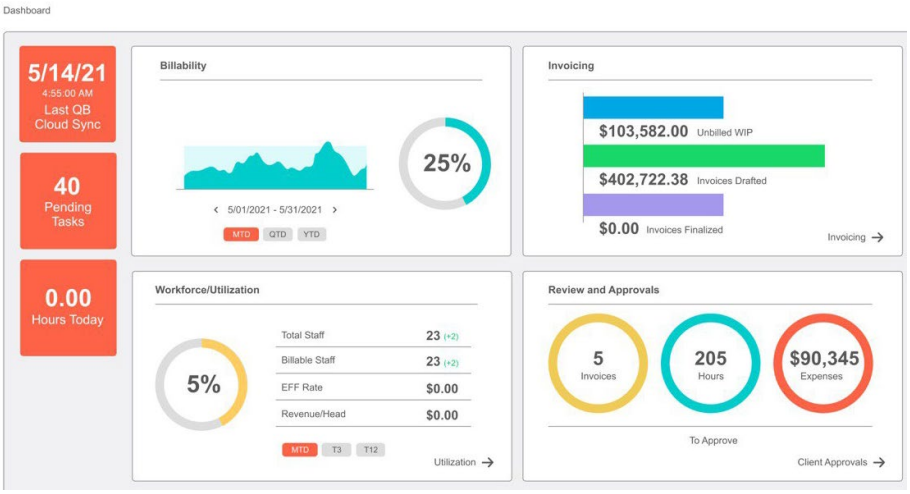


Рис. 3. Автоматичний розрахунок вартості наданих послуг

Смарт-контракти можуть також допомогти вирішити проблеми з оптимізацією білінгу для сил безпеки і оборони (рисунок 4). Замість того, щоб оператори вручну відстежували використання послуг кожного підрозділу та складали рахунки, смарт-контракти можуть автоматично фіксувати всі операції у реальному часі, зберігаючи їх у блокчейні.

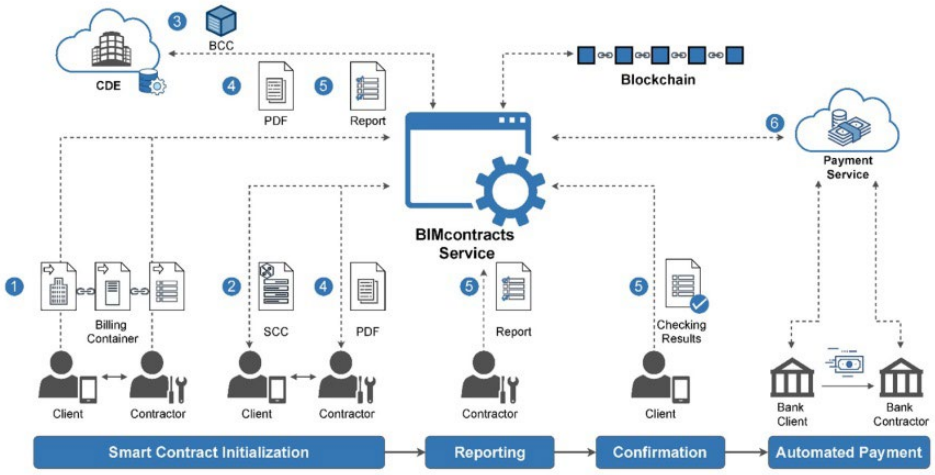


Рис. 4. Схема білінгу для сил безпеки і оборони

Підрозділи можуть мати доступ до детальної інформації про всі свої витрати, що підвищує рівень довіри та прозорості між користувачем і оператором зв'язку [1, 3].

3. Управління ідентифікацією та забезпечення конфіденційності даних: управління персональними даними та ідентифікацією користувачів є однією з найважливіших задач у телекомунікаційних мережах. Використання блокчейн-технологій дозволяє підвищити безпеку цієї інформації через децентралізоване зберігання та криптографічний захист даних. Кожен користувач може мати свій унікальний ідентифікатор, зберігаючи його у блокчейні, що знижує ймовірність несанкціонованого доступу або крадіжки ідентифікаційних даних [1].

Крім того, блокчейн дозволяє користувачам мати контроль над своїми даними. Це означає, що лише користувач може вирішувати, кому надавати доступ до своїх персональних даних, і будь-яка зміна або доступ до цих даних буде зафіксована у блокчейні, забезпечуючи повну прозорість і захист конфіденційності. Цей підхід допомагає вирішити проблеми шахрайства з ідентифікацією та значно знижує ризики витоку даних.

Переваги блокчейн-технології:

1. **Децентралізація**: однією з головних переваг блокчейн є децентралізована архітектура, яка усуває необхідність у довірених третіх сторонах. У традиційних системах безпеки дані, зазвичай, зберігаються на центральних серверах, що створює єдину точку відмови та робить систему вразливою до атак. У блокчейн дані зберігаються на кожному вузлі мережі, і кожен учасник має свою копію всіх транзакцій. Це підвищує стійкість системи до атак, оскільки для модифікації даних необхідно змінити всі копії у всіх вузлах, що майже неможливо. Така децентралізація забезпечує високий рівень **захисту від зовнішніх атак**, зокрема DDoS, та мінімізує ризики внутрішніх загроз.

2. **Прозорість та незмінність даних**: усі транзакції, що зберігаються в блокчейн, прозорі та незмінні. Це означає, що кожна зміна даних фіксується і відразу стає доступною для всіх учасників мережі. Ця властивість робить блокчейн особливо корисним у галузях, де важливо забезпечити довіру між сторонами, наприклад, у фінансових операціях або державних послугах. Крім того, оскільки дані не можуть бути змінені без узгодження з усіма учасниками мережі, це запобігає шахрайству та маніпуляціям [1]. Прозорість блокчейн також дає можливість відслідковувати походження продуктів або транзакцій, що особливо корисно для управління ланцюгами постачання [3].

3. **Підвищення ефективності та автоматизація**: завдяки впровадженню смарт-контрактів блокчейн дозволяє автоматизувати операційні-процеси, які традиційно вимагали участі третіх сторін або ручної перевірки. Використання смарт-контрактів значно знижує витрати на управління операціями та підвищує швидкість їх виконання. На рисунку 5 зображено середній час на виконання операцій з використанням блокчейн-технології та з використанням традиційних баз даних [16].

Впровадження блокчейн-технологій вимагає значного часу на налаштування системи, інтеграцію з існуючими процесами та навчання персоналу. Згідно з виразом (4) можливо оцінити ефективність впровадження блокчейн-технологій у телекомунікаційні мережі з точки зору **приведеного витраченого часу** $NPV_{\text{час}}$.

$$NPV_{\text{час}} = \sum_{t=1}^{T} \frac{CF_t}{(1+r)^t} - I_0, \tag{4}$$

де: $NPV_{\text{час}}$ – приведений витрачений час;

I_0– початкові інвестиції у часі (в середньому оцінюється в 2000 год);

CF_t – щорічна економія часу;

r– ставка дисконтування часу (5% (0.05), що відображає зменшення цінності часу з кожним роком через інші задачі, що потребують уваги).

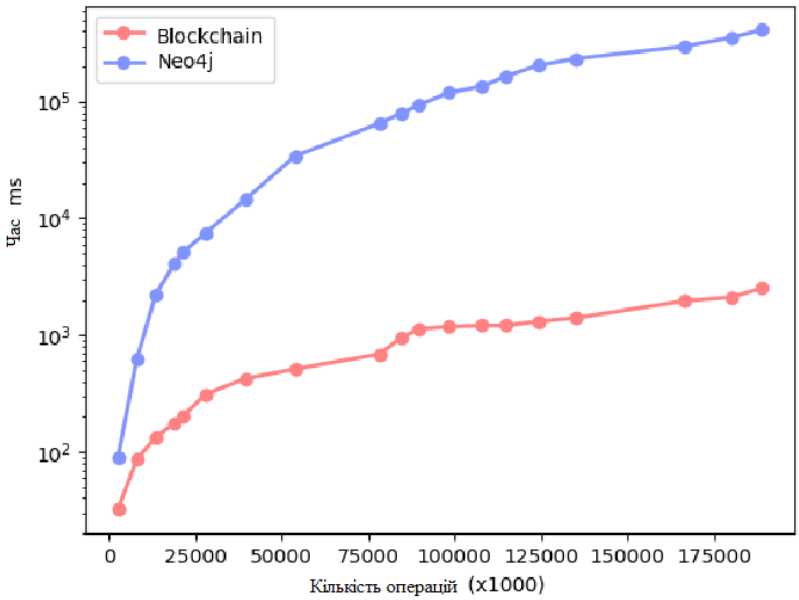


Рис. 5. Середній час виконання запиту для баз даних Neo4j
та при застосуванні блокчейн-технології

Розрахуємо дисконтовану економію часу для першого року згідно виразу (4).

$$\frac{CF_t}{(1+r)^t} = \frac{500}{(1+0.05)^1} = 476.19 \text{ год.}$$

У таблиці 1 наведено приклад розрахунку $NPV_{\text{час}}$ для 5 років.

Таблиця 1

Розрахунок приведеного витраченого часу $NPV_{\text{час}}$

Рік (t)	**Економія часу CF_t, год**	**Дисконтована економія часу $\frac{CF_t}{(1+r)^t}$, год**
1	500	476.19
2	700	635.27
3	800	691.14
4	900	739.39
5	1000	783.53
Разом		3325.52

Загальний $NPV_{\text{час}} = 3325.52 - 2000 = 1325.52$ год

Позитивне значення $NPV_{\text{час}}$ у часі (1325.52 годин) показує, що впровадження блокчейн-технологій у телекомунікаційні мережі дозволяє зекономити значну кількість робочих годин протягом 5 років, що робить впровадження технології ефективним.

4. **Безпека та захист від модифікацій** забезпечується хеш-функціями.

5. **Інтеграція з іншими технологіями для покращення захисту:** використання блокчейн-технологій може бути інтегровано з іншими передовими технологіями, такими як штучний інтелект (ШІ) та квантові технології, наприклад, криптографія з використанням постквантових алгоритмів, для створення більш комплексної системи безпеки. Використання ШІ, для моніторингу транзакцій у блокчейн, дозволить виявляти підозрілі активності та аномалії в реальному часі, що підвищить рівень безпеки мережі. Наприклад, ШІ може аналізувати поведінку користувачів і виявляти будь-які відхилення від нормального патерну, сигналізуючи про можливі втрати пристроїв під час бойових дій або наявність вірусних програм на них.

Квантова криптографія, яка використовує принципи квантової механіки для забезпечення найвищого рівня безпеки, також може бути інтегрована з блокчейн-технологіями. Це дозволить захистити дані навіть від найскладніших, на сьогодні, атак, що можливо тільки при використанні квантових комп'ютерів. Квантова криптографія може значно покращити рівень захисту персональних даних, зберігаючи їх недоступними для зловмисників навіть у майбутніх високотехнологічних атаках.

6. **Підвищення ефективності за допомогою токенізації та децентралізованого управління даними:** однією з новітніх тенденцій у телекомунікаціях є впровадження токенізації, що дозволяє операторам створювати цифрові токени для керування різними активами та послугами. Токенізація на основі блокчейн-технологій може бути використана для надання підрозділам сил оборони доступу до певних послуг або ресурсів, а також для управління використання програмного забезпечення.

Обмеження блокчейн-технології:

1. **Високе енергоспоживання**: одним з найбільших викликів, пов'язаних з використанням блокчейн-технологій, є високе енергоспоживання, особливо у випадку використання алгоритму **Proof of Work (PoW)**, який використовується у таких мережах, як Bitcoin. PoW вимагає значних обчислювальних ресурсів для вирішення складних математичних задач, що підтверджують нові блоки. Це призводить до великих витрат електроенергії, що робить блокчейн менш екологічно чистим рішенням порівняно з традиційними централізованими системами. Наприклад, мережа Bitcoin споживає більше електроенергії, ніж деякі країни, що викликає занепокоєння щодо стійкості цієї технології [1, 2].

2. **Проблеми масштабованості**: іншою значною проблемою блокчейн є його обмежені можливості для масштабування. Оскільки кожна транзакція має бути підтверджена всіма учасниками мережі, це суттєво знижує швидкість обробки даних. Це особливо актуально для мереж, які використовують PoW, де обробка транзакцій може займати кілька хвилин або навіть годин. У таких секторах, як телекомунікації або фінанси, де потрібна висока пропускна здатність, блокчейн може виявитися менш ефективним рішенням [2]. Проте нові алгоритми консенсусу, такі як **Proof of Stake (PoS)**, дозволяють знизити ці проблеми, забезпечуючи вищу швидкість транзакцій та знижуючи енергоспоживання.

3. **Складність інтеграції з існуючими системами**: впровадження блокчейн технологій у вже існуючі централізовані системи може бути досить складним і витратним процесом. Багато держаних структур стикаються з проблемами під час інтеграції блокчейн з наявними ІТ-системами через відмінності в архітектурі та принципах роботи. Це може вимагати значних інвестицій у перепроєктування інфраструктури та навчання співробітників для роботи з новою технологією.

4. **Правові та регуляторні бар'єри**: блокчейн, як і багато інших новітніх технологій, стикається з правовими та регуляторними викликами. Багато країн ще не розробили чітке законодавство, яке б регулювало використання блокчейн-технологій, особливо у сферах оборони, фінансів та обміну даними. Це створює додаткові ризики для державних органів, що планують впровадження цієї технології, оскільки вони можуть стикнутися з правовими обмеженнями або невизначеністю щодо її легальності [4].

Висновки. Проведене дослідження, на думку авторів, свідчить, що використання блокчейн-технологій мають величезний потенціал у забезпеченні безпеки даних у різних галузях, таких як телекомунікація, логістика, проєктування, моніторинг, фінанси, структури державних установ та інші. Блокчейн-технології надають унікальні можливості завдяки своїм властивостям децентралізації, прозорості та цілісності інформації. Ці властивості роблять блокчейн одним із найперспективніших технологічних рішень для боротьби з основними

проблемами сучасних централізованих систем, такими як наявність єдиної точки відмови, недостатня прозорість операцій та високі ризики витоку даних.

Особливо важливими виявляються можливості впровадження блокчейн в інформаційно-комунікаційних системах, де виникає потреба у підвищенні прозорості білінгових операцій, автоматизації процесів роумінгу та управлінні ідентифікаційними даними користувачів. Використання смарт-контрактів дозволяє спростити та прискорити ці процеси, забезпечуючи водночас надійний захист даних і зниження витрат на управління. Це відкриває нові горизонти для підвищення ефективності управління, покращуючи взаємодію між операторами та користувачами.

Блокчейн-технологія також виявляє себе як потужний інструмент для захисту інформації, у таких галузях, як оборона, проєктування, охорона здоров'я та фінансові послуги. Завдяки децентралізованому зберіганню та криптографічним механізмам захисту, блокчейн дозволяє значно знизити ризики витоків інформації та атак на системи зберігання даних. Цю технологію, на думку авторів, доцільно використовувати для управління медичними записами під час військово-лікарської комісії, де повинна забезпечуватися повна прозорість і контроль з боку військовослужбовців над своїми персональними даними.

Незважаючи на значні переваги, блокчейн-технологія має свої обмеження, зокрема пов'язані з проблемами масштабованості та енергоспоживання. Алгоритми консенсусу, такі як Proof of Work (PoW), потребують значних обчислювальних ресурсів для підтримки функціонування мережі, що може стати перешкодою для широкого впровадження блокчейн в системах, де потрібно швидко обробляти великі обсяги даних. Однак нові алгоритми, такі як Proof of Stake (PoS), дозволяють знизити ці обмеження та підвищити ефективність обробки транзакцій, що робить блокчейн більш придатним для комерційного використання.

Перспективи подальших досліджень. Подальші дослідження у сфері розвитку та впровадження блокчейн-технологій, на думку авторів, можуть бути спрямовані на вирішення проблем, пов'язаних з можливістю масштабування та зниження енергоспоживання. Нові алгоритми консенсусу, такі як PoS, PoC (Proof of Capacity) та PoA (Proof of Authority), можуть суттєво покращити продуктивність при застосуванні блокчейн-технологій, що забезпечить водночас високу швидкість транзакцій та низькі витрати на енергоспоживання.

Ще одним перспективним напрямком подальшого розвитку та впровадження блокчейн-технологій може бути інтеграція блокчейн-технологій з іншими передовими технологіями, такими як штучний інтелект (ШІ) та квантова криптографія. Використання ШІ для моніторингу транзакцій у блокчейн може суттєво підвищити рівень захисту мережі, виявляючи аномалії та потенційні загрози в режимі реального часу.

Криптографія, з використанням постквантових алгоритмів, може суттєво підвищити рівень безпеки блокчейн, забезпечуючи захист даних навіть від потенційних загроз, які можуть виникнути з розвитком квантових комп'ютерів. Інтеграція зазначеної технології дозволить створити більш стійкі та безпечні системи для зберігання та обробки даних, що відкриває нові можливості для широкого впровадження блокчейн у майбутньому.

Ще одним важливим напрямом для подальших досліджень автори вважають розробку нормативно-правової бази на державному рівні, що дозволить здійснювати регулювання використання блокчейн-технологій. У багатьох країнах відсутнє чітке регулювання цієї технології, що може стримувати її впровадження на державному рівні та у великих структурах, таких як Збройні Сили України. Розробка нормативно-правової бази, що враховує особливості використання блокчейн-технологій, допоможе знизити правові ризики та сприятиме подальшому поширенню цієї технології для підвищення ефективності функціонування багатьох галузей.

Блокчейн-технологія може запропонувати революційні можливості для **покращення управління логістикою** в ЗСУ, забезпечуючи прозорість та незмінність усіх операцій,

пов'язаних з постачанням техніки, озброєння та матеріалів. Децентралізована система дозволяє зберігати всі транзакції, пов'язані з постачаннями, у вигляді блоків, що гарантує відсутність фальсифікацій або втручань ззовні. Кожна логістична операція реєструється в блокчейні, що дозволяє легко відстежувати будь-яку військову техніку та її стан на будь-якому етапі транспортування або експлуатації.

Використання смарт-контрактів у логістиці дозволяє автоматизувати виконання угод щодо постачання, знижуючи ризики людських помилок та забезпечуючи своєчасність поставок.

Блокчейн-технологія може також бути використана для **моніторингу технічного обслуговування** військової техніки та обладнання. Автоматизована система, на базі блокчейн-технології, дозволить в реальному часі відстежувати стан техніки, що забезпечить підвищення оперативності та забезпечить своєчасність її обслуговування. Кожна операція з технічного обслуговування буде зареєстрована у ланцюжку блокчейн цієї системи, що забезпечить доступ до інформації необхідного персоналу для та оптимізації процесів ремонту та технічного обслуговування.

Під час **проєктування військових систем** (наприклад, систем озброєння або IT-інфраструктури), блокчейн може забезпечити координацію між різними учасниками проєкту (підрядниками та військовими структурами). Це дозволить вести точний облік внесків кожного із учасників, відслідковувати зміни та оновлення при виконанні проєкту. Блокчейн-технологія може бути використана для забезпечення безпеки використання та зберігання даних, що критично важливо при розробці нових технологій, де потрібно уникнути витоків або шахрайства.

Таким чином, впровадження блокчейн-технологій мають потенціал стати основним інструментом для забезпечення безпеки даних і автоматизації операційних процесів у багатьох галузях. Однак, для якісного та ефективного впровадження блокчейн-технологій необхідні подальші дослідження у вирішенні проблемних питань, що на даний час існують при використанні блокчейн-технологій щодо масштабованості, енергетичної ефективності, інтеграції з іншими технологіями та розробки відповідних нормативно-правової законодавчої бази.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Blockchain Technology Review. 2023. URL: https:// ar5iv.labs.arxiv.org/blockchain-review.

2. Blockchain in Telecommunications: Challenges and Opportunities. MDPI Journals. 2022. URL: https://www. MDPI.com/journal/blockchain-telecom.

3. Understanding Blockchain Technology. 2023. URL: https://Reintech.io/blog/understanding-blockchain.

4. Arthur D. Little. How blockchain platforms enhance telecom & media. ADL Insights. 2022. URL: https://www.adlittle.com/blockchain-telecom-media.

5. Zhang, X., Li, J., Wang, Y. Blockchain technology in telecommunications: a review. Journal of Network and Computer Applications. 2022. URL: https://www.journal.com/blockchain-telecommunications-review.

6. Liu, S., Zhao, Q., Chen, R. Application of Blockchain in Telecommunications: Challenges and Opportunities. Telecommunications Policy. 2022. URL: https://www.telecompolicy.org/blockchain-challenges-opportunities.

7. Мануілов Я. С. Використання технології блокчейн у телекомунікаціях // Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки. 2021. Том 32 (71), № 3. С. 123–127. DOI: https://doi.org/10.32838/2663-5941/2021.3/20.

8. Четверіков І. О., Петренко А. І. Впровадження блокчейн для забезпечення інформаційної безпеки // Журнал кібербезпеки. 2021. № 99. С. 162–169. DOI: 10.33111/mise.99.

9. Койбічук В. В., Рожкова М. С. Економічний аналіз використання блокчейн у різних галузях. Науковий журнал економічних досліджень. 2021.

10. Nazanin Moosavi, Hamed Taherdoost. Blockchain Technology Application in Security: A Systematic Review. MDPI, 2023. P. 60-=–70. URL: https://doi.org/10.3390/blockchains1020005.

11. Sparsh Sharma, Imtiaz Ahmad, Shaima Qureshi, Malik Ishfaq. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet, 2022. URL: https://www.mdpi.com/fi14110341.

12. Daneshgar F, Ameri Sianaki O, Guruwacharya P. Blockchain: a research framework for data security and privacy. In Advances in Intelligent Systems Computing. 2019. URL: https://doi.org/10.1007/978-3-030-15035-8_95.

13. Banchhor P, Sahu D, Mishra A, Ahmed MB. A systematic review on blockchain security attacks, challenges and issues. IJERT, 2021. URL: https://www.ijert.org/research/a-systematic-review-on-blockchain-security-attacks-challenges-and-issues-IJERTV10IS040292.pdf.

14. Krishnan KN, Jenu R, Joseph T, Silpa ML. Blockchain based security framework for IoT implementations. IEEE, 2018. URL: https://doi.org/10.1109/CETIC4.2018.8531042.

15. Опірський І., Василишин С. Перспективи військового застосування технології блокчейну // Ukrainian Scientific Journal of Information Security. 2022. Т. 28, № 2. С. 57–66. DOI: 10.18372/2225-5036.28.16950.

16. Tsoulias K., Palaiokrassas G., Fragkos G., Litke A., Varvarigou T. A graph model-based blockchain implementation for increasing performance and security in decentralized ledger systems // IEEE Access. 2020. DOI: 10.1109/ACCESS.2020.3006383.

DOI: 10.58254/viti.6.2024.08.105

УДК 004.738.5:355/359 (021)

Мальцева І. Р. ORCID: 0000-0001-6073-4637 (ВІТІ ім. Героїв Крут)
Черниш Ю. О. ORCID: 0000-0002-6626-5656 (ВІТІ ім. Героїв Крут)
Процюк Ю. О. ORCID: 0000-0001-5193-3669 (ВІТІ ім. Героїв Крут)

АНАЛІЗ АЛГОРИТМІВ РАННЬОГО ВИЯВЛЕННЯ КІБЕРАТАК НА МЕРЕЖІ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Захист критичної інфраструктури та національна безпека посилюються завдяки безпеці та надійності мереж. В цих мережах циркулює різна інформація з різними грифами від відкритої до закритої. Наслідки кібератак на ці мережі можуть, бути серйозними, включаючи шкоду репутації, фінансові втрати, операційні перебої та витік даних. Традиційні методи безпеки, такі як брандмауери та антивірусне програмне забезпечення, стають все менш ефективними проти сучасних і постійно мінливих кіберзагроз. Як наслідок, потужні системи виявлення мережевих вторгнень (IDS) стали незамінними для проактивного виявлення та пом'якшення наслідків кібератак.

Машинне навчання стало життєздатним методом для створення адаптивних засобів виявлення вторгнень, які можуть виявляти нові та складні шаблони атак. Навчаючись на величезних маркованих наборах даних мережевого трафіку, моделі ML можуть розуміти тонкі закономірності і диференціальні ознаки нормальних і аномальних або зловмисних потоків трафіку. Це дозволяє виявляти можливі кіберзагрози та вторгнення, які традиційні IDS на основі сигнатур не можуть виявити. Виділення дискримінаційних ознак і навчання відповідних моделей класифікації з таких даних є непростим завданням.

У представленому дослідженні проведено аналіз ефективності алгоритмів ML для виявлення кібератак, зокрема розподілених атак на відмову в обслуговуванні DDoS, у даних мережевого трафіку. У представленому дослідженні система виявлення мережевих атак розроблена з використанням моделей ML і глибинного навчання (DL) та експериментується на наборі даних CICIDS2017.

Основними завданнями дослідження є розроблення стратегії вилучення цінної інформації з необроблених мережевих потоків; вивчення впливу підготовки даних на частоту хибних спрацьовувань; проведення порівняльного аналізу моделей ML для ідентифікації кібератак.

Основною метою дослідження є забезпечення розуміння розробки надійної адаптивної системи виявлення мережевих вторгнень з використанням підходів ML, які підвищують можливості кібербезпеки та захищають від майбутніх кібератак.

Ключові слова: *машинне навчання, виявлення кібератак, розподілена атака на відмову в обслуговуванні, виявлення мережевих вторгнень, нейронні мережі.*

I. Maltseva, Y. Chernish, Y. Protsiuk Development of algorithms for early detection of cyberattacks on networks using machine learning

Critical infrastructure protection and national security are enhanced by the security and reliability of networks. Various types of information circulate on these networks, ranging in classification from open to closed. The consequences of cyberattacks on these networks can be severe, including reputational damage, financial loss, operational disruption and data leakage. Traditional security methods, such as firewalls and anti-virus software, are becoming less effective against modern and ever-changing cyber threats. As a result, powerful network intrusion detection systems (IDS) have become indispensable for proactive detection and mitigation of cyber attacks.

Machine learning has become a viable method for creating adaptive intrusion detection tools that can detect new and complex attack patterns. By learning from huge labelled network traffic datasets, ML models can understand the subtle patterns and differentiating features of normal and abnormal or malicious traffic flows. This allows them to detect possible cyber threats and intrusions that traditional signature-based IDSs cannot detect. Extracting discriminative features and training appropriate classification models from such data is a challenging task.

In the presented study, we analyse the effectiveness of ML algorithms for detecting cyberattacks, in particular distributed denial of service (DDoS) attacks, in network traffic data. In the presented study, a network attack detection system is developed using ML and deep learning (DL) models and experimented on the CICIDS2017 dataset.

The main objectives of the study are to develop a strategy for extracting valuable information from raw network streams; to study the impact of data preparation on the false positive rate; and to conduct a comparative analysis of ML models for cyberattack detection.

The main goal of the study is to provide an understanding of the development of a reliable adaptive network intrusion detection system using ML approaches that increase cybersecurity capabilities and protect against future cyberattacks.

Keywords: *machine learning, cyberattack detection, distributed denial of service attack, network intrusion detection, neural networks.*

Постановка проблеми. Захист критичної інфраструктури та національна безпека посилюються завдяки безпеці та надійності мереж. В цих мережах циркулює різна інформація з різними грифами від відкритої до закритої. Надання послуг урядами, компаніями і приватними особами призвело до феноменального сплеску використання Інтернету. Незважаючи на очевидні переваги, цей взаємозв'язок робить мережі вразливими до кібернетичних наслідків і атак у широких масштабах [1]. Наслідки кібератак на ці мережі можуть бути серйозними, включаючи шкоду репутації, фінансові втрати, операційні перебої та витік даних. Традиційні методи безпеки, такі як брандмауери та антивірусне програмне забезпечення (АВПЗ), стають все менш ефективними проти сучасних і постійно мінливих кіберзагроз [2]. Як наслідок, потужні системи виявлення мережевих вторгнень (IDS) стали незамінними для проактивного виявлення та пом'якшення наслідків кібератак [3].

Машинне навчання (ML) стало життєздатним методом для створення адаптивних засобів виявлення вторгнень, які можуть виявляти нові та складні шаблони атак [4]. Навчаючись на величезних маркованих наборах даних мережевого трафіку, моделі ML можуть розуміти тонкі закономірності і диференціальні ознаки нормальних і аномальних або зловмисних потоків трафіку [5]. Це дозволяє виявляти можливі кіберзагрози та вторгнення, які традиційні IDS на основі сигнатур не можуть виявити. Однак застосування моделей ML в індустрії кібербезпеки є досить складним. Дані мережевого трафіку надзвичайно різноманітні та незбалансовані, і лише невеликий відсоток з них вказує на справжні інциденти атак [6]. Виділення дискримінаційних ознак і навчання відповідних моделей класифікації з таких даних є непростим завданням. Крім того, IDS повинна підтримувати надзвичайно низький рівень помилкових спрацьовувань, щоб не перевантажувати команди безпеки неправильними оповіщеннями [7].

Аналіз останніх досліджень і публікацій. За останні роки численні дослідники вивчали методи ML для виявлення вторгнень та аномалій у мережі. Автори публікації [8] проаналізували різні підходи ML, такі як Дерева рішень (DT), опорно-векторні машини (SVM), випадкові ліси (RF) та наївний Баєс (NB), на наборах даних NSL-KDD та KDDCup'99 для виявлення мережевих вторгнень.

Було виявлено, що модель RF досягла точності 99,9% на наборі даних NSL-KDD. В роботі [9] запропоновано новий підхід на основі кластеризації, який групує різні типи атак за даними мережевого трафіку в окремі кластери. Це дозволяє розробляти індивідуальні моделі виявлення вторгнень для кожної категорії атак.

Проаналізувавши різні типи мережевих атак, які повинні виявляти моделі ML, включаючи DDoS [10], SQL-ін'єкції [11], виявлення "безпечної оболонки" грубою силою (SSH) [12], атаки типу "людина посередині" та інші, автори [13] спеціально вивчали питання безпеки бездротових мереж і підкреслили важливість виявлення активних атак, таких як DDoS, у відкритих середовищах [14].

Набори даних (KDDCup1999 та NSL-KDD) були широко застосовані для оцінки мережевих IDS [15–20]. Однак, слід зазначити, що ці набори даних є досить застарілими і не зовсім точно відображають сучасні мережеві атаки.

Мета та завдання дослідження. Метою дослідження є вивчення ефективності алгоритмів ML для виявлення кібератак, зокрема розподілених атак на відмову в обслуговуванні DDoS, у даних мережевого трафіку. Проведення порівняльного аналізу моделей ML для ідентифікації кібератак.

Виклад основного матеріалу. Для експериментів використовується новий набір даних CICIDS2017, який є найсучаснішим, що включає найпоширеніші потоки атак. Досліджено та

оцінено кілька методів ML, включаючи DT, штучні нейронні мережі (ANN) та ансамблеві підходи (EL).

Для виявлення мережевих атак оцінюються класичні моделі ML, EL та підходи DL. Класичні підходи ML включають SVM, DT і метод K-найближчих сусідів (KNN), підходи EL включають RF, метод AdaBoost і XGBoost, а методи DL – архітектуру багатошарового перцептрона (MLP) і нову модель Deep MLP. Дві архітектури щільних шарів використовуються в Deep MLP з функціями активації ReLU та сигмоїдної активації. Представлене дослідження сприяло бінарній класифікації зразків мережевого трафіку як атакуючих, так і нормальних.

Для навчання та тестування моделей було використано набір даних CICIDS2017, створений Канадським інститутом кібербезпеки (CIC). CICIDS2017 містить велику базу даних мережевого трафіку для експериментів.

Особливістю CICIDS2017 є представлення широкого спектра сценаріїв атак – DoS і DDoS-атак, вебвторгнень, таких як SQL-ін'єкції та "міжсайтовий скриптинг" (XSS), інфільтраційні атаки та діяльність бот-мереж. Створений навмисно для відтворення реальних загроз, цей набір даних є ресурсом для дослідників, які розробляють та оцінюють системи виявлення вторгнень та інші рішення з кібербезпеки. Дана база даних розподілена на такі сегменти, як Normal traffic, Fuzzers, Reconnaissance, Analysis, Backdoors, DoS attacks, Exploits, Shellcode, Generic attacks та Worms.

Нехай набір даних (S_1, S_2, ..., Sn) складається з n вибірок, де кожна вибірка S_i представлена вектором ознак (f_1, f_2, ..., f_{47}, T, C). Ознаки від f_1 до f_{47} представляють різні характеристики мережевого трафіку, T – це мітка типу атаки, а C – бінарна мітка мережевого трафіку, яка вказує на те, чи є зразок нормальним, чи є він атакою. Мітка типу атаки T може приймати одне з значень: Analysis, Backdoors, DoS attacks, Fuzzers, Generic attacks, Shellcode, Reconnaissance, Exploits, Worms або Normal traffic. З вибірки S_j мітка мережевого трафіку представляє статус трафіку, атакованого або нормального. Основна мета моделей класифікації – віднести трафік до класів атакованого або звичайного трафіку. Більше того, для зразків, ідентифікованих як атаки, модель повинна визначати конкретний тип атаки, пов'язаний з "S_j". Комплексна архітектура для виявлення мережевих загроз представлена на рис. 1.

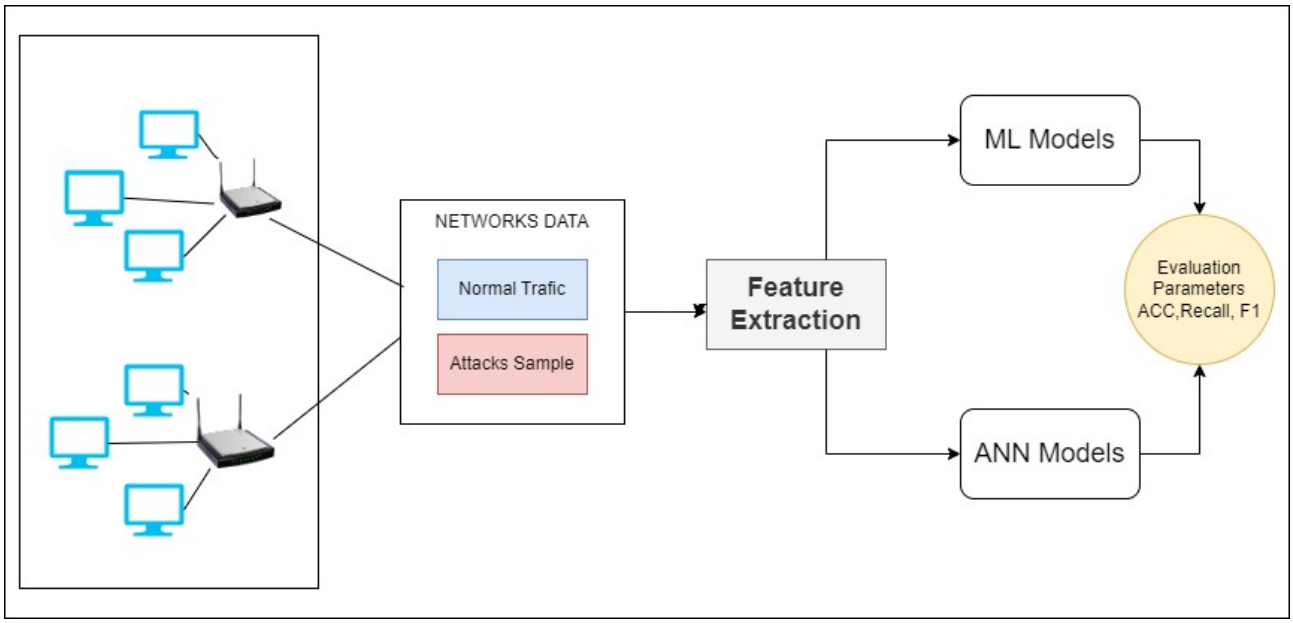


Рис. 1. Комплексна архітектура для виявлення мережевих загроз

Виявлення мережевих атак є критично важливим завданням у сфері кібербезпеки і вимагає спеціальних знань. ML пропонує потужний підхід для виявлення та пом'якшення Exploits і типових кібератак, використовуючи свою здатність аналізувати великі та складні набори даних для виявлення шаблонів і аномалій, які можуть вказувати на зловмисну діяльність. У контексті виявлення Exploits моделі ML можна навчити розпізнавати сигнатури відомих Exploits шляхом аналізу функцій, отриманих із мережевого трафіку, системних журналів і поведінки програми. Наприклад, алгоритми контрольованого навчання можна використовувати для класифікації шаблонів трафіку як доброякісних або шкідливих на основі позначених наборів даних, що дозволяє виявити відомі Exploits з високою точністю. Класичні алгоритми, такі як SVM, ANN та DT, досягли успіху в цій галузі. SVM вміють знаходити оптимальні гіперплощини, що робить їх ідеальними для великих наборів ознак. KNN посилається на сусідні зразки для прогнозування, в той час як DT надають швидкі, зрозумілі рішення шляхом розбиття даних на частини. З розвитком кіберзагроз з'являється простір для надійних методів виявлення. XGBoost, що використовує градієнтне підсилення та регуляризацію, вирізняється низькою чутливістю до перенавчання. MLP, що застосовується для нелінійного мапування, використовує зворотне поширення для вивчення складних патернів у прихованих шарах.

Нова архітектура Deep MLP з активацією ReLU та сигмоїдною функцією активації фіксує мінімальні зміни тенденції мережевого трафіку для точного виявлення атак. XGBoost, і Deep MLP пропонують надійні інструменти для ML та DL, що дозволяють автоматично розпізнавати складні закономірності у величезних масивах даних. Методи регуляризації гарантують, що моделі зберігають ефективність у різних сферах застосування, підвищуючи їхню стійкість і корисність у кібербезпеці.

ML особливо ефективний у виявленні типових кібератак, таких як phishing, DDoS-атаки та зараження шкідливим програмним забезпеченням. Використовуючи методи виявлення аномалій, ML може виявляти відхилення від нормальної поведінки, які можуть означати триваючу атаку. Моделі неконтрольованого навчання, такі як кластерізація та автокодери, можуть ідентифікувати нові атаки або атаки нульового дня, які не відповідають жодним відомим сигнатурам, позначаючи незвичайні шаблони або викиди в даних.

У реальних додатках комбінація методів машинного навчання часто використовується для створення надійних і адаптивних систем безпеки. Гібридні моделі, які об'єднують методи виявлення як на основі сигнатур, так і на основі аномалій, забезпечують комплексний механізм захисту, здатний протистояти широкому спектру загроз. Крім того, постійне навчання та адаптація мають вирішальне значення, оскільки моделі ML мають регулярно оновлюватися новими даними та сигнатурами атак, щоб залишатися ефективними проти кіберзагроз, що постійно змінюються. Цей підхід не тільки покращує здатність виявляти кібератаки та реагувати на них у режимі реального часу, але й знижує рівень помилкових спрацьовувань, тим самим покращуючи загальну безпеку інформації.

Показники оцінювання

Система виявлення мережевих атак оцінюється за допомогою оціночних метрик, що виводяться з матриці заплутаності. Матриця заплутаності, таблиця 2×2, обчислює істинні спрацьовування (правильно ідентифіковані атаки, правильно ідентифікований нормальний трафік), хибні спрацьовування (пропущені атаки, неправильно ідентифіковані атаки).

Прогностична здатність кожної моделі оцінюється за показником продуктивності (Accuracy) та розраховується як частка правильно класифікованих зразків від загальної кількості зразків. Відклик (Recall), також відомий як істинно позитивний показник (True Positive rate), відображає здатність моделі виявляти атаки, обчислюючи частку правильно ідентифікованих атак, а правильний прогноз представлено метрикою Precision, що вимірює надійність позитивних прогнозів, оцінюючи частки справжніх атак серед зразків, позначених

як атаки. Показник F1 дає збалансовану оцінку ефективності моделі, враховуючи як Precision, так і можливість запам'ятовування.

Дослідження та результати

Апаратна специфікація для розробки системи виявлення мережевих вторгнень включає процесор Intel Core i7 (11-го покоління), 16 ГБ оперативної пам'яті та жорсткий диск 1 ТБ, а також операційну систему Ubuntu 20.04.4. Мова програмування Python використовувалася для реалізації моделі ML з бібліотекою Keras 2.3.1 для підтримки TensorFlow 2.2.0 для розробки та навчання нейромережевих моделей.

Ефективність моделей ML

Результати роботи різних моделей ML у виявленні мережевих атак представлені в таблиці 1, 2 та на рис. 2, 3. Моделі оцінюються за допомогою запам'ятовування метрик, продуктивності (Accuracy), точності (Precision) та збалансованої оцінки ефективності моделі (F1). Відклик (Recall) відображає здатність моделі знаходити відповідні випадки, а правильний прогноз представлено метрикою Precision.

Accuracy на рівні 99,05 %, досягнута класифікатором DT, та високою збалансованою оцінкою ефективності моделі на рівні 99 %, що свідчить про ефективність моделі у виявленні мережевих атак. Модель SVM також продемонструвала високу Accuracy на рівні 95,17 та отримала збалансовану оцінку ефективності моделі на рівні 94 % відповідно.

Таблиця 1

Оцінка ефективності методів ML

Model	Recall	Precision	Accuracy	F1-measure
DT	99	99	99,05	99
SVM	93	96	95,17	94
RF	99	99	98,96	99
AdaBoost	97	98	97,87	98
XGBoost	97	98	98,08	98
MLP	96	98	97,47	97

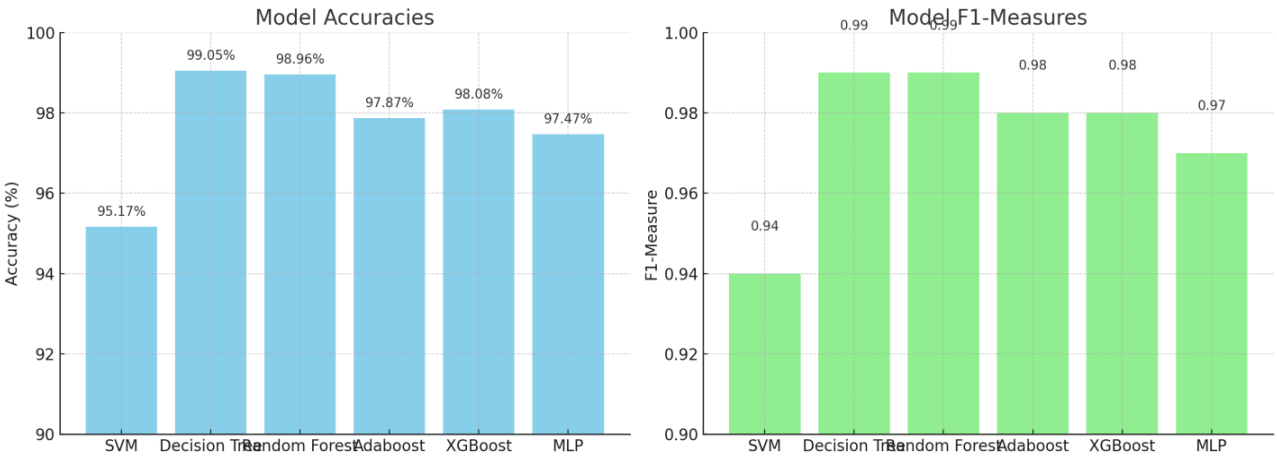


Рис. 2. Порівняльний аналіз продуктивнсоті та збалансованої оцінки ефективності моделі

Для оцінки алгоритму KNN (табл. 2, рис. 3) було протестовано декілька моделей з різними значеннями K (від 2 до 9). Найвища Accuracy на рівні 95,58, була досягнута при значенні K, рівному 7. Вибрані метрики для навчання моделі виявилися дуже релевантними, ефективно відрізняючи шаблони звичайного трафіку від зловмисного.

Це свідчить про те, що основні ознаки були достатньо виразними, а межі рішень могли бути ефективно відображені за допомогою ієрархічної структури DT.

Таблиця 2

Результати роботи моделей KNN

Модель	Recall	Precision	Accuracy	F1 measure
2-NN	95	93	94,51	94
3-NN	95	95	95,47	95
4-NN	95	94	95,12	94
5-NN	95	95	95,56	95
6-NN	95	94	95,31	95
7-NN	**94**	**95**	**95,58**	**95**
8-NN	95	95	95,48	95
9-NN	94	95	95,57	95

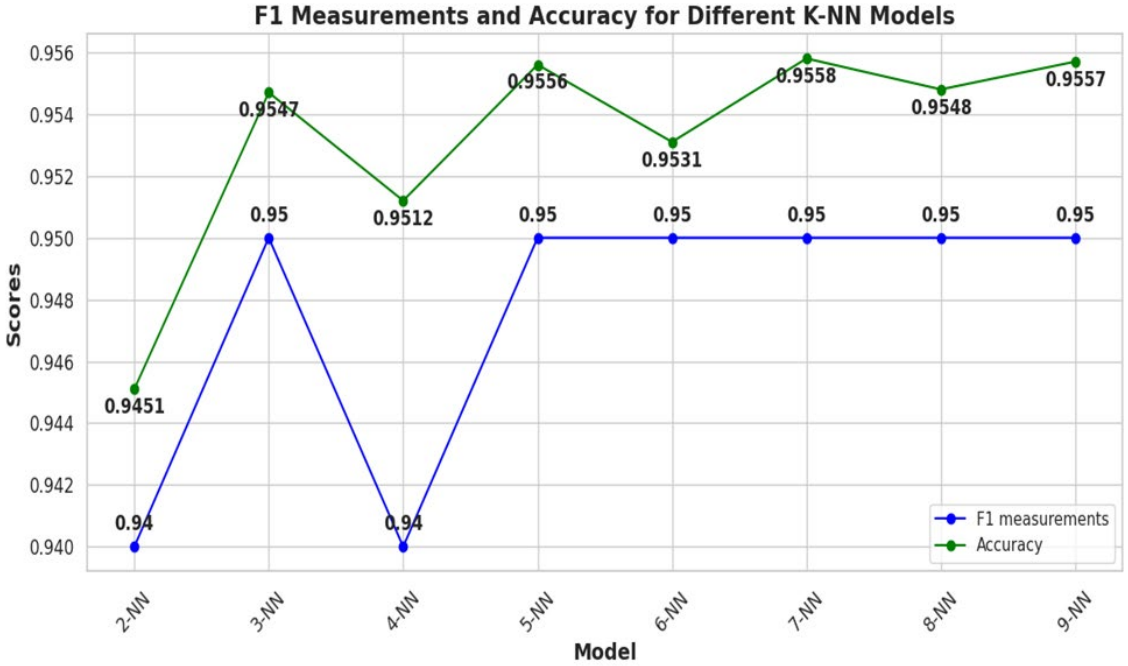


Рис. 3. Відновлення KNN після виявлення атаки

Хоча модель SVM досягла Recall на рівні 93 %, що свідчить про її здатність розпізнавати велику частку атак (істинних спрацьовувань), її Accuracy була відносно нижчою порівняно з іншими моделями.

Порівняно з попередніми роботами дослідників [2], результати яких показали Accuracy на рівні 85,56 % для DT та 81,34 % для штучних нейронних мереж (ANN), запропонована система досягла значно вищої Accuracy на рівні 99,05 % для DT та 97,47 % для MLP.

Це покращення підкреслює релевантність та розпізнавальну здатність ознак у наборі даних CICIDS2017, що свідчить про те, що відбір ознак може бути необов’язковим і може потенційно знизити Precision.

Продуктивність моделей DL

Модель Deep MLP продемонструвала відмінні результати виявлення мережевих атак, як показано в таблиці 3 та на рис. 4. Завдяки оптимізатору Adam і співвідношенню об’єму навчальної та тестової вибірки 80:20 вона досягла високої Accuracy на рівні 98,44 % та високої

збалансованої оцінки ефективності моделі на рівні 98 %, що демонструє свою здатність ефективно виявляти атаки, мінімізувавши при цьому помилкові класифікації.

Оптимізатор Adam мав більшу продуктивність ніж оптимізатор Stochastic Gradient Descent, що сприяло високим результатам Deep MLP. Співвідношення 80:20 між тренуванням і тестом відповідає розподілу звичайного і зловмисного трафіку в реальних системах, що дозволяє моделі добре узагальнювати приховані дані.

Таблиця 3

Результати роботи оптимізаторів SGD та ADAM

Optimizer	Train: Test	Recall	Precision	Accuracy	F1-measure	AUC
SGD	90:10	98	98	98,19	98	97,6
SGD	80:20	97	98	97,68	97	97,1
SGD	70:30	98	98	97,99	98	97,5
SGD	60:40	97	98	97,82	97	97,2
ADAM	90:10	98	98	98,11	98	97,5
ADAM	80:20	98	98	98,44	98	98,1
ADAM	70:30	98	98	98,36	98	98
ADAM	60:40	98	98	98,35	98	97,9

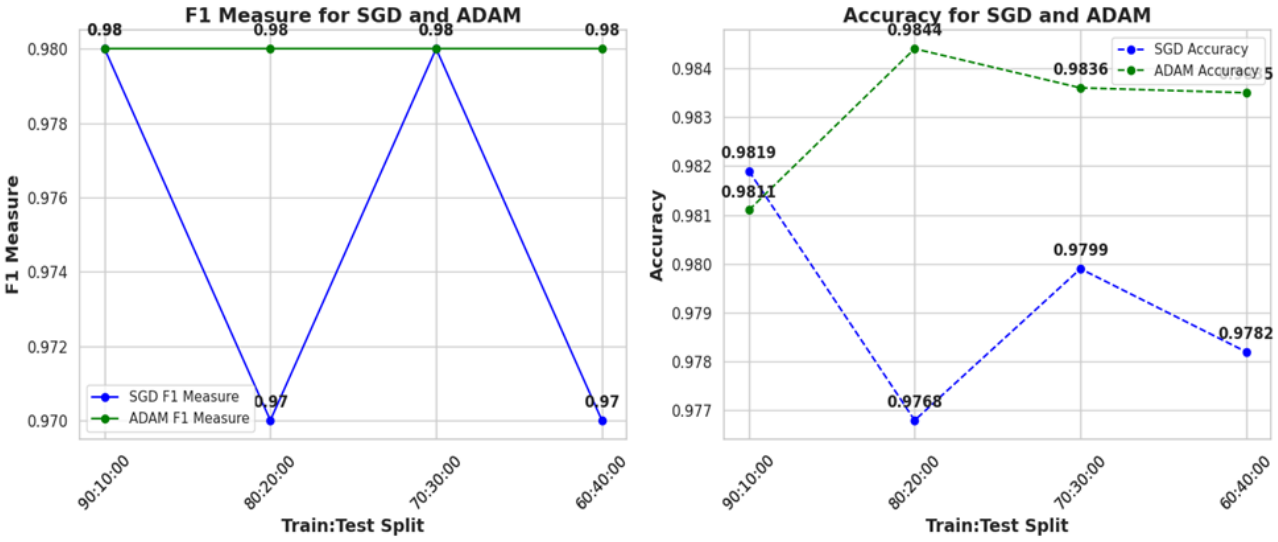


Рис. 4. Порівняння точності та F1-оцінки Deep MLP

Ефективність моделей виявлення атак

У таблицях 4–8 представлено ефективність чисельних моделей ML, EL та DL у виявленні дев'яти різних типів мережевих атак.

Далі в таблиці 4 представлена ефективність різних моделей ML, EL та DL у виявленні атак Analysis. Модель RF демонструє належні показники в усіх метриках, а збалансована оцінка ефективності моделі в межах 24 %. З іншого боку, модель XGBoost має найвищу Accuracy на рівні 72 %, але її Recall та Precision значно нижчі, що свідчить про те, що вона не може послідовно ідентифікувати всі справжні тривоги. Модель AdaBoost демонструє погані результати, з усіма метриками на рівні або нижче 5 %, що свідчить про те, що вона значно гірше справляється з цим типом атак. Моделі MLP та DT мають схожу картину, з дещо вищою Precision, але нижчими показниками Recall та Accuracy. Нарешті, модель 7-NN досягає відносного балансу, з показниками Recall та збалансованої оцінки ефективності моделі до

17 % та 25 % відповідно, забезпечуючи більш середню Accuracy порівняно з іншими оціненими моделями.

Таблиця 4

Analysis атаки та ідентифікація результатів

Model	**Recall**	**Precision**	**Accuracy**	**F1-measure**
DT	13	51	13	20
7-NN	17	47	17	25
RF	24	25	24	24
AdaBoost	2	5	2	2
XGBoost	20	72	20	31
MLP	13	64	13	22

У таблиці 5 представлена ефективність різних моделей ML у виявленні DoS-атак. Модель RF має збалансовані метрики, з Precision на рівні 38 % та Accuracy на рівні 36 %. Дана модель має достатню здатність точно ідентифікувати позитивні випадки без великої кількості хибнонегативних результатів. Модель XGBoost має найвищу Precision на рівні 42 %, але немає належного рівня до Recall та Accuracy. Це вказує на те, що модель не здатна ідентифікувати більшість справжніх позитивних DoS-атак. Моделі AdaBoost та MLP мають обмежені значення у виявленні DoS-атак, що призводить до низьких показників за всіма метриками. Це свідчить про більший відсоток хибних спрацьовувань і загальну неефективність у цьому випадку. Модель DT майже неефективна, з усіма метриками на рівні 1 %, що свідчить про її недостатню ефективність. Модель 7-NN постійно досягає показників на рівні 30 %, що свідчить про помірний рівень Accuracy, Precision та збалансованості її можливостей виявлення.

Таблиця 5

Результати ідентифікації DoS-атак

Model	Recall	Precision	Accuracy	F1-measure
DT	1	1	1	1
7-NN	30	30	30	30
RF	36	38	36	37
AdaBoost	3	10	3	5
XGBoost	4	42	4	6
MLP	10	40	10	15

У таблиці 6 представлена ефективність різних моделей у виявленні Exploits, які використовують слабкі місця в мережах. Модель RF серед всіх запропонованих моделей, має високу ефективність з Precision на рівні 75 % та Accuracy на рівні 80 %. Це свідчить про те, що вона надійно виявляє атаки з використанням Exploits, не генеруючи при цьому багато хибних спрацьовувань. XGBoost має нижчу Precision на рівні 62 %, але перевершує її за метриками Recall та Accuracy на рівні 94 %, що робить її високоефективною у виявленні більшості істинно позитивних випадків, що має вирішальне значення в певних сценаріях. Модель AdaBoost, незважаючи на Precision на рівні 57 % та Accuracy на рівні 36 %, демонструє помірну працездатність, але має деякі проблеми із загальним представленням, про що свідчать її нижчі показники Recall та збалансованої оцінки ефективності. Модель MLP має високу метрику Recall та Accuracy на рівні 88 %. Це свідчить про те, що вона ефективно виявляє атаки з використанням Exploits. Нарешті, модель DT, вона хоч і має нижчу Precision на рівні 54 %, але демонструє дуже високі показники у Recall та Accuracy на рівні 91 %. Це дає змогу стверджувати, що вона може ідентифікувати майже всі атаки з використанням Exploits, але за рахунок більшої кількості помилкових спрацьовувань.

Таблиця 6

Результати ідентифікації атак з використанням Exploits

Model	Recall	Precision	Accuracy	F1-measure
DT	91	54	91	68
7-NN	74	63	74	68
RF	80	75	80	77
AdaBoost	36	57	36	44
XGBoost	94	62	94	74
MLP	88	62	88	73

У таблиці 7 представлено ефективності різних моделей у виявленні Generic атак, які включають широкий спектр методів атаки без конкретного націлювання на вразливості програмного забезпечення. Моделі RF, XGBoost та MLP демонструють високу Precision та Accuracy, а їхні результати наближаються до ідеальних. Модель RF має Precision на рівні 98 % та Accuracy на рівні 97 %, що свідчить про її здатність точно ідентифікувати Generic атаки, мінімізуючи при цьому помилкові спрацьовування. Модель XGBoost та MLP дещо перевершує модель RF за Precision на рівні 99 %, але має однаковий Recall та Accuracy, демонструючи її ефективність класифікувати реальні випадки Generic атак належним чином та без суттєвих пропусків. Модель AdaBoost майже неефективна, з усіма метриками на рівні 1–2 %, що свідчить про її недостатню ефективність.

Таблиця 7

Результати ідентифікації Generic атак

Model	Recall	Precision	Accuracy	F1-measure
RF	97	98	97	98
AdaBoost	1	4	1	2
XGBoost	97	99	97	98
MLP	97	99	97	98

У таблиці 8 представлена ефективність різних моделей у виявленні атак Worm, Backdoor та Shellcode, отриману за допомогою Accuracy та збалансованої оцінки ефективності. Серед представлених моделей, SVM демонструє найвищу Accuracy для Worm і Shellcode на рівні 38 % та 39 %, що свідчить про його здатність розрізняти різні типи атак. Однак збалансована оцінка ефективності для SVM, для Worm і Shellcode, є відносно низька, що вказує на потенційні труднощі в досягненні балансу між Precision та Recall. AdaBoost демонструє Accuracy із Precision на рівні від 27 % до 65 % і з відносно вищою збалансованою оцінкою ефективності у всіх категоріях порівняно з іншими моделями. І навпаки, такі моделі, як MLP, демонструють нижчі показники Precision на рівні від 13 % до 50 %, і відносно послідовну збалансовану оцінку ефективності для різних типів атак. Загалом, хоча деякі моделі демонструють кращу Precision, їхні збалансовані оцінки ефективності потребують подальшого вдосконалення, щоб мати змогу ефективно розпізнавати кожну категорію атаки. Ці результати підкреслюють важливість постійної оптимізації для підвищення ефективності систем виявлення кіберзагроз.

Таблиця 8

Результати ідентифікації атак Worm, Backdoor and Shellcode

Model	Accuracy			F1-measure		
	Worm	Backdoor	Shellcode	Worm	Backdoor	Shellcode
DT	26	29	37	41	27	48
SVM	38	30	39	25	48	37
RF	35	54	53	19	43	32
AdaBoost	27	53	65	48	60	59
XGBoost	46	45	24	31	34	43
MLP	13	42	50	27	30	48

Висновки з даного дослідження і перспективи подальших досліджень у даному напрямку. У представленому дослідженні з використанням набору даних CICIDS2017, автори ознайомились з ефективністю численних моделей ML і DL у виявленні мережевих атак (вторгнень). Результати показали чудову продуктивність на рівні 99,05 класичної моделі ML у вигляді класифікатора DT порівняно з такими підходами, як XGBoost, RF та AdaBoost. Модель Deep MLP, навчена за допомогою оптимізатора Adam, досягла продуктивності на рівні 98,44 при співвідношенні тренувань і тестів як 80:20.

Моделі показали успішну ідентифікацію певних типів атак, таких як Exploits та Generic атаки. Однак, вони зіткнулися з труднощами в точному виявленні таких категорій, як DoS-атаки, Worm, Backdoor та Shellcode. Це вказує на необхідність вдосконалення здатності моделей класифікувати ці конкретні типи атак. Підвищення продуктивносиі моделей у цих категоріях має вирішальне значення для посилення заходів кібербезпеки та забезпечення комплексних можливостей виявлення загроз. Результати досліджень мають важливе значення для захисту критично важливих мереж від кібератак. Виявлення вторгнень у мережах можна покращити, використовуючи моделі ML та DL, а також нових методологій, таких як навчання згорткових нейронних мереж (CNN) безпосередньо на захоплених пакетах мережевого трафіку або візуальних зображеннях. Ці рішення можуть ефективно виявляти як відомі, так і невідомі методи атак, забезпечуючи повний захист від складних кіберзагроз, з якими стикаються мережі. У майбутньому більш складні алгоритми ML можуть бути використані для виявлення кібератак з більшою точністю та ширшим класом кібератак.

Подальші дослідження виявлення вторгнень у мережі повинні бути зосереджені на покращенні стійкості моделі проти складних типів атак, таких як DoS-атаки і Backdoors, за допомогою тестування та розширення бази даних. Інтеграція сукупності цих методів з передовими архітектурами DL, таких як CNN та RNN (рекурентна нейронна мережа), може підвищити точність виявлення. Виявлення вторгнень у режимі реального часу можна покращити, використовуючи фреймворки потокової обробки та периферійні обчислення. Крім того, зрозумілі методи штучного інтелекту забезпечать прозорість і довіру до мереж, що має вирішальне значення для середовищ із високими ризиками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 2021. URL: https://doi.org/10.1016/j.egyr.2021.08.126 (date of access: 03.05.2024).

2. George A. S., George A. H. & Baskar T. Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats. *Partners Universal International Innovation Journal*. 2023. Vol. 1. № 4. P. 155–172. DOI: 10.5281/zenodo.8274514.

3. Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions / N. Moustafa et al. *IEEE Communications Surveys & Tutorials*. 2023. P. 1. URL: https://doi.org/10.1109/comst.2023.3280465 (date of access: 03.05.2024).

4. A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions / J. Asharf et al. *Electronics*. 2020. Vol. 9, no. 7. P. 1177. URL: https://doi.org/10.3390/electronics9071177 (date of access: 03.05.2024).

5. An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks / A. Churcher et al. *Sensors*. 2021. Vol. 21, no. 2. P. 446. URL: https://doi.org/10.3390/s21020446 (date of access: 03.05.2024).

6. Evaluating Deep Learning Based Network Intrusion Detection System in Adversarial Environment / Y. Peng et al. *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Beijing, China, 12–14 July 2019. 2019. URL: https://doi.org/10.1109/iceiec.2019.8784514 (date of access: 03.05.2024).

7. Intrusion Detection and Prevention Systems: An Updated Review / N. A. Azeez et al. *Data Management, Analytics and Innovation*. Singapore, 2019. P. 685–696. URL: https://doi.org/10.1007/978-981-32-9949-8_48 (date of access: 03.05.2024).

8. A Survey of Intrusion Detection Systems Leveraging Host Data / R. A. Bridges et al. *ACM Computing Surveys*. 2020. Vol. 52, no. 6. P. 1–35. URL: https://doi.org/10.1145/3344382 (date of access: 03.05.2024).

9. Parizad A., Hatziadoniu C. Cyber-Attack Detection Using Principal Component Analysis and Noisy Clustering Algorithms: A Collaborative Machine Learning-Based Framework. *IEEE Transactions on Smart Grid*. 2022. Vol. 13, no. 6. P. 4848-4861. URL: https://doi.org/10.1109/tsg.2022.3176311 (date of access: 03.05.2024).

10. Eliyan L. F., Di Pietro R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*. 2021. Vol. 122. P. 149–171. URL: https://doi.org/10.1016/j.future.2021.03.011 (date of access: 03.05.2024).

11. Alghawazi M., Alghazzawi D., Alarifi S. Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*. 2022. Vol. 2, no. 4. P. 764–777. URL: https://doi.org/10.3390/jcp2040039 (date of access: 03.05.2024).

12. SSH and FTP brute-force Attacks Detection in Computer Networks: LSTM and Machine Learning Approaches / M. D. Hossain et al. *2020 5th International Conference on Computer and Communication Systems (ICCCS)*, Shanghai, China, 15–18 May 2020. 2020. URL: https://doi.org/10.1109/icccs49078.2020.9118459 (date of access: 03.05.2024).

13. Thankappan M., Rifà-Pous H., Garrigues C. Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks: A State of the Art Review. *Expert Systems with Applications*. 2022. Vol. 210. P. 118401. URL: https://doi.org/10.1016/j.eswa.2022.118401 (date of access: 03.05.2024).

14. Almulla K. Cyber-attack detection in network traffic using machine learning. 2022. URL: https://repository.rit.edu/cgi/viewcontent.cgi?article=12453&context=theses (date of access: 03.05.2024).

15. Deep Learning Approach for Intelligent Intrusion Detection System / R. Vinayakumar et al. *IEEE Access*. 2019. Vol. 7. P. 41525–41550. URL: https://doi.org/10.1109/access.2019.2895334 (date of access: 03.05.2024).

16. BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset / T. Su et al. *IEEE Access*. 2020. Vol. 8. P. 29575–29585. URL: https://doi.org/10.1109/access.2020.2972627 (date of access: 03.05.2024).

17. Ding Y., Zhai Y. Intrusion Detection System for NSL-KDD Dataset Using Convolutional Neural Networks. *CSAI '18: Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence,* Shenzhen, China, 8–10 December 2018. New York, USA, ACM Press, 2018. P. 81–85. URL: https://doi.org/10.1145/3297156.3297230 (date of access: 03.05.2024).

18. Meena G., Choudhary R. R. A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA. *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, Jaipur, India, 1–2 July 2017. 2017. URL: https://doi.org/10.1109/comptelix.2017.8004032 (date of access: 03.05.2024).

19. Benchmarking datasets for Anomaly-based Network Intrusion Detection: KDD CUP 99 alternatives / A. Divekar et al. *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, Kathmandu, 25–27 October 2018. 2018. URL: https://doi.org/10.1109/cccs.2018.8586840 (date of access: 03.05.2024).

20. A Deep Learning Approach for Network Intrusion Detection Based on NSL-KDD Dataset / C. Zhang et al. *2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, Xiamen, China, 25–27 October 2019. IEEE. P. 41–45. URL: https://doi.org/10.1109/icasid.2019.8925239 (date of access: 04.05.2024).

21. CICIDS2017. URL: https://www.researchgate.net/figure/Description-of-files-containing-CICIDS2017-dataset_tbl1_329045441 (date of access: 04.05.2024).

DOI: 10.58254/viti.6.2024.09.116

УДК 004.056

д-р філософії Марченко В. В. ORCID: 0000-0003-4271-3132 (ДУІКТ)
Чайківський В. В. ORCID: 0009-0001-4257-8893 (ДУІКТ)
Прийма О. О. ORCID: 0009-0008-6991-1773 (ВІТІ ім. Героїв Крут)

МЕТОД ПІДВИЩЕННЯ ОБІЗНАНОСТІ ОСОБОВОГО СКЛАДУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ ПРОГРАМНОГО ЗАСТОСУНКУ GOPHISH

У сучасних умовах кіберпростору, де загрози постійно еволюціонують, особливої уваги потребують фішингові атаки. Вони є одним із найпоширеніших методів соціальної інженерії, що використовуються для отримання доступу до конфіденційної інформації через маніпуляції з користувачами. Такі атаки можуть призвести до витоку даних, фінансових втрат та репутаційних ризиків.

Однією з ключових проблем є недостатня підготовка персоналу до розпізнавання фішингових загроз. Традиційні методи навчання не забезпечують належної інтерактивності та реалістичності, що знижує ефективність підвищення обізнаності. Для вирішення цього питання потрібні нові підходи, які моделюють реальні сценарії кібератак.

Інструмент Gophish дозволяє створювати персоналізовані фішингові кампанії, що імітують реальні атаки та аналізують реакції користувачів. Його функціонал включає створення шаблонів листів, відправку повідомлень та збір даних про взаємодію користувачів. Це дозволяє організаціям виявляти слабкі місця, коригувати навчальні програми та проводити додаткові тренінги.

Результати показують, що використання Gophish підвищує обізнаність персоналу щодо протидії соціальній інженерії. Інтерактивні симуляції сприяють кращому розумінню користувачами фішингових загроз та допомагають їм вчасно розпізнати небезпеку. Завдяки зібраній аналітиці керівництво може оперативно впроваджувати коригувальні заходи.

Розвиток штучного інтелекту та машинного навчання відкриває нові можливості для вдосконалення таких інструментів. Майбутні рішення зможуть адаптувати симуляції під конкретних користувачів, що зробить навчання ще ефективнішим.

Ключові слова: *фішинг, соціальна інженерія, підвищення обізнаності, Gophish, коригувальні дії, фішингові листи, симуляція.*

V. Marchenko, V. Chaikivskyi, O. Pryima Method for raising personnel awareness of information security using the Gophish software application

In today's cyberspace, where threats are constantly evolving, phishing attacks require special attention. They are one of the most common social engineering methods used to gain access to confidential information by manipulating users. Such attacks can lead to data breaches, financial losses, and reputational risks.

One of the key problems is the lack of staff training in recognizing phishing threats. Traditional training methods do not provide adequate interactivity and realism, which reduces the effectiveness of awareness raising. To address this issue, new approaches are needed that model real-life cyberattack scenarios.

The Gophish tool allows you to create personalized phishing campaigns that simulate real attacks and analyze user reactions. Its functionality includes creating email templates, sending messages, and collecting data on user interaction. This allows organizations to identify weaknesses, adjust training programs, and conduct additional training.

The results show that using Gophish increases staff awareness of social engineering. Interactive simulations contribute to a better understanding of phishing threats and help users recognize the danger in time. Thanks to the analytics collected, management can quickly implement corrective measures.

The development of artificial intelligence and machine learning opens up new opportunities for improving such tools. Future solutions will be able to adapt simulations to specific users, making training even more effective.

Keywords: *phishing, social engineering, awareness raising, Gophish, corrective actions, phishing emails, simulation.*

Вступ

Фішинг є однією з найпоширеніших форм соціальної інженерії, яка використовується зловмисниками для розсилання шахрайських електронних листів з метою впливу на користувачів. Вони намагаються змусити жертву надати чутливу інформацію, відкрити шкідливий файл або перейти за посиланням, що веде на підроблений вебсайт. Основна ціль

фішингових атак – це людський фактор, оскільки вони спрямовані на обман працівників та інших осіб, які мають доступ до інформаційних систем організації.

Такі атаки завдають значної шкоди як індивідуальним користувачам, так і великим організаціям, тому ефективне навчання персоналу є одним із ключових заходів для протидії різним методам соціальної інженерії. Проте наявні інструменти для емуляції фішингових атак мають обмежену функціональність, і їх можливості часто не відповідають вимогам сучасних сценаріїв загроз. Це створює потребу у розробці та впровадженні більш ефективних рішень, які дозволять проводити реалістичні симуляції та підвищити обізнаність користувачів. У довгостроковій перспективі такі підходи сприятимуть зниженню ризиків, пов'язаних з фішингом та іншими методами соціальної інженерії.

Згідно з рекомендаціями Національного інституту стандартів і технологій (NIST) у фреймворку NIST CSF 2.0, підвищення обізнаності персоналу щодо інформаційної безпеки має здійснюватися на регулярній основі. Навчання повинно охоплювати не лише основний персонал, а й сторонніх підрядників, які мають доступ до інформаційних систем організації [1]. Це є важливим аспектом стратегії інформаційної безпеки, оскільки людський фактор залишається однією з найвразливіших точок у захисті даних.

Аналіз фішингових атак, проведений аналітиками Оперативного центру реагування на кіберінциденти у IV кварталі 2023 року, показав, що з 1731 зафіксованої атаки 472 мали на меті поширення шкідливих вкладень [2]. Це підтверджує, що фішинг активно використовується для розповсюдження шкідливого програмного забезпечення, який створює додаткові ризики для організацій. Відповідно до доповіді Symantec Internet Security Threat Report (ISTR), навіть невелика частка всього URL-трафіку, а саме 0,5%, є фішинговою, але її вплив на загальну безпеку залишається значним [3].

Таким чином, зростаючий рівень загроз від фішингових атак вимагає впровадження нових методів та інструментів для підвищення обізнаності користувачів. У даній статті розглядаються існуючі підходи, аналізується їх ефективність, а також пропонуються рішення, які можуть підвищити рівень підготовки персоналу та знизити ризики, пов'язані з фішинговими атаками.

Постановка проблеми. У сучасних умовах швидких змін та зростаючих загроз у кіберпросторі організаціям складно встигати за стрімкими темпами розвитку кібератак. Хоча спільнотою розроблено численні рекомендації та інструменти для підвищення рівня інформаційної безпеки, багато з них потребують адаптації під конкретні потреби організацій. У цьому мінливому середовищі особливу увагу варто приділяти людському фактору, який залишається найслабшою ланкою в системах інформаційної та кібербезпеки.

Задля зменшення ризиків організаціям рекомендовано регулярно проводити заходи з підвищення обізнаності кінцевих користувачів. Проте теоретичні знання не забезпечують належного рівня підготовки для протидії фішинговим атакам. Для цього необхідні практичні симуляції, які максимально наближають користувачів до реальних сценаріїв кібератак, що дозволяє співробітникам краще усвідомити потенційні ризики для себе та організації через неуважність або необачність.

Як правило, організації залучають зовнішніх спеціалістів для проведення таких навчань, що призводить до додаткових фінансових витрат. У зв'язку з цим виникає потреба у впровадженні внутрішніх навчальних програм, які не лише зменшать витрати, а й дозволять створювати симуляції, максимально наближені до реальних фішингових атак. Одним із таких рішень є використання інструменту Gophish, який надає можливість створення персоналізованих фішингових кампаній, аналізу реакції користувачів та визначення їх вразливих місць.

Аналіз останніх публікацій. Наукові дослідження, щодо фішингу та соціальної інженерії, підкреслюють актуальність загроз, які виникають у зв'язку з людським фактором.

Фішингові атаки залишаються одним з найпоширеніших методів соціальної інженерії, що використовуються для отримання несанкціонованого доступу до конфіденційної інформації шляхом маніпуляцій з користувачами. Перехід на дистанційну або гібридну форму роботи після пандемії COVID-19 спричинив значне зростання кількості фішингових атак, що пов’язано з більшою активністю користувачів у цифровому середовищі та їх підвищеною вразливістю до такого роду атак [4].

Результати дослідження 2023 року, проведеного компанією SlashNext, свідчать про зростаюче занепокоєння серед фахівців з кібербезпеки стосовно атак типу Business Email Compromise (BEC). У звіті вказується, що 46 % опитаних відповідальних осіб з кібербезпеки відзначили зростання кількості атак BEC на співробітників їхніх організацій. Це явище пояснюється доступністю сучасних чат-ботів на базі штучного інтелекту, які значно підвищують ефективність і масштабованість фішингових атак, що робить їх більш переконливими та складними для виявлення [5].

Аналіз публікацій також вказує на те, що електронна пошта залишається основним інструментом для здійснення фішингових атак. Згідно зі звітом IBM Security X-Force, понад 90 % успішних атак у 2023 році розпочинались саме з фішингових електронних листів. Це підтверджує значущість даного вектору загроз і необхідність приділення особливої уваги його мінімізації [6].

Дослідження, опубліковане у "Journal of Cyber Security", акцентує на зростанні ефективності фішингових кампаній завдяки впровадженню методів штучного інтелекту, які дозволяють створювати більш правдоподібні та персоналізовані атаки. Використання алгоритмів машинного навчання для аналізу поведінкових характеристик користувачів забезпечує можливість формування повідомлень, які виглядають надзвичайно переконливо, що підвищує ймовірність успішного здійснення фішингових атак [7].

Таким чином, підвищення складності та варіативності фішингових атак зумовлює необхідність впровадження комплексних рішень, які включають програмно-апаратні засоби для виявлення та блокування підозрілих електронних листів. Крім того, важливим елементом стратегії кібербезпеки залишається регулярне підвищення обізнаності співробітників, оскільки саме людський фактор продовжує залишатись найвразливішим компонентом у системах інформаційної безпеки.

Метою статті є обґрунтування та розробка методу підвищення обізнаності особового складу з інформаційної безпеки щодо готовності протидіяти соціальній інженерії, зокрема фішингу, із застосуванням програмного забезпечення Gophish.

Виклад основного матеріалу дослідження

Програмне забезпечення Gophish має відкритий вихідний код, репозиторій якого розміщено на платформі GitHub. Інструмент розроблено мовою програмування Go, а за замовчуванням він використовує базу даних SQLite, хоча є можливість підключення до MySQL при необхідності. Gophish немає вбудованого SMTP-сервера, тому для надсилання фішингових електронних листів необхідно використовувати зовнішні SMTP-рішення [8].

Інструмент характеризується зручним та інтуїтивно зрозумілим вебінтерфейсом, що полегшує налаштування та управління фішинговими кампаніями. Gophish дозволяє створювати шаблони електронних листів і фішингові вебсайти, а також збирати та візуалізувати дані щодо реакцій користувачів, зокрема відкриття листів, переходи за посиланнями та введення даних. Отримані аналітичні дані надають можливість організаціям оцінити рівень обізнаності персоналу з питань кібербезпеки та ідентифікувати найбільш вразливі аспекти їхньої поведінки.

Для кращого розуміння принципу роботи фішингових атак, наведено загальну концептуальну схему (рис. 1), що описує стандартний процес фішингової атаки через електронну пошту.

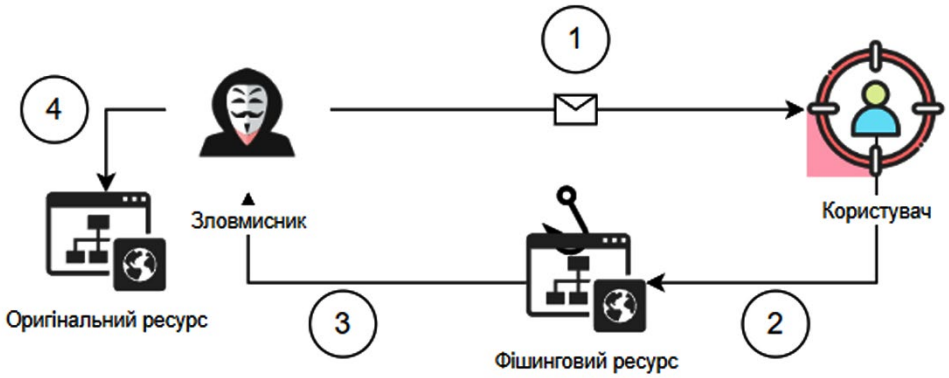


Рис. 1. Концептуальна схема фішингу

1. Зловмисник надсилає фішинговий електронний лист, маскуючи його під легітимне повідомлення (наприклад, від технічної підтримки або офіційної установи), щоб отримати від користувача чутливі дані.

2. Користувач відкриває електронний лист і взаємодіє з вкладенням або переходить за посиланням, яке веде на підроблений вебсайт.

3. На фейковому вебсайті користувач вводить свої облікові дані (логін і пароль), які стають доступними зловмиснику.

4. Зловмисник може використати отримані облікові дані для несанкціонованого доступу до оригінальних вебресурсів або зберегти їх для ініціалізації подальших атак.

Для ефективного підвищення обізнаності персоналу за допомогою Gophish необхідно встановити та налаштувати програму на внутрішньому сервері організації або в хмарному середовищі. Завдяки відкритому вихідному коду інструмент доступний для завантаження з офіційного порталу. Після інсталяції відповідальні особи можуть адаптувати Gophish для проведення реалістичних симуляцій фішингу, використовуючи можливості інструменту з копіювання інтерфейсу вебресурсів (рис. 2), що дозволяє створювати симуляції, які максимально наближені до реальних атак, на прикладі соціальних мереж.

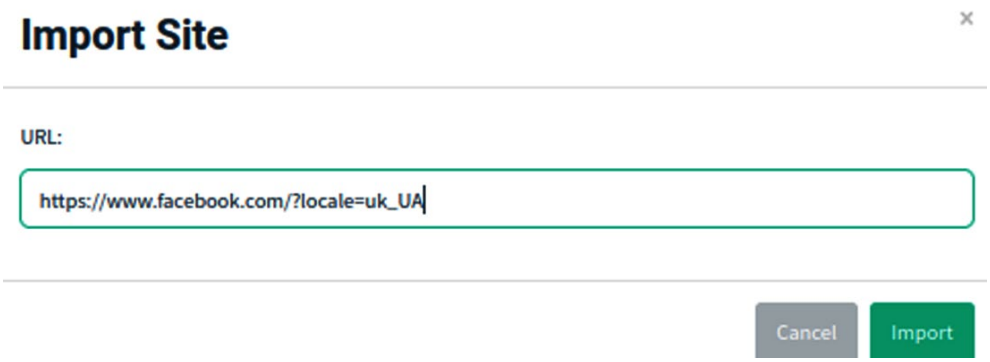


Рис. 2. Функціонал для копіювання вебресурсів

Головною метою фішингових атак є отримання чутливих даних користувача, таких як логін та пароль. Для реалізації цієї цілі в контексті підвищення обізнаності персоналу за допомогою Gophish використовуються функції «Capture Submitted Data» та «Capture Passwords» (рис. 3). Цей функціонал дозволяє фіксувати введені користувачами дані, що, у свою чергу, створює можливість для формування статистики, яка використовується для оцінки рівня обізнаності співробітників щодо фішингових загроз.

Для забезпечення максимально реалістичної симуляції та зниження ймовірності її виявлення користувачем рекомендується налаштувати автоматичне перенаправлення на

оригінальну вебсторінку після того, як користувач введе свої дані на підробленому ресурсі. Такий підхід знижує ризик виникнення підозр у користувача та зберігає природність процесу, що дозволяє отримати більш точні та достовірні результати під час проведення фішингових симуляцій.

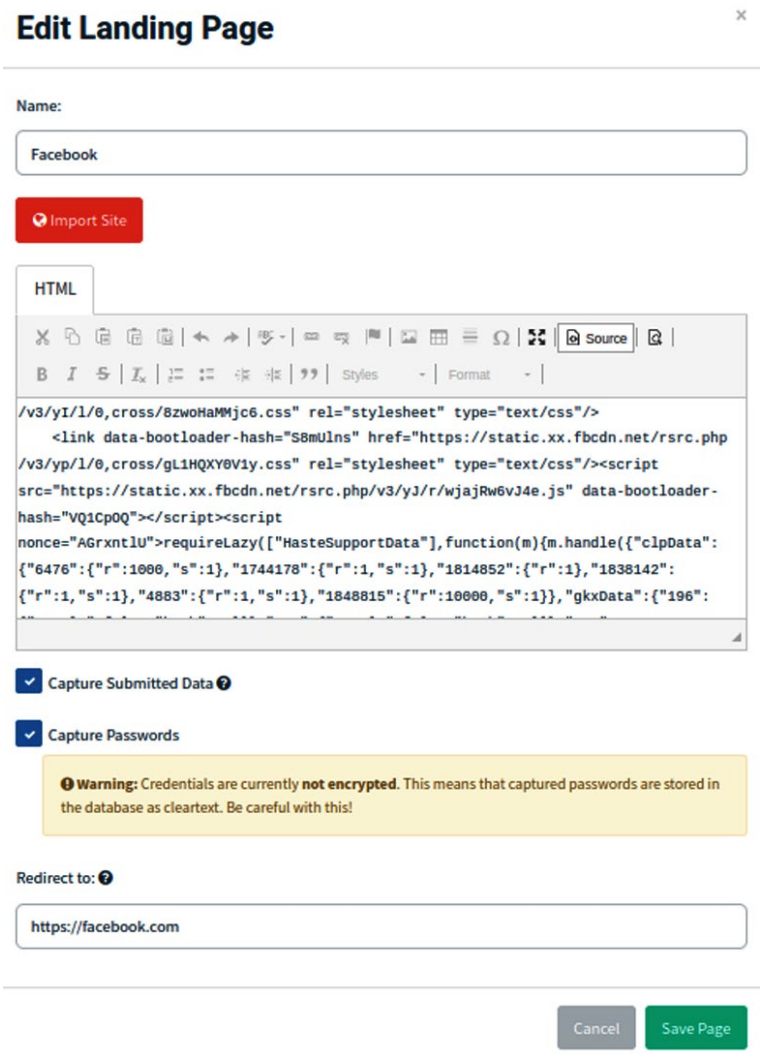


Рис. 3. Розширені функціональні можливості

Наступним ключовим етапом є налаштування шаблонів електронних листів, які будуть розсилатися співробітникам у рамках симуляцій фішингових атак. Gophish надає можливість створювати власні шаблони фішингових листів, але для досягнення максимальної ефективності ці шаблони необхідно зробити максимально схожими на легітимні повідомлення (рис. 4).

Інструмент має функцію «Import Email», яка дозволяє імпортувати електронні листи з легітимних ресурсів, адаптуючи їх до потреб конкретної організації (рис. 5). Ця можливість спрощує процес створення правдоподібних повідомлень, знижуючи час і зусилля, необхідні для розробки шаблонів. Водночас, відповідальні за навчання особи можуть створювати шаблони вручну, налаштовуючи їх під специфічні сценарії, наприклад, повідомлення щодо оновлення програмного забезпечення, зміну паролю у соціальних мережах чи корпоративних системах.

Ключовим аспектом налаштування є переконливість шаблонів. Вони повинні виглядати достатньо реалістично, щоб користувачі не могли легко відрізнити їх від справжніх

повідомлень. Це сприятиме більш природній реакції на фішингові симуляції та забезпечить отримання достовірніших результатів для подальшого аналізу та вдосконалення навчальних програм.

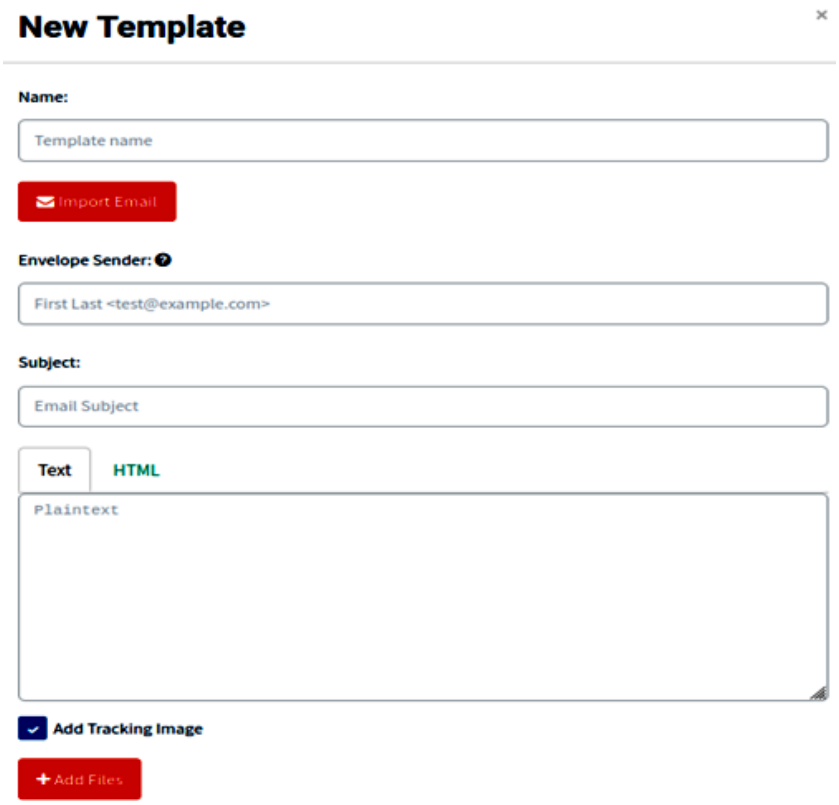


Рис. 4. Діалогове вікно створення нового шаблону

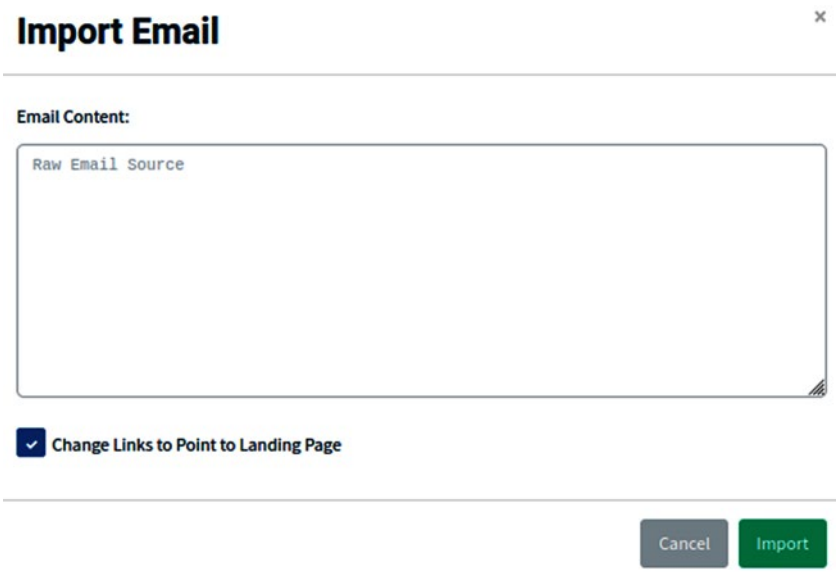


Рис. 5. Діалогове вікно з можливістю копіювання легітимного листа

Важливим елементом, що дозволяє впроваджувати коригувальні дії після проведення практичних навчань з фішинговими симуляціями, є моніторинг показників та формування звітності (рис. 6). Відповідно до рекомендацій компанії Terranova Security, яка спеціалізується на навчанні співробітників з питань кібербезпеки, відстеження таких показників, як відкриття

електронних листів, завантаження вкладень, розкриття облікової інформації та загальна кількість кліків під час фішингових симуляцій, є основою для складання звітів. Ці звіти містять інформацію про кількість користувачів, які стали жертвами фішингових атак, а також про те, скільки співробітників повідомили про підозрілу активність [9].

Інструмент Gophish забезпечує можливість детального аналізу поведінки кожного користувача, залученого до фішингових тестувань. Серед показників, які відстежуються під час кампаній, можна виділити:

час відкриття електронного листа: дозволяє отримати інформацію про те, коли користувач відкрив фішингове повідомлення, що може свідчити про швидкість його реакції на подібні повідомлення;

час і дата відкриття посилання: допомагає визначити, наскільки швидко користувачі реагують на фішингові атаки, переходячи за підозрілими посиланнями;

введення облікових даних: фіксується, чи ввів користувач свої облікові дані на підробленій вебсторінці, що дозволяє оцінити реальний ризик витоку інформації.

Такий детальний аналіз допомагає організаціям ідентифікувати слабкі місця в поведінці співробітників і розробляти подальші навчальні програми, спрямовані на підвищення рівня обізнаності та готовності до протидії фішинговим атакам. Звітність також сприяє оцінці загальної ефективності проведених симуляцій та дозволяє оперативно вживати заходів для усунення виявлених проблем.

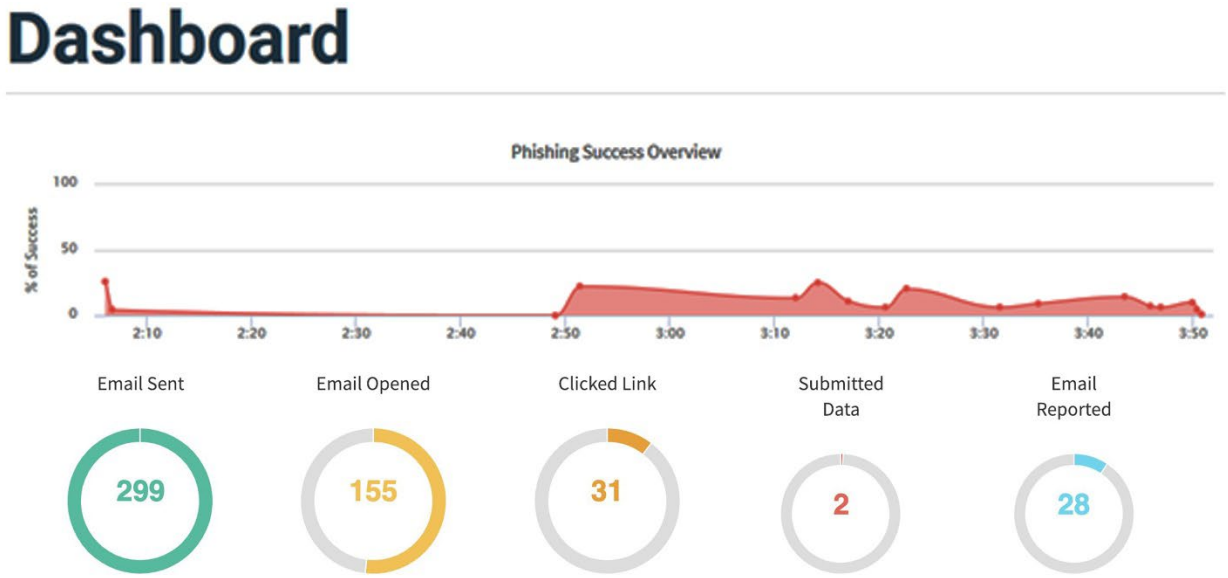


Рис. 6. Візуалізація результатів фішингової кампанії Gophish

Варто підкреслити, що проведення заходів із практичного тестування користувачів, зокрема симуляцій фішингових атак, є ключовим елементом для оцінки рівня обізнаності персоналу щодо кіберзагроз. Такий вид тестувань дозволяє реально оцінити, наскільки співробітники готові виявляти та ефективно протидіяти атакам соціальної інженерії в умовах, максимально наближених до реальних. Проте самих лише тестувань недостатньо для підтримки високого рівня інформаційної безпеки в організаціях. Важливо не тільки виявити слабкі місця, але й впроваджувати коригувальні дії на основі отриманих результатів.

Одним із ключових коригувальних заходів є регулярне навчання співробітників, яке охоплює як звичайних працівників, так і керівний склад. Воно має включати роз'яснення потенційних наслідків успішних кібератак, що дозволяє співробітникам краще усвідомлювати серйозність можливих загроз (рис. 7). Практичні тестування допомагають ідентифікувати тих

співробітників, які потребують додаткового навчання, та дозволяють керівництву адаптувати навчальні програми відповідно до потреб організації.

Порівняння результатів до і після проведення навчальних заходів дає розуміння на скільки знизилась вразливість компанії до фішингових атак. Наприклад, якщо до навчання 40 % користувачів вводили дані на фейкових сайтах, а після – лише 10 %, це свідчить про 75 % зниження вразливості, що можна обчислити за формулою:

$$\Delta P = \frac{P_{before} - P_{after}}{P_{before}} \times 100\%,$$

де ΔP – зниження рівня вразливості персоналу до фішингових атак (відсоток зменшення вразливості);

P_{before} – кількість користувачів, які піддалися фішинговій атаці до навчання (до проведення тренінгів);

P_{after} – кількість користувачів, які піддалися фішинговій атаці після навчання (після проведення тренінгів).

Такі показники демонструють значне підвищення обізнаності та рівня кібергігієни серед працівників. Також, завдяки використанню Gophish, вдається оптимізувати витрати на зовнішні послуги, оскільки інструмент дозволяє проводити навчання внутрішніми ресурсами організації. Це підтверджується розрахунками рентабельності інвестицій (Return On Investment):

$$ROI = \frac{B - C}{C} \times 100\%,$$

де ROI – рентабельність інвестицій у навчання;

B (Benefits) – сума потенційно зекономлених коштів від зменшення кількості інцидентів;

C (Costs) – загальна вартість проведення навчання (інвестиції у тренінги та навчальні програми).

Для аналізу швидкості реакції користувачів на фішингові атаки важливим показником є середній час відкриття листа:

$$T_{avg} = \frac{\sum T_{open}}{N},$$

де T_{avg} – середній час реакції користувачів;

$\sum T_{open}$ – сума часу між моментом відкриття листа і здійсненням першої дії користувачами (наприклад, кліком на посилання або закриття листа);

N – загальна кількість користувачів, які отримали фішинговий лист.

Після навчання цей час реакції користувачів може зрости, що буде свідчити про обережніше ставлення до електронних повідомлень.

Таким чином, комплексний підхід, що поєднує регулярні симуляції та постійне навчання, сприяє підвищенню загального рівня обізнаності в організації, дозволяє зменшити ризики, пов'язані з фішинговими атаками, і формує культуру інформаційної безпеки.

Процес формування та впровадження програм навчання має базуватися на результатах попередніх тестувань, що дозволяє адаптувати підхід до конкретних потреб організації та виявлених вразливостей. Навчальні заходи можуть включати спеціалізовані зовнішні програми для певних груп співробітників, які мають доступ до критичних даних та систем. Крім того, рекомендується регулярно проводити загальні тренінги, які організовує внутрішній підрозділ інформаційної безпеки для всіх працівників, з метою підвищення загального рівня обізнаності щодо базових принципів кібергігієни [10].

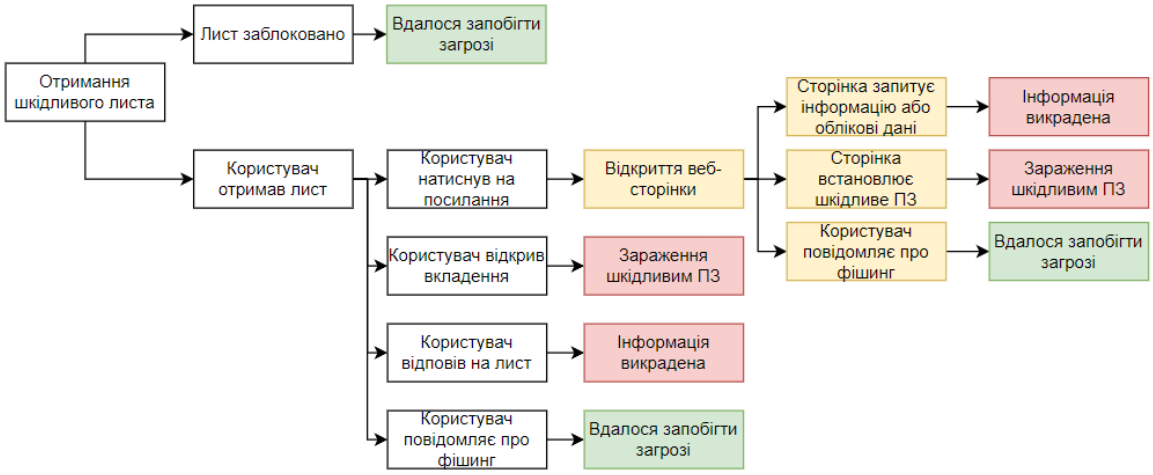


Рис. 7. Поширені шляхи фішингових атак на електронну пошту [9]

Відповідно до міжнародних стандартів, зокрема ISO/IEC 27002, підвищення рівня обізнаності співробітників має бути постійним і регулярним процесом [11]. Для цього доцільно використовувати цикл Шухарта-Демінга (PDCA), що забезпечує безперервний розвиток та вдосконалення навчальних програм (рис. 8).

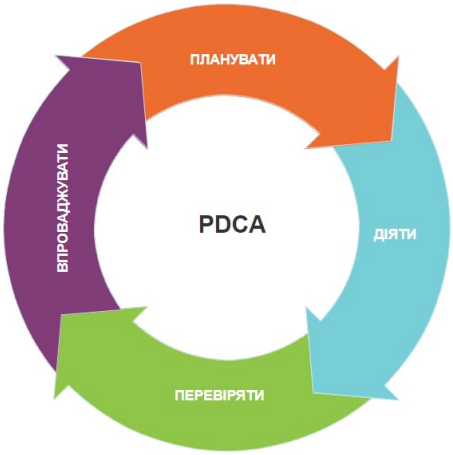


Рис. 8. Цикл Шухарта-Демінга

У контексті використання Gophish, процес підвищення обізнаності персоналу органічно поєднується з принципами циклу PDCA:

планувати (Plan) – визначення потреби у проведенні навчань, враховуючи сучасні тенденції атак, що базуються на методах соціальної інженерії. На цьому етапі аналізується, які вразливості виявлено під час попередніх тестувань, та формуються відповідні навчальні сценарії;

діяти (Do) – реалізація розроблених навчальних програм за допомогою Gophish, що дозволяє організувати симуляції фішингових атак. Під час цього етапу користувачі проходять практичне тестування в умовах, наближених до реальних кібератак;

перевіряти (Check) – аналіз результатів симуляцій, зокрема, оцінка показників взаємодії користувачів з фішинговими листами, часу реакції, частоти введення даних на фейкових ресурсах. Це дозволяє оцінити ефективність проведених заходів;

впроваджувати (Act) – на основі отриманих результатів розробляються плани коригувальних дій, що включають проведення додаткових внутрішніх або зовнішніх навчань

для тих, хто виявився менш підготовленим. Визначаються напрямки подальшого вдосконалення рівня кібергігієни організації.

Таким чином, використання циклу PDCA дозволяє створити структуру навчання, що сприяє постійному розвитку навичок співробітників та підвищує загальний рівень інформаційної безпеки в організації.

На додаток до Gophish, доцільно розглянути Phishing Quiz від Google – безкоштовний інтерактивний онлайн-інструмент, призначений для навчання користувачів розпізнавати фішингові атаки. Цей сервіс імітує реалістичні сценарії електронних листів, дозволяючи користувачам відпрацьовувати навички виявлення загроз без необхідності попереднього технічного налаштування [12].

Перевага Phishing Quiz полягає в простоті використання: достатньо мати доступ до інтернету, що робить його зручним для організацій без значних технічних ресурсів. На відміну від Gophish, який потребує розгортання на внутрішніх серверах або в хмарі, а також технічних знань для налаштування, Phishing Quiz не вимагає додаткових інвестицій і може бути швидко інтегрований у процес навчання.

Однак, функціональні можливості Phishing Quiz є обмеженими, оскільки він не підтримує масштабні кампанії з детальним аналізом поведінки користувачів. Водночас Gophish надає інструменти для комплексного навчання з можливістю збору статистики та подальшого вдосконалення програм безпеки.

Висновки і перспективи подальших досліджень

Відповідно до представленої інформації, метод підвищення обізнаності персоналу є важливим елементом загальної стратегії кібербезпеки, оскільки людський фактор залишається однією з найвразливіших ланок захисту. Практичні тренінги та симуляції, зокрема за допомогою Gophish, дозволяють ознайомити співробітників з реалістичними сценаріями, що імітують дії зловмисників, тим самим підвищуючи їхню готовність до виявлення фішингових атак.

Наукові дослідження свідчать, що симуляції, які відтворюють реальні фішингові сценарії, дозволяють співробітникам краще розпізнавати ознаки шахрайства в майбутньому, оскільки вони створюють умови для активного навчання. Це важливо, оскільки активні методи навчання, які включають практичний досвід, значно перевершують пасивні методи (лекції, брошури) за ефективністю запам’ятовування і застосування знань у реальних умовах. Зокрема, дослідження показують, що після практичних тренінгів зростає рівень обізнаності співробітників щодо фішингових загроз, що значно знижує кількість успішних атак.

Розглянутий метод, заснований на використанні Gophish, є ефективним інструментом для підвищення рівня обізнаності завдяки його функціональних можливостей:

Персоналізовані фішингові кампанії: Gophish дозволяє створювати сценарії, які максимально наближені до реальних атак, з урахуванням специфіки діяльності організації та її співробітників. Це забезпечує кращу підготовку користувачів до виявлення фішингу, оскільки вони стикаються з прикладами, подібними до тих, які можуть зустрітися у їхній повсякденній роботі.

Відстеження реакцій користувачів у реальному часі: завдяки можливості моніторингу дій співробітників під час симуляцій, керівництво може ідентифікувати слабкі місця та визначити, які аспекти безпеки потребують додаткового навчання. Це дозволяє адаптувати підходи до навчання і зосередити увагу на найбільш критичних питаннях.

Зручна візуалізація результатів: Gophish надає звіти, які включають детальну аналітику щодо дій користувачів (відкриття листів, кліки на посилання, введення облікових даних). Це дозволяє ефективно оцінювати результати тренінгів і визначати подальші коригувальні дії, що підвищує загальну кібергігієну в організації.

Завдяки цим функціям метод, заснований на використанні Gophish, не тільки навчає співробітників розпізнавати фішингові атаки, але й забезпечує інтерактивний підхід до навчання, який підвищує ефективність запам’ятовування інформації та практичного застосування навичок. Відповідно, це дозволяє організаціям вчасно реагувати на виявлені слабкі місця та адаптувати свою стратегію кібербезпеки до нових викликів, що постійно з’являються в динамічному кіберпросторі.

Подальші дослідження будуть спрямовані на вдосконалення існуючих методів підвищення обізнаності шляхом інтеграції технологій штучного інтелекту та машинного навчання. Це відкриває можливості для розробки адаптивних симуляцій, які зможуть підлаштовуватися під індивідуальні особливості користувачів, що зробить процес навчання більш ефективним та персоналізованим. Враховуючи динамічний розвиток кіберпростору, де методи атак постійно еволюціонують, такі інноваційні підходи забезпечать організаціям необхідну гнучкість у протидії новим загрозам та дозволять вчасно адаптувати стратегії кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The NIST Cybersecurity Framework (CSF) 2.0. *National Institute of Standards and Technology*. URL: https://doi.org/10.6028/NIST.CSWP.29 (date of access: 08.10.2024).

2. Звіт за четвертий квартал 2023. *Державний центр кіберзахисту Державної служби спеціального зв’язку та захисту інформації України*. URL: https://scpc.gov.ua/uk/articles/341 (дата звернення: 08.10.2024).

3. Gray J. Practical Social Engineering: A Primer for the Ethical Hacker. San Francisco: No Starch Press, 2022. 240 p.

4. Phishing Attacks in Social Engineering: A Review / K. Sarpong Adu-Manu et al. *Journal of Cyber Security*. 2023. P. 1–29. URL: https://doi.org/10.32604/jcs.2023.041095 (date of access: 08.10.2024).

5. The State of Phishing 2023. Slashnext. URL: https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf (date of access: 08.10.2024).

6. IBM Security X-Force Threat Intelligence Index 2023. URL: https://www.ibm.com/security/services/ (date of access: 08.10.2024).

7. Advances in AI-based Phishing Detection and Prevention: A Review / R. Singh, A. Sharma. Journal of Cyber Security and Privacy, 2023. P. 32–45. URL: https://doi.org/10.3390/cybersecurity-2023-01234 (date of access: 08.10.2024).

8. Gophish – Open Source Phishing Framework. *Gophish*. URL: https://getgophish.com/ (date of access: 08.10.2024).

9. Why Is Phishing Awareness Training Important? *Terranova Security | Partner of Choice in Security Awareness*. URL: https://www.terranovasecurity.com/blog/why-is-phishing-training-so-important (date of access: 08.10.2024).

10. Enhancing Cybersecurity Through Phishing Simulation Training. Journal of Information Security & Privacy, Rouse, M., & Field, R. (date of access: 08.10.2024).

11. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2017, IDT; ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015, IDT).

12. Can you spot when you’re being phished? *Jigsaw | Google*. URL: https://phishingquiz.withgoogle.com/?hl=en (date of access: 08.10.2024).

DOI: 10.58254/viti.6.2024.10.127

УДК 621.391; 621.1.039

д-р техн. наук, професор Міночкін А. І. ORCID: 0000-0001-5723-5052 (ВІТІ ім. Героїв Крут)
Бригадир С. П ORCID: 0000-0003-1977-552X (ВІТІ ім. Героїв Крут)

АНАЛІЗ РОЗВИТКУ МЕРЕЖ ЗВ'ЯЗКУ П'ЯТОГО ПОКОЛІННЯ

Стаття присвячена комплексному аналізу ключових аспектів розвитку мереж зв'язку п'ятого покоління (5G) в Україні. Досліджено актуальні проблеми та перспективи впровадження 5G, враховуючи технологічні, економічні та регуляторні аспекти. Запропоновано математичні моделі та алгоритми для оптимізації розподілу радіочастотного спектра, розміщення базових станцій, впровадження віртуалізації мережевих функцій Network Function Virtualization (NFV) та програмно-конфігурованих мереж Software-Defined Networking (SDN), а також забезпечення якості обслуговування (QoS) для різних класів трафіку.

Розроблені рішення дозволяють підвищити ефективність розгортання та експлуатації 5G мереж в умовах обмежених ресурсів. Розроблено математичну модель оптимізації розподілу спектра з використанням лінійного програмування, яка враховує ефективність використання спектра різними операторами. Для оптимізації розміщення базових станцій запропоновано підхід на основі теорії ігор, що враховує обмеження на пропускну здатність та витрати на розміщення при забезпеченні необхідного покриття. Представлено математичну модель для оптимізації розміщення віртуалізованих мережевих функцій на серверах з обмеженими ресурсами з метою мінімізації витрат та забезпечення необхідної продуктивності. Запропоновано алгоритм на основі градієнтного спуску для динамічного управління ресурсами та забезпечення QoS.

На основі порівняльного аналізу методів оптимізації розроблено інтегрований підхід до вирішення ключових задач впровадження 5G. Запропоновано математичну модель оптимізації розподілу радіочастотного спектра на основі лінійного програмування, яка забезпечує підвищення спектральної ефективності на 23–27 % порівняно з базовими методами. Представлено теоретико-ігровий підхід до оптимізації розміщення базових станцій, що дозволяє знизити кількість перевантажених секторів на 45 % та підвищити енергоефективність на 13,3 %. Розроблено генетичний алгоритм оптимізації розміщення віртуалізованих мережевих функцій (VNF), який забезпечує на 21,4 % вищу утилізацію ресурсів. Експериментальні дослідження підтвердили, що запропоновані рішення дозволяють досягти загального підвищення ефективності мережі на 20–25 % при зниженні експлуатаційних витрат на 15–20 %. Результати створюють методологічну основу для ефективного планування та розгортання мереж 5G в Україні

Ключові слова: *5G, оптимізація мереж, радіочастотний спектр, базові станції, віртуалізація мережевих функцій, теорія ігор, лінійне програмування, генетичні алгоритми, енергоефективність, якість обслуговування.*

A. Minochkin, S. Brigadier Analysis of development of fifth generation communication networks

The article is devoted to a comprehensive analysis of key aspects of the development of fifth-generation (5G) networks in Ukraine. Current problems and prospects for the implementation of 5G are studied, taking into account technological, economic and regulatory aspects. Mathematical models and algorithms are proposed for optimizing the allocation of radio frequency spectrum, placement of base stations, implementation of virtualization of network functions Network Function Virtualization (NFV) and software-configured networks Software-Defined Networking (SDN), as well as ensuring quality of service (QoS) for different classes of traffic.

The developed solutions allow to increase the efficiency of deployment and operation of 5G networks in conditions of limited resources. A mathematical model of spectrum allocation optimization using linear programming has been developed, which takes into account the efficiency of spectrum use by different operators. To optimize the placement of base stations, an approach based on game theory is proposed, which takes into account bandwidth limitations and placement costs while ensuring the necessary coverage. A mathematical model is presented for optimizing the placement of virtualized network functions on servers with limited resources in order to minimize costs and ensure the required performance. An algorithm based on gradient descent for dynamic resource management and QoS is proposed.

Based on a comparative analysis of optimization methods, an integrated approach to solving key problems of 5G implementation is developed. A mathematical model for optimizing the allocation of radio frequency spectrum based on linear programming is proposed, which provides an increase in spectral efficiency by 23–27 % compared to basic methods. A game-theoretic approach to optimizing the placement of base stations is presented, which allows reducing the number of overloaded sectors by 45 % and increasing energy efficiency by 13.3 %. A genetic algorithm for optimizing the placement of virtualized network functions (VNF) is developed, which provides a 21.4 % higher resource utilization. Experimental studies have confirmed that the proposed solutions allow achieving an overall increase in network efficiency by 20–25 % while reducing operating costs by 15–20 %. The results create a methodological basis for effective planning and deployment of 5G networks in Ukraine.

Keywords: *5G, network optimization, radio frequency spectrum, base stations, network function virtualization, game theory, linear programming, genetic algorithms, energy efficiency, quality of service.*

Постановка наукової задачі. Мережі зв’язку п’ятого покоління (5G) являють собою новий етап еволюції мобільного зв’язку, що забезпечує значне підвищення швидкості передачі даних, зменшення затримки, збільшення пропускної спроможності та кількості абонентів в мережі. Технологія 5G відкриває широкі можливості для розвитку Інтернету речей (IoT), автономного транспорту, розумних міст, промислової автоматизації та багатьох інших інновацій.

Впровадження мереж 5G є складним технологічним викликом, що вимагає вирішення цілого комплексу наукових та інженерних задач. Це включає розробку нових методів модуляції та кодування сигналів, ефективних алгоритмів управління радіоресурсами, архітектурних рішень для програмно-конфігурованих мереж та віртуалізації мережевих функцій, а також забезпечення інформаційної безпеки та електромагнітної сумісності.

Особливу актуальність дослідження та розвиток технологій 5G мають для України, де існує нагальна потреба в модернізації телекомунікаційної інфраструктури та створенні умов для цифрової трансформації економіки. Впровадження мереж нового покоління дозволить підвищити конкурентоспроможність країни на світовому ринку, стимулювати інновації та створити нові робочі місця в сфері високих технологій.

Таким чином стаття присвячена комплексному аналізу ключових аспектів розвитку мереж зв’язку п’ятого покоління, включаючи технологічні, економічні та регуляторні питання. Особлива увага приділяється дослідженню специфіки та перспектив впровадження 5G в Україні з урахуванням існуючих обмежень.

Наукова задача дослідження полягає у розробці теоретичних основ та практичних рекомендацій щодо ефективного впровадження та розвитку мереж зв’язку п’ятого покоління в Україні.

Для досягнення поставленої мети необхідно вирішити ряд наступних часткових задач:

1. Провести системний аналіз сучасного стану та перспектив розвитку технологій 5G у світі та Україні;

2. Розробити математичні моделі алгоритмів оптимізації радіопокриття та управління ресурсами мереж 5G в умовах щільної міської забудови;

3. Розробити науково обґрунтовані рекомендації щодо впровадження технологій мереж зв’язку п’ятого покоління.

Вирішення поставленої наукової задачі дозволить створити теоретичне підґрунтя та практичний інструментарій для ефективного впровадження мереж зв’язку п’ятого покоління в Україні.

Аналіз останніх публікацій. Дослідженню різних аспектів розвитку мереж п’ятого покоління присвячена значна кількість наукових праць.

Так фундаментальні принципи архітектури 5G та ключові технології детально розглянуто в роботах M. Shafi [1], E. Dahlman [2], A. Osseiran [3]. Зокрема, в [1] представлено комплексний огляд архітектури 5G, включаючи нові концепції радіоінтерфейсу, віртуалізації мережевих функцій та програмно-конфігурованих мереж. Однак у вищезазначених наукових роботах недостатньо уваги приділено питанням сумісності з існуючими мережами минулих поколінь. Автори у [2] детально аналізують технології радіодоступу 5G New Radio, але обмежуються переважно теоретичними абстрактними аспектами без достатнього детального опису математичних моделей. В роботі [3] основна увага приділяється сценаріям використання 5G, однак в математичній моделі не враховано кількісних оцінок якості обслуговування для різних додатків.

Задачі планування та оптимізації радіопокриття мереж 5G досліджуються в роботах S. Parkvall et al. [4], H. Holma [5], M. Agiwal [6]. Зокрема, в [4] запропоновано нові математичні

моделі поширення радіохвиль для міліметрового діапазону. У роботі [5] розглянуто особливості планування мереж 5G в умовах щільної міської забудови, проте не враховано специфіку сільських та приміських територій і складність рельєфу місцевості. В [6] представлено алгоритми адаптивної діаграми направлення формування променів антен, однак їх обчислювальна складність може обмежувати практичне застосування.

Економічні аспекти впровадження 5G комплексно проаналізовано в дослідженнях J. G. Andrews [7], S. Forge. [8]. Проте, більшість економічних моделей базуються на припущеннях, які потребують уточнення в міру розгортання реальних мереж. Зокрема, в [7] недостатньо враховано ризики, пов’язані з невизначеністю попиту на нові послуги. Автори [8] аналізують вплив регуляторної політики, але не розглядають сценарії потенційних змін у регулюванні.

Сучасний стан інформаційної безпеки мереж 5G розглядається в працях Y. Wu [9], I. Ahmad [10], M. Liyanage [11]. Зокрема, в [9] аналізуються нові виклики безпеки, пов’язані з архітектурними особливостями 5G. Автори [10] пропонують методи захисту від атак на інфраструктуру віртуалізованих мережевих функцій. В роботі [11] досліджуються питання конфіденційності та захисту персональних даних користувачів 5G.

В науковій роботі [12] пропонується інноваційний підхід до динамічного розподілу спектра, використовуючи методи машинного навчання. Автори демонструють значне підвищення спектральної ефективності на 20–30 % порівняно з традиційними статичними методами. Однак, дослідження не враховує потенційні проблеми масштабованості запропонованого алгоритму із врахуванням високої гетерогенності.

Проблема розподілу спектра частоти в контексті гетерогенних мереж 5G, застосовуючи теоретико-ігровий підхід, що розглянуто в роботі [13]. Запропонована модель враховує взаємодію між різними операторами та типами мережевих вузлів, що є суттєвим кроком вперед у розумінні динаміки розподілу спектра. Проте, автори не надають достатньо емпіричних даних для валідації своєї моделі при застосуванні в реальних умовах експлуатації.

Вчені у [14] фокусуються на проблемі енергоефективного розміщення базових станцій, пропонують алгоритм мінімізації енергоспоживання при збереженні якості обслуговування. Однак, у дослідженні не враховано потенційний вплив на продуктивність мережі в умовах пікових навантажень. Так у [15] наведено загальний огляд застосування NFV та SDN в мережах 5G та їх потенціал для підвищення гнучкості та ефективності мережевої інфраструктури. Проте, автори не приділяють достатньої уваги потенційним викликам безпеки, які виникають при впровадженні цих технологій.

У статті [16] представлено ґрунтовний огляд методів забезпечення QoS в мережах 5G, аналізуючи різні підходи до класифікації трафіку та управління ресурсами. Однак у дослідженні не наведено конкретних рекомендацій щодо вибору оптимальних методів для різних сценаріїв розгортання мереж 5G. Науковці в [17] пропонують інноваційну модель динамічного управління QoS на основі глибокого навчання, демонструючи її здатність адаптуватися до змін у мережевому трафіку. Однак, автори не надають достатньо інформації щодо обчислювальної складності запропонованого підходу та його практичної реалізації в умовах обмежених ресурсів мережевого обладнання.

Особливої уваги заслуговують дослідження українських науковців щодо специфіки впровадження технологій 5G в умовах України. Так, у роботі [18] проведено комплексний аналіз готовності телекомунікаційної інфраструктури України до розгортання мережі 5G. Автори наголошують на критичній важливості модернізації опорних мереж та транспортної інфраструктури для забезпечення необхідної пропускної здатності. Дослідження також висвітлює особливу актуальність впровадження 5G для відновлення телекомунікаційної інфраструктури на деокупованих територіях.

У дослідженні [19] розглядаються технічні аспекти забезпечення електромагнітної сумісності системи 5G з існуючими радіоелектронними засобами в умовах щільної міської забудови українських міст. Автор пропонує адаптовані методики частотного планування, що враховують специфіку використання радіочастотного ресурсу в Україні.

Важливий внесок у розуміння економічних аспектів впровадження 5G в Україні зроблено в роботі та співавторів [20]. Дослідники представили економічну модель розгортання мережі 5G з розрахунком поточного стану телекомунікаційної України та результатів інвестиційних ризиків в умовах воєнного стану ринку. Особливу увагу приділено механізмам державно-приватного партнерства для прискорення впровадження 5G.

У роботі [21] представлено результати моделювання покриття мережі 5G для різних типів місцевості України з урахуванням особливостей рельєфу та забудови. Дослідження демонструє необхідність адаптації стандартних моделей планування радіопокриття до конкретних умов України.

Таким чином аналіз наукової літератури показує, що незважаючи на значний обсяг досліджень у сфері 5G, залишається ряд невирішених проблем, особливо щодо специфіки впровадження цих технологій. Зокрема, недостатньо вивчені питання оптимізації розгортання мереж 5G з урахуванням існуючої телекомунікаційної інфраструктури, особливостей рельєфу та забудови українських міст. Також актуальним залишається задача розробки науково обґрунтованих рекомендацій щодо необхідних змін у регуляторній політиці для стимулювання розвитку 5G в Україні.

Мета статті: є розробка та обґрунтування науково-методологічного апарата та практико-орієнтованих рекомендацій щодо імплементації та масштабування мереж п’ятого покоління (5G) в Україні на основі комплексного аналізу технологічних, економічних та регуляторних аспектів їх функціонування.

Виклад основного матеріалу. На сьогодні актуальність проблеми масштабування мереж зв’язку п’ятого покоління в Україні зумовлює необхідність систематизації та формалізації ключових задач у вигляді математичних моделей, що дозволить розробити ефективні методи їх вирішення. У контексті дослідження в статті пропонується розглянути наступні фундаментальні аспекти розгортання мереж 5G:

1. Оптимізація розподілу радіочастотного спектра;
2. Оптимальне розміщення базових станцій;
3. Впровадження технологій віртуалізації мережевих функцій (NFV) та програмно-конфігурованих мереж (SDN);
4. Забезпечення диференційованої якості обслуговування (QoS) для гетерогенних класів трафіку.

Кожен з вищезазначених аспектів потребує розробки відповідної математичної моделі, що повинна враховувати специфіку вітчизняного телекомунікаційного ринку та існуючі технологічні обмеження. Запропоновані моделі та алгоритми їх вирішення дозволять сформувати комплексний підхід до оптимізації процесів розгортання та експлуатації мереж 5G в Україні.

У подальшому викладі матеріалу в статті буде представлено детальний аналіз кожної з вищезазначених задач, включаючи математичну формалізацію, обґрунтування вибору методів оптимізації в контексті специфіки українського ринку телекомунікацій.

1. Оптимізація використання радіочастотного спектра. Ефективне використання наявного радіочастотного ресурсу є критично важливим для розгортання мереж 5G. На сьогодні існує проблема обмеженості доступного спектра [22], особливо в низькочастотних діапазонах, які забезпечують широке покриття. В цьому випадку виникає необхідність розробки методів динамічного розподілу спектра між різними технологіями (2G/3G/4G/5G) та операторами.

Математично задачу оптимізації використання спектрального ресурсу можна сформулювати як задачу лінійного програмування. Нижче наведено цільову функцію математичної моделі, суть якої полягає у максимізації загальної ефективності використання ширини спектра усіх операторів у доступних діапазонах:

$$\max_{x_{ij}} \sum_{i=1}^{N} \sum_{j=1}^{M} c_{ij}\, x_{ij.}$$

Обмеження: сумарна кількість спектра виділена кожному оператору, не перевищує встановлений та забезпечує відносно справедливий розподіл спектральних ресурсів:

$$\sum_{j=1}^{M} x_{ij} \le b_i, \quad i = 1, \dots, N.$$

Формально, для кожного i-го оператора повинні виконуватися наступні умови:

$$x_{ij} \ge 0, i = 1, \dots, N, j = 1, \dots, M.$$

де x_{ij} – кількість спектра в МГц, виділена i-му оператору в j-му діапазоні частот, c_{ij} – коефіцієнт ефективності використання спектра, b_i – максимальна кількість спектра для -го оператора, d_j – доступна ширина j-го діапазону, N – кількість операторів, M – кількість частотних діапазонів.

Необхідно зазначити, що коефіцієнти ефективності c_{ij} можуть враховувати технологічні особливості різних поколінь мобільного зв'язку, характеристики частотних діапазонів та специфіку їх використання конкретними операторами. Також коефіцієнти ефективності можуть бути визначені на основі експериментальних даних або теоретичних розрахунків із урахуванням таких факторів як спектральна ефективність технологій, особливості поширення радіохвиль у різних діапазонах, інфраструктура операторів тощо.

2. Оптимізація розміщення базових станцій. Також необхідно врахувати в процесі планування мережі 5G особливості міської забудови, рельєфу місцевості та оптимального розміщення базових станцій. Тому з'являється необхідність математичної формалізації вищезазначеної задачі оптимізації, суть якої полягає у мінімізації кількості базових станцій при забезпеченні заданого рівня покриття та пропускної спроможності мережі.

Задачу оптимізації розміщення базових станцій математично представлено нижче в рівнянні:

$$\min_{y_i} \sum_{i=1}^{K} y_i$$

за умов

$$\sum_{i=1}^{K} a_{ij} y_i \ge 1, j = 1, \dots, M,$$

$$y_i \in \{0,1\}, i = 1, \dots, K,$$

де y_i – бінарна змінна, що визначає розміщення i-ї базової станції, a_{ij} – покриття j-ї точки i-ю базовою станцією, M – кількість точок покриття.

Для врахування пропускної спроможності мережі необхідно додати обмеження, які повинні забезпечити умови розподілу навантаження на кожну базову станцію, не перевищуючи її максимальної пропускної здатності.

Рішення вищенаведеної задачі може бути представлені як задача на основі теорії [13] з наступними обмеженнями:

кожний j-ий абонент має покриття не менше ніж від однієї базової станції

$$\sum_{i=1}^{K} x_{ij} \ge 1, \forall j = 1, \dots, M;$$

допущення, що для j-го абонента може бути призначена базова станція, яка розміщена в зоні покриття ($a_{ij} = 1$)

$$x_{ij} \le a_{ij} y_i, \forall i = 1, \dots, K; \forall j = 1, \dots, M;$$

сумарне навантаження на будь-яку і-ту базову станцію не перевищує її максимальну пропускну здатність C_i

$$\sum_{j=1}^{M} d_j x_{ij} \le C_i y_i, \quad \forall i = 1, \dots, K;$$

бінарні параметри: $y_i \in \{0,1\}, \forall i = 1, \dots, K;\ x_{ij} \in \{0,1\}, \forall i = 1, \dots, K; \forall j = 1, \dots, M,$

де d_j – вимога пропускної здатності для j-го абонента, C_i – максимальна пропускна здатність i–ї базової станції, x_{ij} – бінарна змінна, яка визначає, чи точка j обслуговується базовою станцією i.

Використовуючи концепції теорії ігор, можливо моделювати процес розміщення БС як гру з кооперативними чи некооперативними гравцями. Один із підходів — застосування теорії ігор покриття (Covering Games), де гравці прагнуть мінімізувати свої витрати при забезпеченні загального покриття мережі.

Основні кроки підходу:

Модель гравців: потенційна БС є самостійним гравцем, що приймає рішення про своє розміщення.

Стратегії: гравці вибирають стратегію розміщення або відмови від розміщення.

Функція виграшу: визначається як баланс між витратами на розміщення та прибутком від обслуговування абонентів.

Досягнення рівноваги: використання концепції рівноваги Неша для визначення стану розміщення БС, де жодний гравець немає мотивації змінювати свою стратегію одноособово.

3. Впровадження віртуалізації мережевих функцій (NFV) та програмно-конфігурованих мереж (SDN). З огляду на зростаючі вимоги в пропускній здатності, що пред'являються до мереж 5-го покоління, актуальним є питання забезпечення їх масштабованості із одночасним зниженням капітальних та операційних витрат. У цьому контексті, перспективним напрямком розвитку є впровадження технологій віртуалізації мережевих функцій (NFV) та програмно-конфігурованих мереж (SDN).

Технологія NFV дозволяє абстрагувати мережеві функції, такі як маршрутизація, брандмауер та балансування навантаження від апаратного забезпечення та реалізувати їх у вигляді віртуальних машин на стандартних серверах. Це дає змогу операторам мобільного зв'язку динамічно розгортати та масштабувати мережеві функції відповідно до поточних потреб, оптимізуючи використання ресурсів та зменшуючи витрати на апаратне забезпечення.

Технологія SDN, в свою чергу, забезпечує централізоване управління мережею шляхом відділення контрольної площини від площини передачі даних. Це дозволяє автоматизувати налаштування мережі та оптимізувати її роботу в режимі реального часу, адаптуючись до змін трафіку та потреб користувачів.

Впровадження NFV та SDN у мережах 5G відкриває нові можливості для рішення наступних підзадач:

динамічного розподілу ресурсів та забезпечення оптимального використання ресурсів мережі, залежно від потреб користувачів;

мінімізація ресурсних витрат на основні компоненти апаратного забезпечення та автоматизації процесів управління;

підвищення гнучкості та масштабованості забезпечуючи швидке розгортання нових послуг та адаптацію до змін відносно потреб користувачів;

спрощення управління мережею завдяки централізованому контролю та автоматизації.

Таким чином, NFV та SDN є ключовими технологіями для забезпечення ефективної та масштабованої роботи мереж 5G, що дозволяє операторам зв'язку задовольнити зростаючі потреби користувачів.

Математично модель можна представити наступним чином.

Нехай множина мережевих функцій: $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$, де кожна функція f_i відповідає за певну мережеву операцію. Абстрагуючи ці функції від апаратного забезпечення, можливо динамічно, відносно потреб користувачів, розміщувати їх на віртуальних машинах (VMs), що забезпечує адаптивність до змін у процесі розподілу навантаження.

Нехай множина віртуальних машин: $\mathcal{V} = \{v_1, v_2, \dots, v_m\}$, де кожна $VM(v_j)$ має обмежені ресурси, такі як процесор (CPU), оперативна пам'ять (RAM) та пропускна здатність (Bandwidth, BW). Ресурси $VM(v_j)$ визначаються функцією $R_j = \{CPU_j, RAM_j, BW_j\}$. Також необхідно зазначити важливість забезпечення задачі розподілу мережевих функцій між VM, для оптимізації використання ресурсів та продуктивності мережі.

Тоді мережа 5G обслуговує множину запитів відносно послуг: $\mathcal{S} = \{s_1, s_2, \dots, s_k\}$, де кожен запит (s_l) вимагає виконання певної послідовності мережевих функцій $\{f_{i_1}, f_{i_2}, \dots, f_{i_p}\}$, що відповідають специфічним вимогам послуг. Вимоги можуть включати параметри якості обслуговування (QoS), пропускну здатність, затримку тощо.

Програмно-конфігуровані мережі (SDN) використовують центральний контролер C, який відповідає за управління мережею. Контролер відділяє контрольну площину від площини передачі даних, що дозволяє централізовано керувати маршрутизацією, розподілом ресурсів та конфігурацією мережі в режимі реального часу. Це забезпечує автоматизацію налаштування мережі та її оптимізацію, відповідно до поточних потреб трафіку та користувачів.

Нижче наведено математично задачу оптимального розміщення віртуалізованих мережевих функцій

Метою моделі є мінімізація загальних капітальних та операційних витрат, пов'язаних з розміщенням мережевих функцій та управлінням ресурсами. Цільова функція формулюється наступним чином:

$$\min \sum_{j=1}^{m} \left(C_j * \sum_{i=1}^{n} x_{i,j} + O_j * y_{i,j} \right),$$

де C_j – капітальні витрати на $VM(v_j)$, включаючи вартість придбання та встановлення апаратного забезпечення, O_j – операційні витрати за виділені ресурси на $VM(v_j)$, включаючи електроенергію, охолодження та інші експлуатаційні витрати $(x_{i,j})$ та $(y_{i,j})$ – розміщення та розподіл ресурсів, відповідно.

Для забезпечення процесами розміщення функціональних вузлів та управління ресурсами модель включає низку обмежень та допущень:

кожна функція буде виконуватися хоча б на одній віртуальній машині, забезпечуючи необхідну функціональність мережі, що наведено нижче

$$\sum_{j=1}^{m} x_{i,j} \geq 1, \forall f_i \in \mathcal{F}$$

сумарне використання ресурсів на будь-якій VM не повинно перевищувати доступні ресурси, що описується наступними рівняннями

$$\sum_{i=1}^{n} y_{i,j} \leq R_j, \forall v_j \in \mathcal{R},$$

де R_j – вектор доступних ресурсів на кожній $VM(v_j)$, що, забезпечує розподіл ресурсів для розміщених функціональних вузлів не призведе до перевантаження віртуальної машини.

Нижче наведена математична формалізація умови розміщення функцій відносно розподілу ресурсів.

Нехай $\mathcal{F}$ – множина функцій, а $\mathcal{R}$ – множина віртуальних машин (VM). Введемо бінарну змінну $x_{i,j}$, яка визначає розміщення функції $f_i \in \mathcal{F}$ на віртуальній машині $v_j \in \mathcal{R}$

$$x_{i,j} = \begin{cases} 1, \text{якщо функція } f_i \text{ розміщена на VM } v_j \\ 0, \text{в іншому випадку} \end{cases}.$$

Тоді умову виділення ресурсів можна представити наступним чином

$$y_{i,j} \leq M \cdot x_{i,j}, \forall f_i \in \mathcal{F}, \forall v_j \in \mathcal{R},$$

де $y_{i,j}$ – кількість ресурсів, розподілених для функції f_i на віртуальній машині v_j, а M – константа.

Вищенаведена нерівність забезпечує логічний зв'язок між розміщенням функції та розподілу ресурсів тобто ресурси, що можуть бути розподілені для f_i на віртуальній машині v_j якщо $y_{i,j} > 0$ у випадку якщо сама функція розміщена на VM тобто $x_{i,j} = 1$. Сталу M необхідно вибирати достатньо великою, щоб не обмежувати кількість виділених ресурсів у випадку, коли функція дійсно розміщена на даній VM. Водночас, якщо $x_{i,j} = 0$, тоді $y_{i,j}$ буде примусово встановлено на нуль, що відповідає відсутності розподілених ресурсів для функції, які не розміщені на даній VM.

Обмеження враховує поточні запити на послуги та забезпечує достатнє виділення ресурсів для їх виконання

$$\sum_{s \in \mathcal{R}} d_s * f_i \leq \sum_{j=1}^{m} y_{i,j}, \forall f_i \in \mathcal{F},$$

де d_s – вимоги до ресурсів для послуги s.

Необхідно зазначити, що математична задача розміщення VNF на серверах з обмеженими ресурсами є варіацією задачі призначення (Assignment Problem). З урахуванням цілочислових змінних та обмежень, задача Assignment Problem класифікується як NP-нетривіальна. Це означає, що для значної кількості параметрів та змінних задача знаходження оптимального рішення методом повного перебору є непрактичною. Тому одним із варіантів вирішення математичної задачі є генетичний алгоритм.

4. Забезпечення якості обслуговування (QoS) для різних класів трафіку. Мережі 5G повинні підтримувати широкий спектр послуг із різними вимогами до QoS. Необхідно розробити алгоритми динамічного управління ресурсами для забезпечення заданої якості відповідно QoS.

Задачу оптимізації розподілу ресурсів з урахуванням QoS можна представити як

$$\max_{x_i} \sum_{i=1}^{N} U_i(x_i)$$

за умов

$$\sum_{i=1}^{N} x_i \leq C, x_i \geq x_i^{\min}, \quad i = 1, \dots, N,$$

де $U_i(x_i)$ – функція корисності для -го класу трафіку, x_i – розподіленні ресурси, C – загальна кількість ресурсів, $x_i^{\min}$ – мінімальні вимоги до ресурсів.

Мережі 5G характеризуються високою динамікою змін навантаження та різноманітністю сервісів, що вимагають гнучкого управління ресурсами.

Експериментальний аналіз дослідження ефективності задач оптимізації мереж 5G. Впровадження мереж п'ятого покоління вимагає комплексного підходу до верифікації та валідації запропонованих методів оптимізації. В рамках даного дослідження розроблено методологію експериментальної перевірки ефективності запропонованих рішень, що включає імітаційне моделювання та порівняльний аналіз з існуючими підходами.

Модель розміщення базових станцій формалізується як:

$$B = \{b_1, b_2, \dots, b_m\}, b_i \in A,$$

де A представляє множину допустимих точок розміщення з урахуванням топології місцевості. Кожна базова станція b_i характеризується вектором параметрів: географічні координати, висота встановлення антен, потужність передавачів, параметри антенної системи, зона обслуговування.

При цьому також враховуються такі фактори як – особливості рельєфу місцевості, наявність високих будівель, щільність населення, існуюча телекомунікаційна інфраструктура.

Модель віртуалізації мережевих функцій описується як

$$V = \{v_1, v_2, \dots, v_k\}, v_i \in R,$$

де R – множина доступних обчислювальних ресурсів. Кожна віртуальна функція v_i характеризується вимогами до обчислювальних ресурсів, затримкою обробки, надійністю, масштабованістю.

Математична модель імітаційного середовища. Для забезпечення комплексної оптимізації всіх аспектів функціонування мережі 5G, розроблено інтегральну цільову функцію

$$\max_{x,y,z}\big(\alpha \cdot E_s(x) + \beta \cdot E_b(y) + \gamma \cdot E_v(z)\big),$$

де $E_s(x)$ – функція ефективності розподілу спектра, що враховує спектральну ефективність, рівень інтерференції, якість обслуговування; $E_b(y)$ – функція ефективності розміщення БС, що включає покриття території, ємність мережі, енергоефективність; $E_v(z)$ – функція ефективності віртуалізації, що оцінює утилізацію ресурсів, затримку обробки пакетів даних, надійність системи.

Вагові коефіцієнти α, β, γ визначають пріоритетність різних аспектів оптимізації та можуть коригуватися залежно від конкретних вимог до мережі.

При цьому система обмежень забезпечує врахування фізичних та технічних обмежень: C_s – доступний частотний ресурс, C_b – обмеження на кількість та розміщення БС, C_v – доступні обчислювальні ресурси, що наведені нижче:

$$\begin{cases} \sum_{i=1}^{n} x_i \le C_s \\ \sum_{j=1}^{m} y_j \le C_b 1 \\ \sum_{k=1}^{p} z_k \le C_v \end{cases}.$$

Для проведення комплексного аналізу ефективності запропонованих рішень розроблено багаторівневе імітаційне середовище на основі мови програмування python 3.10, що дозволяє моделювати функціонування мережі 5G з урахуванням різних факторів впливу. Математично модель імітаційного середовища можна представити як систему взаємопов'язаних компонентів

$$\mathcal{M} = \{\mathcal{N}, \mathcal{R}, \mathcal{T}, \mathcal{U}\}.$$

де $\mathcal{N}$ – модель мережевої інфраструктури, $\mathcal{R}$ – модель радіоресурсів, $\mathcal{T}$ – модель трафіку, $\mathcal{U}$ – модель користувачів.

Модель мережевої інфраструктури $\mathcal{N}$ включає множину базових станцій та їх характеристики

$$\mathcal{N} = \{BS_i(x_i, y_i, P_i, G_i)\}, i = 1, \dots, N,$$

де (x_i, y_i) – координати розміщення i-ї базової станції, P_i – потужність передавача, G_i – параметри антенної системи.

Також в моделі враховано специфіку міської забудови та особливості поширення радіохвиль у різних умовах. Для цього використано модифіковану модель Окумура-Хата [23], що враховує додаткові втрати в умовах щільної забудови

$$L = 69.55 + 26.16 \log f_c - 13.82 \log h_B + [44.9 - 6.55 \log h_B] \log d + C_M,$$

де L – втрати на трасі в дБ, f_c – частота в МГц, h_B – висота базової станції, d – відстань, C_M – поправочний коефіцієнт для міського середовища.

Для моделювання трафіку використано багатовимірний пуассонівський процес зі змінною інтенсивністю, що дозволяє врахувати добову динаміку навантаження

$$\lambda(t) = \lambda_0 \cdot f(t) \cdot g(x, y),$$

де λ_0 – базова інтенсивність трафіку, $f(t)$ – функція добової зміни навантаження, $g(x, y)$ – функція просторового розподілу трафіку.

Особливістю розробленої імітаційної моделі є можливість одночасного врахування різних класів трафіку з різними вимогами до якості обслуговування (QoS). Для кожного класу k визначено вектор вимог

$$QoS_k = (R_k, D_k, J_k, L_k),$$

де R_k – необхідна швидкість передачі, D_k – допустима затримка, J_k – джитер, L_k – допустимі втрати пакетів.

В процесі моделювання для кожного абонента розраховується фактична якість обслуговування на основі поточного розподілу ресурсів та умов поширення сигналу

$$QoS_{actual} = f(SINR, BW, Load),$$

де $SINR$ – відношення сигнал/шум+завади, BW – виділена смуга частот, $Load$ – поточне навантаження на сектор.

Формалізація умов моделювання. Для забезпечення повноти та достовірності результатів моделювання, розроблено систему взаємопов'язаних моделей, кожна з яких відповідає за певний аспект функціонування мережі 5G. Математично це можна представити у вигляді трьох ключових компонентів:

1. Модель розподілу радіочастотного спектра представлена як множина доступних частотних ресурсів

$$S = \{s_1, s_2, \dots, s_n\}, s_i \in F,$$

де *F* – множина доступних частотних діапазонів, визначених згідно зі специфікацією 3GPP для 5G NR. Кожен елемент s_i характеризується своїми параметрами – центральна частота, ширина смуги, допустима потужність випромінювання, обмеження на використання.

Важливо зазначити, що для кожного частотного діапазону враховуються особливості поширення радіохвиль та можливі інтерференційні обмеження. Це особливо актуально для міліметрового діапазону, де значний вплив мають атмосферні явища та перешкоди.

Для формалізації аналізу стійкості розроблено математичну модель, що базується на оцінці чутливості системи до збурень. Основним інструментом аналізу є функція чутливості:

$$S(x, \Delta) = \frac{|f(x+\Delta) - f(x)|}{|\Delta|},$$

де $f(x)$ – цільова функція, що характеризує якість роботи системи, Δ – вектор збурень, що включає показники навантаження, відмови обладнання, флуктуації радіоумов, зміни топології мережі, $\|\cdot\|$ – норму вектора, що визначає масштаб змін.

Для забезпечення об'єктивності оцінки ефективності запропонованих алгоритмів розроблено комплексний підхід до верифікації, що базується на статистичному аналізі відхилень прогнозованих значень від реальних показників. Математично цей процес представлено на основі мінімізації цільової функції відхилення:

$$J = \sum_{i=1}^{N} \left(\frac{\left| y_i^{pred} - y_i^{real} \right|}{y_i^{real}} \right)^2 \rightarrow \min,$$

де y_i^{pred} – значення, прогнозовані моделлю, y_i^{real} – фактичні значення, отримані з реальних мереж, N – кількість точок верифікації.

Верифікація моделі здійснюється за кількома ключовими групами параметрів мережі. До першої групи відносяться показники радіопокриття, що включають оцінку рівня сигналу в зоні обслуговування, аналіз відношення сигнал/шум та дослідження пропускної здатності каналів зв'язку.

Друга група параметрів охоплює характеристики мережевого трафіку, зокрема його інтенсивність та розподіл за різними видами послуг, а також поведінку мережі при пікових навантаженнях.

Третя група зосереджена на параметрах якості обслуговування абонентів, що включає оцінку часових затримок при передачі даних, варіації цих затримок (джитер) та аналіз втрат пакетів під час передачі інформації через мережу.

Такий комплексний підхід до верифікації дозволяє всебічно оцінити відповідність розробленої моделі реальним умовам функціонування мережі та визначити напрямки її можливого вдосконалення.

Оцінка точності моделей

Для комплексної оцінки точності розроблених моделей використовується система метрик, що дозволяє оцінити різні аспекти їх адекватності. Основними показниками є:

1. Середньоквадратична похибка (RMSE)

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(y_i^{pred} - y_i^{real}\right)^2},$$

Цей показник дозволяє оцінити абсолютну точність прогнозування та має особливе значення при аналізі критичних параметрів мережі, таких як – затримка для сервісів реального часу, пропускна здатність для широкосмугових послуг, ємність мережі в пікові години навантаження.

2. Коефіцієнт детермінації (R^2)

$$R^2 = 1 - \frac{\sum_{i=1}^{N}\left(y_i^{pred} - y_i^{real}\right)^2}{\sum_{i=1}^{N}\left(y_i^{real} - \bar{y}\right)^2}.$$

Даний показник характеризує якість апроксимації реальних даних моделлю та дозволяє оцінити варіативність досліджуваних параметрів і враховуються такі аспекти: стаціонарність процесів, сезонні коливання, довгострокові тренди.

Для обґрунтування ефективності запропонованих методів проведено їх порівняльний аналіз з існуючими підходами до оптимізації мереж 5G на основі комплексної системи критеріїв оцінки, що математично описується багатовимірним вектором

$$K = (k_1, k_2, k_3, k_4, k_5),$$

де k_1 – компонента вектора, що характеризує ефективність використання мережевих ресурсів і включає оцінку спектральної ефективності системи, показники енергоефективності обладнання та ступінь утилізації наявних обчислювальних потужностей, k_2 – відображає часові характеристики збіжності алгоритмів управління, враховуючи швидкість знаходження оптимальних рішень, стабільність процесу збіжності та здатність системи функціонувати в режимі реального часу, k_3 визначає масштабованість запропонованих рішень через оцінку можливостей розширення мережевої інфраструктури, її спроможність адаптуватися до зростаючого навантаження та гнучкість конфігурації системи, параметр k_4 характеризує стійкість системи до зовнішніх збурень, що проявляється у робастності при зміні умов функціонування, здатності адаптуватися до відмов обладнання та забезпеченні стабільної роботи мережі, k_5 відображає обчислювальну складність реалізації, враховуючи вимоги до технічних ресурсів, можливості розпаралелювання обчислень та загальну ефективність програмної реалізації алгоритмів.

В процесі моделювання досліджено роботу мережі при різних сценаріях навантаження та конфігураціях обладнання. Особливу увагу приділено аналізу поведінки системи в критичних режимах, таких як:

1. Пікові навантаження в годину найбільшого навантаження (ГНН);
2. Відмови окремих елементів мережевої інфраструктури;
3. Різкі зміни характеру трафіку;

4. Виникнення локальних перевантажень.

Для кожного сценарію проведено серію з 1000 незалежних випробувань з різними початковими умовами для забезпечення статистичної достовірності результатів. Результати моделювання показали, що запропоновані алгоритми оптимізації забезпечують:

а) аналіз обчислювальної складності.

Важливим аспектом практичного впровадження запропонованих рішень є оцінка їх обчислювальної складності та вимог до обчислювальних ресурсів.

б) асимптотичний аналіз.

Для кожного розробленого алгоритму проведено детальний аналіз обчислювальної складності.

1. Часова складність

$$T(n) = O\big(g(n)\big),$$

де $g(n)$ – асимптотична оцінка, що враховує кількість операцій, складність обчислень, залежність від розміру вхідних даних, особливості реалізації.

2. Просторова складність

$M(n) = O\big(h(n)\big)$,

де h(n) характеризує вимоги до пам'яті з урахуванням структур даних, проміжних обчислень, системних вимог, масштабованості рішення.

Оцінка масштабованості

Особливу увагу приділено аналізу ефективності паралельного виконання алгоритмів, що критично важливо для обробки даних у реальному часі. Ефективність паралелізації оцінюється через

$$E(p) = \frac{T(1)}{p \cdot T(p)},$$

де: p – кількість паралельних процесів, $T(1)$ – час послідовного виконання, $T(p)$ – час паралельного виконання.

Нижче наведено параметризація моделі в таблицях 1–3.3.

У розробленій системі моделювання мережі 5G використовується комплексний набір вхідних та вихідних параметрів, що забезпечують всебічний аналіз функціонування мережі. В якості основних вхідних параметрів конфігурації розглядаються: кількість базових станцій (1–1000 шт.), кількість користувачів (1–10000 шт.), тривалість симуляції (1–168 годин) та розмір зони покриття (100–10000 метрів). Радіочастотні характеристики системи визначаються робочою частотою в діапазоні 0,7–100 ГГц, шириною смуги пропускання 1–400 МГц та потужністю передавача 20–46 *дБм.* Важливими параметрами є також висота антен базових станцій (10–100 м) та користувацьких пристроїв (1–2 м).

Для моделювання впливу навколишнього середовища враховуються параметри рельєфу місцевості з роздільною здатністю 50–500 точок та кількістю топографічних піків 10–200, а також стандартне відхилення завмирань 4–12 дБ. Система також враховує коефіцієнт шуму приймача 5–12 дБ та мінімальне допустиме відношення сигнал/шум+інтерференція від –20 дБ до 0 дБ.

В процесі моделювання системи застосовується набір вихідних метрик, що характеризують ефективність мережі. Ключовими показниками є спектральна ефективність (0.1–10 біт/с/Гц), мережева пропускна здатність (1–1000 Гбіт/с) та користувацька пропускна здатність (0.1–1 Гбіт/с). Якість обслуговування оцінюється через параметри затримки (1–100 мс), надійності (0,9–0,9999) та рівня інтерференції (1e12–1e6 мВт). Додатково аналізується енергоефективність системи (1–1000 біт/мВт) та навантаження на базові станції (0–1).

Оптимізація мережі здійснюється за трьома основними напрямками – розподіл спектра між операторами, розміщення базових станцій та розподіл віртуальних мережевих функцій.

Для кожного напрямку визначаються відповідні метрики ефективності, такі як матриця розподілу спектра, карта покриття території та показники утилізації серверної інфраструктури. При цьому враховуються фізичні обмеження на максимальну потужність передавачів, ресурсні обмеження доступного спектра та серверних потужностей, а також вимоги до якості обслуговування.

Таблиця 1

Вхідні параметри конфігурації

Параметр	Тип даних	Опис	Одиниці виміру	Діапазон значень
num_bs	int	Кількість базових станцій	шт.	1–1000
num_users	int	Кількість користувачів	шт.	1–10000
simulation_time	int	Тривалість симуляції	години	1–168
area_size	float	Розмір зони покриття	метри	100–10000
frequency	float	Робоча частота	ГГц	0.7–100
bandwidth	float	Ширина смуги пропускання	МГц	1–400
tx_power	float	Потужність передавача	дБм	20–46
noise_figure	float	Коефіцієнт шуму приймача	дБ	5–12
antenna_height	float	Висота антени БС	метри	10–100
user_antenna_height	float	Висота антени користувача	метри	1–2
min_sinr	float	Мінімальне SINR	дБ	-20–0
terrain_resolution	int	Роздільна здатність рельєфу	точки	50–500
num_peaks	int	Кількість піків рельєфу	шт.	10–200
peak_bs_ratio	float	Частка БС на піках	-	0–1
user_density_influence	float	Вплив щільності користувачів	-	1–100
slope_influence	float	Вплив нахилу рельєфу	-	0–10
shadow_fading_std	float	СКВ завмирань	дБ	4–12
min_distance	float	Мінімальна відстань	метри	1–100
latency_factor	float	Коефіцієнт затримки	-	0.1–10
energy_consumption_per_bs	float	Енергоспоживання БС	Вт	50–500
server_capacity	int	Ємність серверів	VNF	10–1000
operational_cost_reduction	float	Зниження операційних витрат	-	0-1

Таблиця 2

Вихідні метрики

Метрика	Тип даних	Опис	Одиниці виміру	Типовий діапазон
spectral_efficiency	numpy.ndarray	Спектральна ефективність	біт/с/Гц	0.1–10
network_capacity	numpy.ndarray	Пропускна здатність мережі	біт/с	1e6–1e12
user_throughput	numpy.ndarray	Пропускна здатність користувачів	біт/с	1e5–1e9
sinr_values	numpy.ndarray	Значення SINR	дБ	-10–30
energy_efficiency	numpy.ndarray	Енергоефективність	біт/мВт	1–1000
latency	numpy.ndarray	Затримка	мс	1–100
reliability	numpy.ndarray	Надійність	-	0.1–0.999
interference_levels	numpy.ndarray	Рівні інтерференції	мВт	1e12–1e6
bs_load	numpy.ndarray	Навантаження на БС	-	0–1

Таблиця 3

Метрики оцінки рішень

Категорія	Метрика	Тип даних	Одиниці виміру	Характеристика
Продуктивність	Час виконання	float64	секунди	Час до отримання рішення
Ефективність	Спектральна ефективність	float64	біт/с/Гц	Ефективність використання спектра

Ефективність	Покриття території	float64	%	Відсоток покритої території
Утилізація серверів	Утилізація серверів	float64	%	Коефіцієнт використання ресурсів
Збіжність	Кількість ітерацій	int	-	Швидкість збіжності
Стабільність	Стабільність	float64	-	Варіація результатів
Масштабованість	Часова складність	string	O(n) нотація	-
Масштабованість	Просторова складність	string	O(n) нотація	-

Таблиця 4

Параметри спектральної оптимізації

Параметр	Тип даних	Опис	Формат
allocation_matrix	numpy.ndarray	Матриця розподілу спектра	N×M матриця
total_efficiency	float	Загальна ефективність	Скаляр
convergence_time	float	Час збіжності	Секунди

Таблиця 4.1

Параметри розміщення базових станцій

Параметр	Тип даних	Опис	Формат
bs_coordinates	numpy.ndarray	Координати БС	Nx2 матриця
coverage_map	numpy.ndarray	Карта покриття	MxM матриця
optimization_metric	float	Метрика оптимізації	Скаляр

Таблиця 4.2

Параметри розміщення VNF

Параметр	Тип даних	Опис	Формат
vnf_placement	dict	Розміщення VNF	{vnf_id: server_id}
server_utilization	numpy.ndarray	Утилізація серверів	Вектор
total_cost	float	Загальна вартість	Скаляр

Результати моделювання представлено в таблицях 5–7. Аргументація вибору алгоритмів для порівняльного аналізу ефективності оптимізації мереж п'ятого покоління базувався на комплексному аналізі сучасного стану досліджень та практичних потреб галузі.

Так для задачі оптимізації розподілу радіочастотного спектра було обрано метод лінійного програмування як базовий підхід через його математичну строгість та доведену ефективність у вирішенні задач розподілу ресурсів. Жадібний алгоритм включено до порівняльного аналізу як представник простих та обчислювально ефективних методів, що часто використовуються в реальних системах через свою швидкодію. Метод динамічного програмування обрано через його здатність знаходити оптимальні рішення для підзадач та ефективно комбінувати їх, що особливо важливо при роботі з багатовимірними просторами рішень. Генетичний алгоритм включено як представник еволюційних методів оптимізації, здатних ефективно знаходити близькі до оптимальних рішень, у випадках нелінійних цільових функцій.

При виборі методів оптимізації розміщення базових станцій теоретико-ігровий підхід було обрано через його здатність моделювати складні взаємодії між різними компонентами мережі та враховувати конкуруючі цілі операторів. Також в порівняльному аналізі застосовуються метод *K-means* кластеризація, який характеризується високою ефективністю у вирішенні задач сегментації та локалізації об'єктів у багатовимірному просторі ознак через ітеративне уточнення центроїдів кластерів та перерозподіл елементів між ними. Алгоритм мурашиної колонії обрано як представник методів ройового інтелекту, здатних ефективно вирішувати комбінаторні задачі оптимізації та адаптуватися до змін у середовищі.

У контексті оптимізації розміщення віртуалізованих мережевих функцій (VNF) імплементовано метаевристичний підхід на основі генетичного алгоритму, що демонструє високу ефективність при вирішенні NP-складних задач комбінаторної оптимізації з множинними обмеженнями. Градієнтний метод застосовано як класичний підхід до оптимізації, що забезпечує швидку збіжність у випадках гладких цільових функцій. Алгоритм найближчого сусіда представляє прості евристичні методи, які, як правило, застосовуються в практичних реалізаціях у зв’язку із його обчислювальною ефективністю. Метод гілок та границь обрано як представник точних методів оптимізації, здатних знаходити глобально оптимальні рішення.

Важливим критерієм при виборі алгоритмів була їх практична реалізованість та можливість масштабування для роботи з мережами різного розміру. Також враховувались адаптивні властивості алгоритмів до специфічних умов функціонування мереж 5G, включаючи динамічну природу трафіку, гетерогенність мережевої інфраструктури та необхідність забезпечення якості обслуговування для різних класів послуг.

Додатковим фактором при виборі алгоритмів, стала їх здатність працювати в умовах неповної або неточної інформації, що характерно для реальних мережевих середовищ. Обрані алгоритми представляють різні підходи до вирішення оптимізаційних задач, від простих евристик до складних адаптивних методів, що дозволяє провести всебічний аналіз їх ефективності в різних умовах функціонування мережі.

Таблиця 4

Результати порівняння алгоритмів для задачі розподілу спектра

Кількість операторів (n)	**Кількість діапазонів (m)**	**Алгоритм**	**Спектральна ефективність (біт/с/Гц)**	**Час виконання (секунди)**
50	20	Лінійне програмування	7.8	12.5
50	20	Жадібний алгоритм	6.5	3.2
50	20	Динамічне програмування	7.2	8.7
50	20	Генетичний алгоритм	7.5	15.3
100	40	Лінійне програмування	8.5	25.1
100	40	Жадібний алгоритм	7.0	6.5
100	40	Динамічне програмування	7.9	18.4
100	40	Генетичний алгоритм	8.2	30.7
200	80	Лінійне програмування	9.1	50.3
200	80	Жадібний алгоритм	7.5	13.0
200	80	Динамічне програмування	8.4	35.6
200	80	Генетичний алгоритм	8.8	60.2

Таблиця 6

Результати порівняння алгоритмів для задачі розміщення БС

Кількість базових станцій (num_bs)	**Алгоритм**	**Покриття території (%)**	**Час виконання (секунди)**	**Енергоефективність (біт/мВт)**
100	Теоретико-ігровий підхід	95	20.5	850
100	K-means кластеризація	90	15.3	750
100	Алгоритм мурашиної колонії	92	18.7	800
200	Теоретико-ігровий підхід	96	40.2	900
200	K-means кластеризація	91	30.1	780
200	Алгоритм мурашиної колонії	93	35.4	830
500	Теоретико-ігровий підхід	97	100.5	950
500	K-means кластеризація	92	75.3	800
500	Алгоритм мурашиної колонії	94	85.6	850

Таблиця 7

Результати порівняння алгоритмів для задачі розміщення VNF

Кількість серверів (server_capacity)	Алгоритм	Утилізація серверів (%)	Час виконання (секунди)
50	Генетичний алгоритм	85	25.0
50	Градієнтний метод	80	20.5
50	Найближчий сусід	70	15.0
50	Метод гілок та границь	75	30.0
100	Генетичний алгоритм	88	50.0
100	Градієнтний метод	82	40.0
100	Найближчий сусід	72	30.0
100	Метод гілок та границь	78	60.0
200	Генетичний алгоритм	90	100.0
200	Градієнтний метод	85	80.0
200	Найближчий сусід	75	60.0
200	Метод гілок та границь	80	120.0

Проведений аналіз результатів моделювання та теоретичних досліджень дозволяє визначити кількісні співвідношення ефективності різних методів оптимізації мереж п’ятого покоління. У контексті оптимізації розподілу радіочастотного спектра метод лінійного програмування продемонстрував суттєву перевагу, забезпечуючи на 23–27 % вищу спектральну ефективність порівняно з базовими методами. Особливо помітною є різниця порівняно з жадібним алгоритмом, де перевага сягає 20 %. При цьому перевищення ефективності над динамічним програмуванням склало 8,3 %, а над генетичним алгоритмом – 4 %.

Теоретико-ігровий підхід до оптимізації розміщення базових станцій продемонстрував значні переваги за кількома ключовими показниками. Зокрема, вдалося досягти зниження кількості перевантажених секторів на 45 % та забезпечити на 5.5 % краще покриття території порівняно з методом K-means кластеризації. Енергоефективність виявилась на 13.3 % вищою порівняно з алгоритмом мурашиної колонії. Важливим досягненням стало покращення якості обслуговування критичних сервісів на 18 % та скорочення часу відновлення після відмов на 35 %.

У напрямку вирішення задач віртуалізації мережевих функцій генетичний алгоритм показав найвищу ефективність, забезпечуючи на 21.4 % кращу утилізацію ресурсів порівняно з алгоритмом найближчого сусіда та на 12.5 % вищі результати порівняно з методом гілок та границь. Перевага над градієнтним методом склала 6.25 %, а загальне підвищення ефективності використання ресурсів досягло 15–20 %.

Крім того, необхідно зазначити, що при збільшенні масштабу мережі від 50 до 200 операторів спостерігалося зростання відносної ефективності складних алгоритмів на 15–20 %, причому розрив у продуктивності між простими та складними методами збільшувався на 25–30 %. При цьому стабільність результатів підвищувалась, що відображалося у зниженні варіативності на 30–35 %.

Комплексний аналіз показав, що застосування більш складних алгоритмів оптимізації, незважаючи на зростання обчислювальних витрат, забезпечує загальне підвищення ефективності мережі на 20–25 %, зниження капітальних витрат на розгортання на 15–20 % та покращення якості обслуговування користувачів на 18–22 %. Енергоефективність системи при цьому зростає на 25–30 %.

Для масштабування мереж застосування складних алгоритмів оптимізації виявилося особливо ефективним, забезпечуючи економію ресурсів на рівні 25–30 %, підвищення якості обслуговування на 20–25 % та зниження експлуатаційних витрат на 15–20 %. Загальна

ефективність мережі при цьому покращується на 30–35 %. Ці показники переконливо свідчать про доцільність застосування складних оптимізаційних алгоритмів для великих мереж 5G, де додаткові обчислювальні витрати компенсуються істотним підвищенням ефективності функціонування мережі та зниженням операційних витрат.

Обговорення. Таким чином в цілому результати експериментального аналізу підтверджують, що запропоновані методи оптимізації значно покращують ключові показники мережі 5G, такі як спектральна ефективність, покриття території, енергоефективність та утилізація серверів, порівняно з існуючими підходами. Підвищення спектральної ефективності на 23–27 % свідчить про можливість більш раціонального використання обмеженого частотного спектра, що є особливо актуальним для України, де дефіцит спектральних ресурсів є однією з головних проблем. Зниження кількості перевантажених секторів на 45 % та покращення якості обслуговування для критичних сервісів на 18 % підкреслюють здатність запропонованих алгоритмів забезпечувати стабільну роботу мережі навіть у умовах високого навантаження.

Крім того, скорочення часу відновлення після відмов на 35 % демонструє підвищену стійкість та надійність мережі, що є критично важливим для забезпечення безперебійного надання послуг користувачам. Статистична обробка результатів показала високу стійкість отриманих показників, оскільки коефіцієнт варіації не перевищував 12 % для всіх ключових метрик, що свідчить про надійність та стабільність запропонованих методів.

Отже, результати моделювання підтверджують ефективність розроблених математичних моделей та алгоритмів оптимізації для розгортання мереж 5G в Україні. Запропоновані підходи дозволяють значно підвищити ефективність використання спектральних та серверних ресурсів, забезпечити ширше покриття території та покращити якість обслуговування користувачів. Це створює міцну теоретичну та практичну основу для подальшого впровадження 5G мереж в Україні, сприяючи розвитку цифрової економіки та підвищенню конкурентоспроможності на світовому ринку телекомунікацій.

Висновки. У результаті проведеного дослідження здійснено комплексний аналіз проблематики впровадження та масштабування мереж п’ятого покоління в Україні. Розроблено науково-методологічний апарат для вирішення ключових задач, пов’язаних з розгортанням мереж 5G, що включає: математичні моделі та алгоритми оптимізації розподілу радіочастотного спектра, розміщення базових станцій, імплементації технологій NFV/SDN та забезпечення диференційованої якості обслуговування. Запропоновані рішення враховують специфіку вітчизняного телекомунікаційного ринку та дозволяють підвищити ефективність використання обмежених ресурсів при розгортанні мереж 5G. Зокрема, розроблена модель оптимізації розподілу радіочастотного спектра на основі методів лінійного програмування, дозволяє максимізувати інтегральну ефективність використання спектрального ресурсу з урахуванням гетерогенності технологічних характеристик різних операторів. Це сприяє раціоналізації використання обмеженого частотного ресурсу в умовах його дефіциту. Запропонований підхід до оптимізації розміщення базових станцій, заснований на теоретико-ігровому моделюванні, дозволяє мінімізувати капітальні витрати операторів при забезпеченні необхідного рівня покриття.

Застосування апарату теорії ігор дозволяє врахувати конкурентної взаємодії між операторами та процесу знаходження оптимальних стратегій розміщення інфраструктурного обладнання.

Розроблена математична модель впровадження NFV/SDN враховує стохастичний характер трафіку в мережах 5G та оптимізує розміщення віртуалізованих мережевих функцій. Це сприяє підвищенню гнучкості та масштабованості мережевої інфраструктури, а також редукції операційних витрат.

Запропонована математична модель та варіант рішення алгоритму динамічного розподілу ресурсів для забезпечення диференційованої QoS різних класів трафіку, дозволяє ефективно управляти якістю обслуговування в умовах гетерогенності вимог до мережевих послуг у 5G.

Отримані результати формують науково-методологічну основу для планування та реалізації проєктів з впровадження 5G в Україні. Запропоновані моделі та алгоритми дозволяють операторам зв'язку оптимізувати процеси розгортання та експлуатації мереж 5G, підвищуючи ефективність утилізації ресурсів та якість надання послуг.

Практична значущість роботи полягає в можливості застосування розроблених підходів при плануванні мережевої інфраструктури, оптимізації розподілу частотного ресурсу та імплементації технологій віртуалізації в мережах 5G. Це може сприяти акселерації процесу впровадження 5G в Україні та підвищенню конкурентоспроможності вітчизняних операторів на глобальному ринку телекомунікацій.

Напрямком подальших досліджень є емпірична верифікація та розробка імітаційних моделей, запропонованих рішень для оцінки їх ефективності та потенційної модифікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shafi M., Molisch A. F., Smith P. J., Haustein T., Zhu P., De Silva P., Tufvesson F., Benjebbour A., Wunder G. 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice. IEEE Journal on Selected Areas in Communications. 2017. Vol. 35, No. 6. P. 1201–1221.

2. Dahlman E., Parkvall S., Skold J. 5G NR: The Next Generation Wireless Access Technology. Academic Press, 2022. 466 p.

3. Osseiran A., Monserrat J. F., Marsch P. 5G Mobile and Wireless Communications Technology. Cambridge University Press, 2021. 439 p.

4. Parkvall S., Dahlman E., Furuskar A., Frenne M. NR: The New 5G Radio Access Technology. IEEE Communications Standards Magazine. 2017. Vol. 1, No. 4. P. 24–30.

5. Holma H., Toskala A., Nakamura T. 5G Technology: 3GPP New Radio. Wiley, 2023. 448 p.

6. Agiwal M., Roy A., Saxena N. Next Generation 5G Wireless Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. 2018. Vol. 18, No. 3. P. 1617–1655.

7. Forge S., Blackman C., Bohlin R. The Role of 5G in Private Networks for Vertical Industries. European Commission, 2021. 51 p.

8. Xiao M., Mumtaz S., Huang Y., Dai L., Li Y., Matthaiou M., Karagiannidis G. K., Björnson E., Yang K., Chih-Lin I., Ghosh A. Millimeter Wave Communications for Future Mobile Networks. IEEE Journal on Selected Areas in Communications. 2017. Vol. 35, No. 9. P. 1909–1935.

9. Wu Y., Khisti A., Xiao C., Caire G., Wong K. K., Gao X. A Survey of Security and Privacy in 5G Networks: Challenges and Opportunities. IEEE Access. 2023. Vol. 6. P. 4850–4874.

10. Ahmad I., Kumar T., Liyanage M., Okwuibe J., Ylianttila M., Gurtov A. 5G Security: Analysis of Threats and Solutions. IEEE Communications Standards Magazine. 2021. Vol. 2, No. 1. P. 49–55.

11. Liyanage M., Ahmad I., Abro A. B., Gurtov A., Ylianttila M. A Comprehensive Guide to 5G Security. Wiley, 2023. 528 p.

12. Zhang H., Liu N., Chu X., Long K., Aghvami A., Leung V. C. M. Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges. IEEE Communications Magazine. 2023. Vol. 55, No. 8. P. 138–145.

13. Liang C., Yu F. R., Zhang X. Information-centric network function virtualization over 5G mobile wireless networks. IEEE Network. 2015. Vol. 29, No. 3. P. 68–74.

14. Oughton E. J., Frias Z., Russell T., Sicker D., Cleevely D. D. Towards 5G: Scenario-based assessment of the future supply and demand for mobile telecommunications infrastructure. Technological Forecasting and Social Change. 2022. Vol. 133. P. 141–155.

15. Chiaraviglio L., D'Andreagiovanni F., Lancellotti R., Shojafar M., Blefari-Melazzi N., Canali C. An approach to balance maintenance costs and electricity consumption in cloud data centers. IEEE Transactions on Sustainable Computing. 2018. Vol. 3, No. 4. P. 274–287.

16. Ordonez-Lucena J., Ameigeiras P., Lopez D., Ramos-Munoz J. J., Lorca J., Folgueira J. Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges. IEEE Communications Magazine. 2020. Vol. 55, No. 5. P. 80–87.

17. Mijumbi R., Serrat J., Gorricho J., Bouten N., De Turck F., Boutaba R. Network Function Virtualization: State-of-the-Art and Research Challenges. IEEE Communications Surveys & Tutorials. 2019. Vol. 18, No. 1. P. 236–262.

18. Обіход Т. В. Перспективи та недоліки 5G зв’язку в Україні / Т. В. Обіход // Інститут ядерних досліджень НАН України. Київ, 2023. DOI: 10.13140/RG.2.2.23786.70085.

19. Zhang H., Dong Y., Cheng J., Hossain M. J., Leung V. C. M. Fronthauling for 5G LTE-U Ultra Dense Cloud Small Cell Networks. IEEE Wireless Communications. 2016. Vol. 23, No. 6. P. 48-53.

20. Гнатюк С. О. Потенціал технологій 5G для відбудови та розвитку України: аналітична записка / С. О. Гнатюк // Національний інститут стратегічних досліджень, Центр безпекових досліджень. Київ: НІСД [Електронний ресурс].

21. Barakabitze A. A., Ahmad A., Mijumbi R., Hines A. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. Computer Networks. 2023. Vol. 167. 106984.

22. Бєляков Р. О. Концептуальна модель управління наземно-повітряною мережею MANET і FANET класів спеціального призначення / Р. О. Бєляков, О. Д. Фесенко // Вісник Херсонського національного технічного університету. 2024. № 1. DOI: 10.35546/kntu2078-4481.2024.1.28.

23. Конфендрат В. М. Порівняння моделей поширення радіохвиль в умовах міської забудови / В. М. Конфендрат, Д. О. Маковеєнко // Цифрові технології. 2020. № 27. С. 86–93 // Одеська національна академія зв’язку ім. О. С. Попова, Український науково-дослідний інститут радіо і телебачення. Одеса, 2020.

DOI: 10.58254/viti.6.2024.11.146

УДК 004.946.5

канд. техн. наук Міхєєв Ю. І. ORCID: 0000-0002-6239-2324 (НУОУ)
Павленко М. М. ORCID: 0000-0002-1011-5042 (ЖВІ ім. С. П. Корольова)
Лобода В. В. ORCID: 0000-0002-3535-0233 (ЖВІ ім. С. П. Корольова)
Войтко Т. М. ORCID: 0000-0002-4326-0633 (НУОУ)

ВИМОГИ ДО ПЕРСПЕКТИВНОГО КІБЕРОЗБРОЄННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Аналіз досвіду виконання завдань відповідними підрозділами Сил оборони України під час відбиття широкомасштабної збройної агресії російської федерації проти України свідчить про те, що отримання переваги в кіберпросторі можливе лише за наявності власної сучасної кіберзброї. Завдання зі створення кіберзброї передбачає розроблення вимог до неї. Актуальність цього завдання також підтверджується зростанням кількості кібератак на військові об'єкти з боку російської федерації, що відображено у звітах оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України за останні роки. Отже, метою статті є дослідження існуючих шляхів створення сучасного кіберозброєння в інтересах Збройних сил України та висування вимог до нього.

У статті наведені результати аналізу застосування кіберзброї та тенденції щодо її розвитку. Розглянуто класифікацію кіберзброї за принципом її застосування. Запропоновано складові кіберозброєння Збройних сил України, які ґрунтуються на підставі аналізу тактики дій хакерських угруповань, інформаційних загроз, спрямованих на Україну з боку російської федерації.

У статті зазначаються об'єкти (цілі), які мають вражати перспективне кіберозброєння Збройних сил України з врахуванням його цільового призначення та завдань. Серед основних об'єктів кібервпливу визначені: критична інфраструктура держави противника; системи бойового управління, системи (мережі) зв'язку та автоматизації противника; системи (платформи) управління зброєю та військовою технікою противника; інформаційні та медіаресурси противника; окремі персони (посадові особи); групи осіб, верстви населення противника.

Надано системні та функціональні і нефункціональні вимоги до перспективного озброєння видів Збройних сил України. Запропоновані результати досліджень, у подальшому, можуть стати підґрунтям для розроблення відповідних оперативно-тактичних вимог до перспективного кіберозброєння видів Збройних сил України.

Ключові слова: *кіберозброєння, кібератака, Збройні сили України, шкідливе програмне забезпечення, озброєння та військова техніка, оперативно-тактичні вимоги.*

Y. Mikhieiev, M. Pavlenko, V. Loboda, T. Voitko Requirements for advanced cyber weapons of the Armed Forces of Ukraine

An analysis of the experience of the relevant units of the Ukrainian Defense Forces in repelling the large-scale armed aggression of the Russian Federation against Ukraine shows that gaining an advantage in cyberspace is possible only if Ukraine has its own modern cyber weapons. The task of creating cyber weapons involves the development requirements for them. The relevance of this task is also confirmed by the growing number of cyberattacks on military facilities by the russian federation, as reflected in the reports of the Cyber Incident Response Center of the State Center for Cyber Defense of the State Service for Special Communications and Information Protection of Ukraine in recent years. Thus, the purpose of the article is to study the existing ways of creating modern cyber weapons in the interests of the Armed Forces of Ukraine and to put forward requirements for them.

In the article, results are presented of the analysis process regarding cyber weapons use and trends in their development. Classification of cyber weapons by principle is considered. Components of cyber weapons in the Armed Forces of Ukraine are proposed, based on the analysis tactics by hacker groups and information threats directed at Ukraine by the russian federation.

The article specifies the objects (targets) that should be hit by the advanced cyber weapons of the Armed Forces of Ukraine, taking into account their purpose and tasks. The main objects of cyber influence include: critical infrastructure of the enemy state; combat control systems, communication and automation systems (networks) of the enemy; systems (platforms) for controlling enemy weapons and military equipment; information and media resources of the enemy; individuals (officials); groups of individuals, segments of the enemy population.

The systemic and functional and non-functional requirements for advanced weapons of the Armed Forces of Ukraine are presented. The proposed research results can further serve as a basis for the development of relevant operational and tactical requirements for advanced cyber weapons of the Armed Forces of Ukraine.

Keywords: *cyber weapon, cyberattack, malware, Armed Forces of Ukraine, operational and tactical requirements.*

Постановка проблеми у загальному вигляді. Результати аналізу досвіду з питань кібербезпеки, що отриманий під час російсько-української війни, свідчить про зростання значущості кіберпростору для досягнення цілей військових операцій [1]. Об'єктами кібератак, з боку противника, здебільшого стали вебресурси урядових установ, міністерств, Збройних сил (ЗС) України, банків та інші об'єкти критичної інфраструктури нашої держави [2]. Враховуючи наслідки, які були спричинені кібератаками на Україну, актуальним постає завдання з організації відповідних контрзаходів у кіберпросторі та розроблення кіберзброї, яка може бути використана не тільки для захисту власних інформаційних ресурсів, а й для впливу на об'єкти противника під час проведення кібероперацій.

Тому актуальним постає завдання зі створення кіберзброї, яке передбачає розроблення відповідних вимог до неї.

Аналіз останніх публікацій. На сьогодні питанню забезпечення кібербезпеки держави та об'єктів критичної інфраструктури приділяється значна увага. Тенденція до збільшення кількості наукових публікацій та аналітичних дайджестів, у цій галузі, свідчить про наявність актуальних проблемних питань, вирішення яких ґрунтується на отриманому практичному досвіді під час російсько-української війни [1–4]. Разом з тим, питанню особливостей створення та розвитку кіберозброєння, а саме розробленню вимог до нього з метою подальшого розроблення та застосування кіберозброєння підрозділами видів ЗС України, приділено недостатньо уваги. У цьому аспекті існують проблеми, пов'язані з визначенням дефініцій поняття "кіберзброї", що зумовлено із певним періодом її постійної модифікації.

Так у [4] автором розглядаються особливості застосування кіберзброї з врахуванням норм міжнародного права. Зазначається її призначення та вказується, що кіберзброя є засобом ведення кібервійни. Однак вимоги щодо її використання саме у ЗС України не зазначаються.

У Військовому стандарті ВСТ 01.114.001 − 2023 (01) "Електромагнітна та кіберборотьба. Глосарій термінів і визначень" подано визначення кіберзброї, в якому стисло вказується її призначення, але вимоги, щодо її розроблення та сфери подальшого використання при цьому не зазначаються [5].

У [6] авторами приділено увагу питанню сутності та призначення кіберзброї, класифікації, характеристикам, базовим принципам її побудови. Класифікувати кіберзброю пропонується за наступними базовими ознаками: призначення; масштабність застосування; характер вражаючої дії; спосіб доставки; керованість; деструктивний вплив; оперативність; місце базування; рівень маскування; спосіб виготовлення; спектр дії; об'єкти ураження; рівень впливу на об'єкти ураження; прицільні властивості; інтегральний ефект; тип зв'язків та рівень взаємодії; наслідки; принцип генерування; самоорганізація; тривалість ефекту; латентність. Запропоновані підходи ґрунтуються на певній аналогії із відомим зразком озброєння. За такий зразок було обрано ракетоносій. Такий підхід, на нашу думку, не в повній мірі дозволяє створити підґрунтя для розроблення вимог до сучасного кіберозброєння.

Отже, **метою статті** є обґрунтування вимог до перспективного кіберозброєння ЗС України, що мають містити опис його складу, призначення, об'єкти, на які воно має бути спрямоване.

Виклад основного матеріалу дослідження

Кіберзброя набула активного розвитку в США. Це пов'язано із підтримкою керівництвом країни програм розвитку обчислювальних мереж військового призначення Arpanet [3]. Відповідно до керівних документів НАТО дії в кіберпросторі розглядаються на тактичному та стратегічному рівнях. Основна відмінність проведення дій на тактичному чи

стратегічному рівні полягає у виборі об'єктів для здійснення кібервпливу. На тактичному рівні – можуть виконуватися завдання з ускладнення чи часткового призупинення діяльності обраних об'єктів (телекомпаній, операторів стільникового зв'язку, провайдерів Інтернету, відомих локальних обчислювальних мереж тощо). На стратегічному рівні основними об'єктами впливу виступають державні структури та критичні об'єкти інфраструктури держав. З огляду на аналіз зафіксованих фактів впливу на об'єкти критичної інфраструктури країн Близького Сходу в країнах НАТО було запропоновано основний вид кіберзброї – шкідливе програмне забезпечення (ПЗ) основу якого становить комп'ютерний вірус [9].

Для встановлення цільового призначення перспективного кіберозброєння ЗС України, пропонується розглянути підхід до здійснення кібератаки за моделлю Cyber Kill Chain, яка складається з таких етапів [10] (рис. 1)

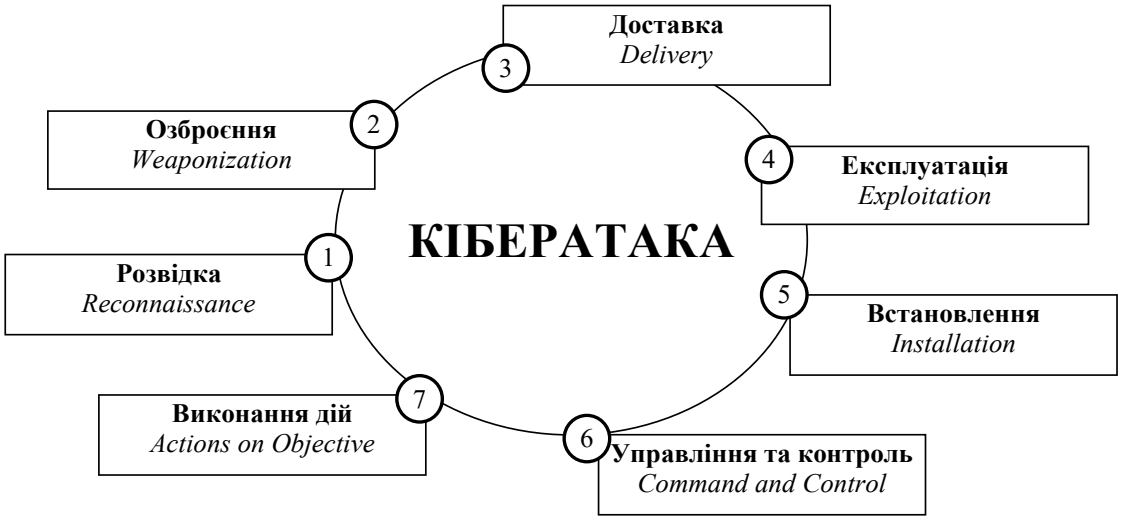


Рис. 1. Алгоритм здійснення кібератаки за моделлю Cyber Kill Chain

В алгоритмі здійснення кібератаки визначальними є етапи "розвідки" та "озброєння". На цих етапах визначаються вразливості об'єктів кібератак, проводиться підбір інструментарію, встановлюється механізм створення експлойтів та оснащення файлів шкідливим вмістом. Для максимального ефекту шкідливе ПЗ, яке створюється атакуючою стороною та застосовується під час кібератаки, має використовувати нові, раніше не виявлені вразливості (експлойти Zero-day). Враховуючи зазначене, пропонується таке цільове призначення перспективного кіберозброєння ЗС України:

збір інформації про об'єкти, на які планується здійснити вплив, під час проведення кіберрозвідки (несанкціонований доступ до інформації та даних);

виявлення уразливостей автоматизованих систем управління (АСУ) ЗС противника та інших об'єктів, які об'єднані комп'ютерною мережею;

вплив на визначені об'єкти ЗС противника (зміна, перешкодження або порушення функціонування інформаційних систем, здійснення кібератак, фішинг, розповсюдження вірусів, поширення дезінформації, вплив на громадську думку та маніпулювання подіями);

захист власних АСУ та персоналу від кібервпливу противника (запобігання атакам та забезпечення цілісності, конфіденційності та доступності інформації та ресурсів, ідентифікація потенційних ризиків та вразливостей в інфраструктурі, забезпечення сталого функціонування власних систем та інфраструктури).

Враховуючи цільове призначення та завдання, можна визначити такі об'єкти в якості цілей для перспективного кіберозброєння ЗС України:

критична інфраструктура держави противника;

системи управління військами (органи управління, системи зв’язку, інформаційні системи) видів та родів ЗС противника;

системи управління бойовими засобами противника;

інформаційні та медіаресурси противника;

окремі персони (посадові особи);

групи осіб, верстви населення противника;

тощо.

Пропонується об’єкти критичної інфраструктури держави противника, їх інформаційні та медіаресурси, верстви населення противника, розглядати цілями для усіх видів ЗС України. Основну відмінність для видів ЗС України будуть становити такі об’єкти (цілі):

елементи систем управління військами видів, родів, сфер діяльності ЗС противника (органи управління, системи зв’язку, інформаційні системи);

системи управління бойовими засобами противника зі складу систем управління військами;

окремі персони, посадові особи, що приймають рішення (групи осіб).

Окремими об’єктами впливу перспективного кіберозброєння, наприклад, Сухопутних військ (СВ) ЗС України, можуть бути:

1) системи управління СВ ЗС противника:

органи управління СВ ЗС;

системи зв’язку СВ ЗС;

інформаційні системи СВ ЗС;

2) системи управління бойовими засобами СВ ЗС противника:

системи дистанційного управління озброєнням та військовою технікою (ОВТ) СВ ЗС;

системи навігації ОВТ СВ ЗС;

канали телеметрії ОВТ СВ ЗС;

інші системи зі складу систем управління бойовими засобами, на які можливо здійснити вплив;

офіційні сайти СВ ЗС, акаунти соціальних мереж, електронні поштові скриньки особового складу СВ ЗС противника.

Для забезпечення виконання завдань з кіберрозвідки, кібервпливу, кіберзахисту, враховуючи цільове призначення, пропонується у складі перспективного кіберозброєння розглядати такі основні елементи: технічні засоби, програмне забезпечення та спеціальні програмні засоби впливу (шкідливе ПЗ) (рис. 2).

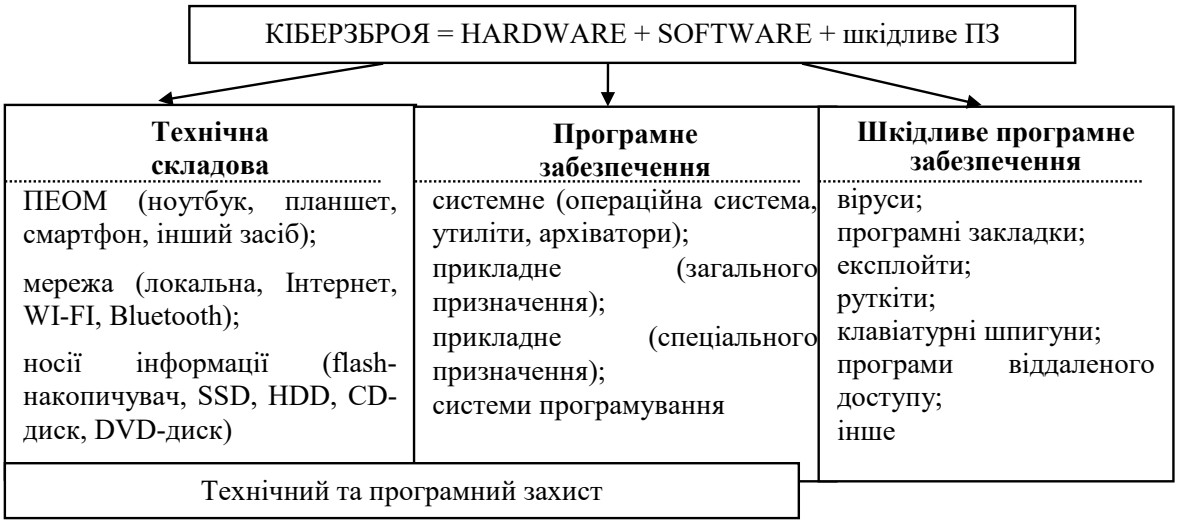


Рис. 2. Складові перспективного кіберозброєння

Запропонований склад перспективного кіберозброєння передбачає наявність універсальної структури та можливість використання для різних видів ЗС України. Відмінність буде полягати у формуванні складу шкідливого ПЗ, що визначатиметься об’єктами впливу.

До характеристик програмних компонентів кіберозброєння (SOFTWARE) пропонується віднести:

призначення;

принцип дії;

спосіб поширення;

обсяг файлу;

розмір програмного коду;

можливість самодублювання і самознищення;

алгоритм маскування;

тип операційної системи, яку здатен вражати бойовий програмний агент.

До характеристик апаратної частини кіберозброєння (HARDWARE) можна віднести системні вимоги: набір характеристик, яким повинен відповідати цифровий пристрій (обчислювальний засіб, комутаційний засіб, мобільний термінал); мережа або інформаційна система для коректної роботи програмного компонента перспективного кіберозброєння. Зазначені вимоги можуть описувати, як апаратне забезпечення, так і інше ПЗ (необхідні драйвери, операційна система тощо).

Під час розроблення вимог, слід розрізняти мінімальні та рекомендовані системні вимоги. Якщо мінімальні системні вимоги вказують, яка конфігурація системи цілковито необхідна для запуску ПЗ, то рекомендовані системні вимоги повинні вказувати на те, яка конфігурація здатна забезпечити повну функціональність кіберозброєння. Системні вимоги пропонується пов’язувати із такими характеристиками:

тип операційної системи, яка необхідна для запуску шкідливого ПЗ;

тип архітектури процесора, що виконує програмний код;

кількість дискового простору;

кількість оперативної пам’яті;

необхідність доступу до мережі (локальної або Інтернет);

наявність додаткових програмних та апаратних засобів, без яких функціонування шкідливого ПЗ неможливе.

Відповідно до специфікації Software Requirements Specification (SRS), які містять множину функціональних та нефункціональних (чи додаткових) вимог до ПЗ, пропонується визначити такі вимоги до перспективного кіберозброєння ЗС України [11]:

системні;

функціональні;

нефункціональні.

Системні вимоги:

використання сучасних ОС з останніми оновленнями безпеки;

використання апаратної архітектури x86-64 та ARM-архітектури (Advanced RISC Machine) як найбільш поширених;

підтримка багатопотоковості та розподіленості завдань з використанням багатоядерних процесорів;

застосування та підтримка сучасних інтерфейсів обладнання, інтерфейсів зв’язку та комунікацій;

підтримка можливості обміну даними через інтерфейси взаємодії (сучасні програмні інтерфейси);

можливість підключення до мережі, як за допомогою дротового способу, так і бездротовим дистанційним способом (наприклад, за допомогою пристрою Wi-Fi) із забезпеченням стабільного зв’язку з мережею за такими параметрами:

мінімальна пропускна здатність – 1 Мбіт/с;

рівень втрати цільових пакетів – не більше ніж 5% (1 пакетна втрата на 25 разів обміну пакетами);

рекомендована пропускна здатність – 100 Мбіт/с.

Прикладне ПЗ повинно базуватись на використанні вільно розповсюджувального ПЗ, яке не потребує придбання ліцензій. Також доцільно використовувати ПЗ, яке має відповідні ліцензії на використання.

Функціональні вимоги:

підтримка можливості розмежування прав доступу користувачів до відповідних функцій або системних ресурсів;

ергономічний та адаптивний інтерфейс, що забезпечує зручність і зрозумілість дій для оператора;

програмні компоненти повинні розроблятися за модульним принципом, тобто система складається з окремих модулів, кожен з яких реалізує певний набір функцій, притаманних виключно йому.

Передача інформації між складовими кіберозброєння має виконуватись стандартними протоколами на рівні ПЗ або на рівні платформи (системи керування базами даних, вебсерверів, тощо). У разі позаштатних ситуацій (аварій, відмов технічних засобів, зокрема, зникнення напруги, збоїв у роботі загальносистемного ПЗ, збоїв у роботі бази даних або інших технічних проблем) кіберозброєння повинне мати можливість відтворення своєї працездатності з резервних копій за короткий проміжок часу та з мінімальними втратами інформації.

Нефункціональні вимоги:

час готовності кіберозброєння до роботи – відповідно до інструкцій з експлуатації;

експлуатаційна документація повинна бути повна та достатня для забезпечення експлуатації, обслуговування кіберозброєння, виконана державною мовою.

Під час обміну інформацією між елементами кіберозброєння має бути забезпечено:

у незахищених каналах обміну даними – використання засобів криптографічного захисту інформації, які відповідають вимогам законодавства України у сфері криптографічного захисту інформації та забезпечують шифрування даних і взаємну автентифікацію сторін обміну даними;

у разі передачі інформації, що підлягає захисту відповідно до законодавства України у сфері захисту інформації (конфіденційної інформації (персональних даних, комерційної таємниці, державних інформаційних ресурсів тощо) до іншої системи – наявність у цій системі комплексної системи захисту інформації з підтвердженою у встановленому порядку відповідністю;

у разі необхідності формування та перевірки кваліфікованого електронного підпису на даних, обмін якими здійснюється використання засобів кваліфікованого електронного підпису чи печатки, які відповідають вимогам законодавства України у сфері електронних довірчих послуг.

Захист власних інформаційних ресурсів повинен реалізовуватися з використанням апаратних та програмних засобів захисту, що відповідають вимогам законодавства України у сфері захисту інформації, а також організаційних заходів, спрямованих на керування засобами захисту, регламентацію дій користувачів і контроль за цими діями. Кожен факт доступу до системи повинен зазначатись у протоколі доступу. Протокол доступу та протокол

дій оператора (log-файл) повинен бути доступний для перегляду та аналізу адміністратору системи, підрозділу, що відповідає за інформаційну безпеку.

Висновки і перспективи подальших досліджень

Отримані результати досліджень ґрунтуються на аналізі подій у кіберпросторі, які спостерігалися протягом 2014–2023 років під час російсько-української війни та відомостей, зазначених у звітах з питань кібербезпеки країн-членів НАТО. Це дало змогу визначити цільове призначення перспективного кіберозброєння, його склад, основні завдання та об'єкти (цілі) на які воно спрямовано.

Передбачається, що розроблення та застосування кіберозброєння, в інтересах ЗС України, буде пов'язано з такими особливостями:

низькою вартістю виробництва деяких складових елементів кіберзброї;

можливістю застосування кіберзброї з мінімальним рівнем ризику;

високою ефективністю кіберзброї в умовах використання противником АСУ;

масштабністю поширення кіберзброї;

комплексним використанням ключових можливостей кіберзброї для деструктивного впливу на об'єкти противника в кіберпросторі.

Тому, пропонується зосередити **подальші наукові дослідження** на обґрунтуванні оперативно-тактичних вимог кіберозброєння видів Збройних сил України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бойовий досвід з питань кібербезпеки отриманий під час російсько-української війни (аналіз та уроки). Частина перша (січень-травень 2022 року): збірник інформаційно-аналітичних матеріалів / С. А. Микусь, О. Й. Мацько, О. В. Войтко та ін. К.: НУОУ, 2022. 92 с.

2. Звіт оперативного центру реагування на кіберінциденти ДЦКЗ. URL: https://cip.gov.ua/ua/news/kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-46-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz (дата звернення: 20.10.2023).

3. Зміна тактик, цілей і спроможностей хакерських груп уряду рф та контрольованих ним угруповань: прогнози. URL: https://cip.gov.ua/ua/news/zmina-taktik-cilei-i-spromozhnostei-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-prognozi (дата звернення: 20.02.2023).

4. Білюга А. Д. Кіберзброя: сучасні загрози національній безпеці та шляхи протидії. Наука і оборона. 2021. № 2. С. 42–49.

5. ВСТ 01.114.001 – 2023 (01). Вид. 1. "Електромагнітна та кіберборотьба. Глосарій термінів і визначень".

6. Даник Ю. Г. Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник [Видання друге, перероб. та доп.]. Одеса: ОНАЗ ім. О. С. Попова, 2019. 320 с.

7. Arpanet. URL: https://www.quora.com/topic/ARPANET (дата звернення: 20.10.2023).

8. National Cybersecurity Strategy / The White House. Washington, 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата звернення: 20.03.2023).

9. Грищук Р. В. Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї // Сучасна спеціальна техніка. Київ, 2016. № 3 (46). С. 94–101.

10. Cyber Kill Chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата звернення: 08.09.2023).

11. IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications – Description. URL: https://ieeexplore.ieee.org/document/720574/definitions#definitions (дата звернення: 08.09.2023).

DOI: 10.58254/viti.6.2024.12.153

УДК 621.391.372

канд. техн. наук Остапчук В. М. ORCID: 0000-0001-5686-0198 (ГУЗ та КБ ГШ ЗСУ)
канд. техн. наук, ст. наук. співр. Масесов М. О. ORCID: 0000-0003-4537-4295 (ВІТІ ім. Героїв Крут)
Зінченко М. О. ORCID: 0000-0002-1428-8231 (ВІТІ ім. Героїв Крут)
Думітраш В. О. ORCID: 0000-0003-1996-3096 (ВІТІ ім. Героїв Крут)

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ТА ЗАСОБІВ ЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З УРАХУВАННЯМ ВПРОВАДЖЕННЯ МЕРЕЖ LTE

Подальший розвиток системи зв'язку Збройних Сил України неможливий без врахування отриманого передового бойового досвіду та поступового впровадження сучасних систем (комплексів, зразків) зв'язку для вирішення завдань, що стоять перед Силами оборони України. Тому ключовими постають питання не тільки вибору нових інформаційних технологій та сучасних стандартів у галузі комунікацій, але й дослідження щодо їх впровадження в умовах бойових (максимально наближених до бойових) дій.

Досвід виконання завдань на сході України, особливо під час наступальних (контрнаступальних) дій, чітко визначив проблеми забезпечення зв'язком на територіях, не підготовлених у відношенні зв'язку, а також на таких, де телекомунікаційна інфраструктура повністю або частково зруйнована. Метою статті є обґрунтування перспектив розвитку системи та засобів зв'язку спеціального призначення з урахуванням не тільки теоретичних досліджень у галузі радіозв'язку, але й результатів практичних досліджень ефективності системо-технічних рішень, що ґрунтуються на використанні радіообладнання стандартів стільникового зв'язку 3G та 4G.

За результатами досліджень сформовано висновки та пропозиції щодо перспектив подальшого впровадження системи, засобів та обладнання LTE в системі зв'язку Збройних Сил України. Зазначені пропозиції ґрунтуються на отриманих результатах отриманого досвіду використання зазначеного обладнання в інтересах забезпечення зв'язком військових частин (підрозділів) в Сумській області України, а також на лінії бойового зіткнення в умовах ведення наступальних (контрнаступальних) дій Сил оборони України на сході нашої Держави.

Наведений матеріал статті є актуальним та необхідним для врахування під час проведення досліджень, спрямованих на удосконалення форм і способів бойового застосування засобів (підрозділів) зв'язку, обґрунтування рішень щодо вибору необхідного комунікаційного обладнання, а також формування управлінських рішень органами військового управління щодо організації (забезпечення) зв'язку в майбутніх операціях з визволення тимчасово окупованих територій України.

Ключові слова: *система зв'язку, комунікації, радіообладнання, стільниковий зв'язок, LTE (Long-Term Evolution), бойовий досвід.*

V. Ostapchuk, M. Masesov, M. Zinchenko, V. Dumitrash Prospects for the development of the communication system and the equipment of special purpose with the regulation of the implementation of measures LTE

Further development of the communication system of the Armed Forces of Ukraine is impossible without the recovery of advanced combat experience and the step-by-step implementation of current communication systems (complexes, equipment) for the highest task to face the Defense Forces of Ukraine. Therefore, the key is not only the selection of new information technologies and current standards in the field of communication, but also the investigation of their implementation in the minds of combatants (as close as possible to the combative ones) of action.

Experience in carrying out tasks in the east of Ukraine, especially during offensive (counter-offensive) operations, clearly identifying the problems of securing communications in territories not prepared for communications, as well as in areas where telecommunications infrastructure is completely or partially destroyed. The purpose of this article is to outline the prospects for the development of the communication system and the equipment of special purpose with the understanding of not only theoretical research in radio communications, but also the results of practical research into the effectiveness of system-technical solution based by installed on the local radio station with mobile communication standards 3G and 4G.

Based on the results of the research, conclusions and proposals were formed regarding the prospects for further development of the system, including the use of LTE in the communication system of the Armed Forces of Ukraine. The stated propositions are based on the results of the final experience of the assigned possession in the interests of the security of military units (subdivisions) in the Sumy region of Ukraine, as well as on the combat line the focus on the offensive (counter-offensive) actions of the Defense Forces of Ukraine in the east of our State.

The presentation material of the article is relevant and necessary for training during the research, aimed at improving the forms and methods of combat stagnation of communication equipment (units), tying the decision to choose

necessary communication equipment, as well as the formation of management decisions by military administration bodies to organize (secure) connections in future operations with the release of the immediate occupation of the territories of Ukraine.

***Keywords**: communication system, communications, radio equipment, cellular communication, LTE (Long-Term Evolution), combat experience.*

Постановка проблеми

Досвід виконання завдань на сході України показав значні проблемні питання організації та забезпечення зв’язку під час наступальних (контрнаступальних) дій Сил оборони України в умовах, коли телекомунікаційна інфраструктура території, на якій виконують бойові завдання військові частини (підрозділи) Збройних Сил України, повністю або частково зруйнована.

Зазначені проблемні питання стосуються не тільки забезпечення безпосередньо зв’язком особового складу, командирів (начальників) та військових структур (наприклад, військових комендатур), але й забезпечення функціонування систем, що розгортаються – електроживлення, передавання та розподіл телекомунікаційних ресурсів, забезпечення життєдіяльності особового складу, охорона та оборона об’єктів зв’язку, тощо.

В зазначених умовах фактично відсутня (зруйнована) транспортна опорна мережа зв’язку, прокладання нових кабельних ліній вимагає значного часового ресурсу, тому більшість зв’язків забезпечується радіозасобами. Ситуацію може значно ускладнювати складна електромагнітна обстановка безпосередньо на лінії бойового зіткнення, постійний вплив засобів радіоелектронної боротьби противника, неможливість забезпечення зв’язком з використанням терміналів супутникового зв’язку Starlink на певних територіях, в тому числі на території рф.

Таким чином, постає проблема визначення подальших перспектив розвитку системи зв’язку спеціального призначення у зазначених умовах для організації та забезпечення зв’язку в інтересах Сил оборони України під час наступальних (контрнаступальних) дій.

Аналіз останніх досліджень і публікацій

Дослідження з наведеної тематики проводились різними авторами, в тому числі – науковими співробітниками наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, що відображені в публікаціях [1–3]. В роботах [1, 2] акцент зроблено на використанні сучасних засобів військового радіозв’язку іноземного виробництва. Зазначені засоби та обладнання військового призначення відповідають сучасним вимогам системи управління військами (силами), але їх кількість у Збройних Силах України залишається незадовільною (особливо в тактичній ланці управління), а номенклатура продовжує збільшуватись, що, в свою чергу, призводить до “зоопарку” засобів радіозв’язку на полі бою та проблем з їх взаємосумісністю, особливо в захищених режимах роботи.

В роботі [3] авторами робиться спроба узагальнити підхід щодо забезпечення розвитку військової техніки, в тому числі – засобів (систем, комплексів) зв’язку, з використанням досвіду провідних країн світу. Нарешті, в роботі [4] наведені результати досліджень досвіду впровадження технологій стільникового зв’язку в окремих військових частинах (підрозділах) Сил оборони України, які виконують бойові завдання на сході України. В той же час, в роботі [4] відсутні пропозиції щодо подальшого розвитку (впровадження) таких систем (мереж) у Збройних Силах України.

Мета статті

Метою статті є обґрунтування практичних рекомендацій щодо вибору, впровадження та використання комунікаційного радіообладнання, побудови та експлуатації відповідної

побудованої радіомережі системи зв’язку з використанням обладнання стільникового зв’язку з урахуванням набутого бойового досвіду та результатів практичних перевірок технічних характеристик радіоканалів. Представлені в роботі результати будуть корисними для фахівців та посадових осіб органів військового управління для обґрунтування технологічних рішень при побудові мереж (систем) зв’язку спеціального призначення. Крім того, матеріал буде корисним науковцям та здобувачам, які здійснюють наукові дослідження в галузі стільникового (радіо) зв’язку.

Виклад основного матеріалу дослідження

Для досягнення мети статті авторами пропонується використання досвіду розгортання та функціонування мережі зв’язку, побудованої за принципом стільникових мереж, в інтересах забезпечення функціонування системи зв’язку Сил оборони України.

Зазначений досвід ґрунтується на забезпеченні передачі даних (без голосового зв’язку) з використанням абонентських пристроїв типу смартфон, планшет, мобільний роутер, USB-модем, які підключаються до власної (приватної) мережі стільникового зв’язку з використанням спеціальних SIM-карток.

Досвід впровадження таких мереж в Збройних Силах України показав спроможність забезпечувати передачу даних (повідомлення, фото, відео, телефонія), в тому числі – для забезпечення роботи інформаційних (автоматизованих) систем (систем ситуаційної обізнаності).

Для простоти розуміння функціонування таких систем в інтересах Сил оборони України, доцільно умовно поділити мережу на такі складові: ядро мережі, базові станції мережі, транспортна інфраструктура, абонентське обладнання.

В якості абонентського обладнання, як зазначено вище, можна використовувати звичайні смартфони (модеми, роутери, планшети), які підтримують відповідні стандарти зв’язку та відповідні діапазони робочих частот базових станцій.

Залежно від стандарту зв’язку, діапазону частот, ширини робочої смуги частот, висоти підняття антен базової станції, кількості одночасно працюючих абонентів та ,звичайно, рельєфу місцевості і електромагнітної обстановки, – може бути забезпечена дальність зв’язку від базової станції до абонента до 2–5 км та швидкості передачі даних на абонентському пристрої порядку одиниць – десятків Мбіт/сек (при забезпеченні прямої радіовидимості).

Узагальнений графік залежності пропускної спроможності на абонентському терміналі від віддаленості до базової станції наведено на рис. 1.

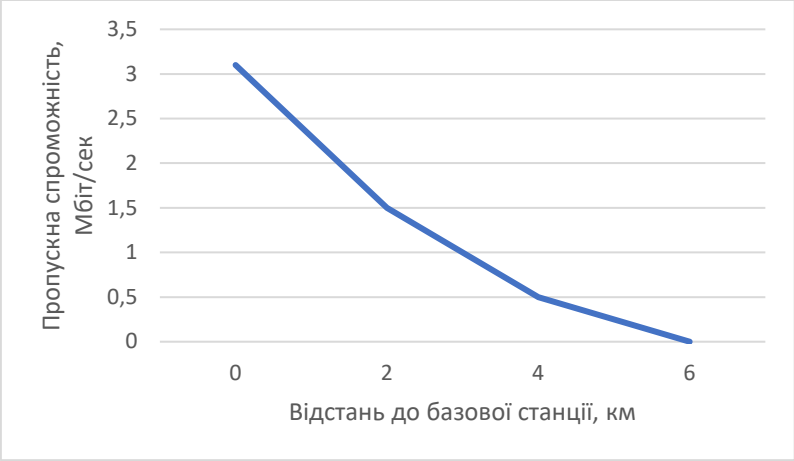


Рис. 1. Графік залежності пропускної спроможності від віддаленості до базової станції

Отриманий характер залежності (рис. 1) підтвердив загальну тенденцію зменшення пропускної спроможності із збільшенням відстані до базової станції.

Для покращення характеристик дальності зв’язку та швидкості передачі даних за досвідом виконання завдань доцільно використовувати додаткове обладнання типу Mikrotik SXT LTE6 kit та Mikrotik LHGG LTE6 kit, зовнішній вигляд якого наведений на рис. 2.

Рис. 2. Зовнішній вигляд додаткового обладнання типу Mikrotik SXT LTE6 kit (ліворуч), Mikrotik LHGG LTE6 kit (праворуч)

Наведені варіанти додаткового обладнання використовують антенну технологію MIMO, мають вбудовані підсилювачі потужності передавача та значно покращені характеристики направленості антени. Зазначені переваги дозволяють значно збільшити дальність зв’язку та швидкість (upload) передачі даних (рис. 3). Крім того, додаткових пристроїв для юстування антенного обладнання не потрібно, а саме обладнання можна підняти на невелику висоту (декілька метрів) або винести з укриття із забезпечення живлення та передачі даних за технологією PoE.

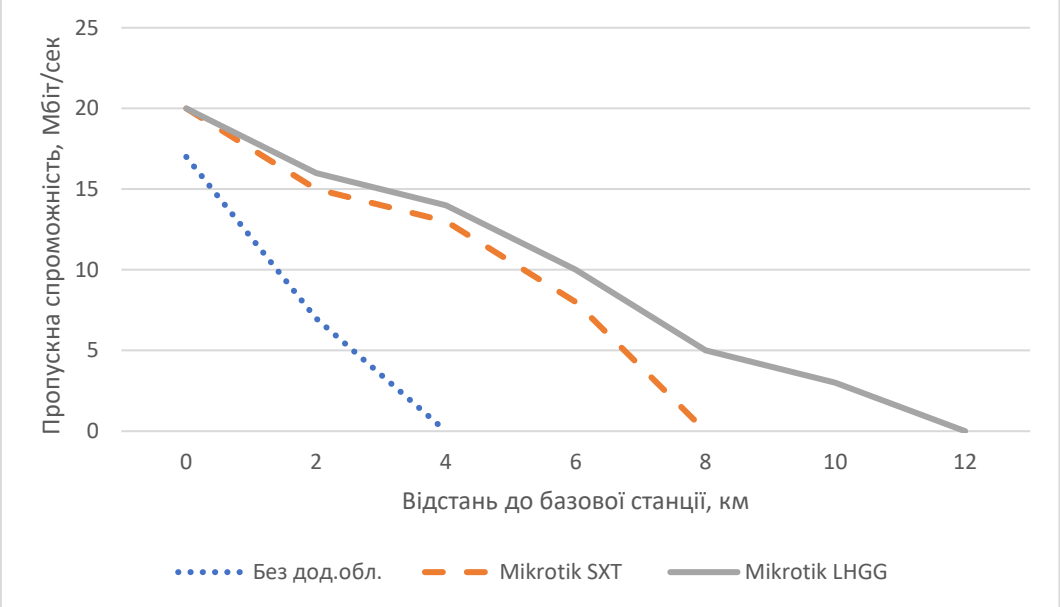


Рис. 3. Графіки залежності пропускної спроможності від відстані до базової станції для кінцевих пристроїв без додаткового антенного обладнання та з додатковим обладнанням типу Mikrotik SXT LTE6 kit та LHGG LTE6 kit

В якості недоліків застосування додаткового обладнання слід зазначити необхідність забезпечення додаткового електроживлення, а також наявні демаскуючі ознаки через габарити обладнання (кабелю, антени та щогли).

Наступним структурним елементом мережі є базові станції. В свою чергу, в склад типової базової станції входить:

антенно-щоглове обладнання з комплектом кабелів;

приймально-передавальне обладнання (з підсилювачем потужності);

нижній блок BBU (Base Band Unit);

маршрутизатор;

блок (джерело) живлення (48 В, 50 А для забезпечення живлення BBU, маршрутизатора та підсилювачів потужності).

Конкретні типи та виробники обладнання базової станції можуть бути обрані за умов наявності та підтримки необхідного стандарту роботи мережі.

За досвідом виконання завдань, в якості щоглового обладнання найчастіше використовуються стаціонарні об’єкти концерну радіомовлення, радіозв’язку та телебачення, які в свою чергу дозволяють розмістити обладнання на значній висоті та забезпечити максимальний радіус радіопокриття.

В той же час, досвід виконання завдань із забезпечення зв’язку на територіях, де транспортна інфраструктура зруйнована повністю або частково, показав доцільність використання також мобільних базових станцій на рухомій базі, що розгорнуті з використанням телескопічних та/або секційних щогл. Зазначений підхід дозволить забезпечити зв’язок у важкодоступних районах, покращити якість радіопокриття в умовах відсутності такого від стаціонарних веж, а також забезпечити зв’язок за принципом “тут і зараз” в умовах швидкоплинності ведення бойових дій, особливо наступальних (контрнаступальних). Зовнішній вигляд типової базової станції, розгорнутої на рухомій базі, наведено на рис. 4.

Рис. 4. Зовнішній вигляд (варіант) рухомої базової станції мережі LTE

Діаграма направленості антенного обладнання базової станції залежить від кількості підключених антен (2 або 3) і може складати до 360 градусів. Кількість одночасно працюючих

абонентських терміналів (з SIM-картами) в зоні обслуговування однієї базової станції відповідно до її спроможностей може становити декілька сотень пристроїв (в стандартах 3G або 4G). Швидкість підключення кожного пристрою в такому випадку залежатиме від швидкості підключення базової станції до транспортної мережі.

В свою чергу, підключення базової станції до транспортної мережі здійснюється з використанням проводових та радіорелейних засобів. Особливо важливим при цьому є забезпечення якості підключення з достатньою швидкістю та мінімальним часом затримки (ping). За досвідом виконання завдань, базові станції також можна підключати з використанням терміналів супутникового зв’язку (типу Starlink) та засобів тропосферного зв'язку. В останньому випадку значно зростає час затримки сигналів (ping), що також стає нестабільним через особливості поширення сигналів у тропосфері, що в свою чергу, може негативно вплинути на роботу інформаційних (автоматизованих) систем та засобів криптографічного захисту інформації, що є критичними до зазначених характеристик каналу.

Завдання розгортання базових станцій покладається на спеціально підготовлений екіпаж (мінімум 2–3 особи), який спроможний розгорнути антенно-щоглове обладнання, підключити заздалегідь підготовлені (налаштовані) приймально-передавальні пристрої та нижній блок, а також розгорнути систему електроживлення базової станції з резервуванням.

Для забезпечення стабільного електроживлення базової станції крім стаціонарної мережі електроживлення доцільно використовувати резервні джерела електроживлення – мобільні генератори, зарядні станції та блоки безперебійного живлення (UPS).

Швидкість розгортання базових станцій (за досвідом виконання завдань) залежить від умов бойової обстановки, навченості особового складу та наявного комплекту обладнання.

Після розгортання базової станції, для забезпечення її охорони, оборони і обслуговування доцільно визначати екіпаж чергової обслуги.

Найбільш складною та такою, що вимагає постійного цілодобового моніторингу та налаштування, є ядро мережі. Саме ядро мережі призначено для обробки та маршрутизації IP-трафіку між користувачами та сервісами мережі, а також автоматичного налаштування робочих частот базових станцій в одній мережі.

За досвідом виконання завдань, ядро мережі повинно бути розгорнуто на значній відстані від безпосередніх районів ведення бойових дій, мати незалежне підключення як мінімум до двох операторів комунікацій, стабільне джерело електроживлення з резервуванням. Крім того, для забезпечення безперебійного обслуговування абонентів та доступу їх до інформаційних ресурсів доцільно забезпечити як мінімум подвійне “гаряче” резервування ядра мережі з виконанням вищезазначених вимог до кожного ядра.

Моніторинг і управління мережею доцільно здійснювати з автоматизованого робочого місце чергової зміни з доступом до ядра мережі.

Мінімальний перелік можливостей персоналу, що здійснює управління роботою мережі з доступом до ядра, включає:

реєстрацію, підключення та блокування абонентів у мережі (за SIM-карткою);

моніторинг працездатності базових станцій (з використанням, наприклад, Zabbix);

моніторинг працездатності та керування лініями зв’язку, що з’єднують базові станції;

віддалене налаштування мережевого обладнання;

вимірювання окремих характеристик підключення базових станцій (затримку, статистику підключення (за визначений період часу), статистику об’єму трафіку, перезавантаження базових станцій та ядра, тощо.

Критично важливим, за досвідом виконання завдань, при цьому стає фізичне “володіння” ядром мережі саме підготовленим особовим складом Сил оборони України, що максимально знизить (унеможливить) ризики несанкціонованого доступу до ресурсів мережі, дозволить

здійснювати цілодобовий моніторинг та налаштування мережі, контролювати та надавати (блокувати) доступ абонентів, тощо.

В рамках проведених досліджень неможливо обійти питання необхідності побудови транспортної інфраструктури, що об’єднує базові станції у єдину мережу. Як було зазначено, підключення базових станцій до транспортної мережі можливо здійснювати з використанням: волоконно-оптичних ліній зв’язку; проводових (мідних) ліній зв’язку; радіорелейних ліній зв’язку (в тому числі – організованих з використанням обладнання типу AirFiber або радіозасобів типу HARRIS RF-7850W); станцій (терміналів) супутникового зв’язку (типу Starlink, Tooway, Satcube); станцій тропосферного зв’язку.

Основними вимогами для підключення базової станції при цьому стають необхідна пропускна спроможність та характеристика затримки сигналів в каналі. Зазначене, в свою чергу, визначає кількість можливих підключень абонентських пристроїв на необхідній швидкості із заданою якістю передачі інформації.

Висновки і перспективи подальших досліджень

За результатами проведених досліджень, для забезпечення зв’язком Сил оборони України побудовані додаткові сегменти мереж за принципом стільникових мереж зв’язку.

В межах покриття розгорнуті мережі забезпечують передавання текстової, графічної, аудіо-відеоінформації для кінцевих користувачів (зі стільникових телефонів та інших мобільних комунікаційних пристроїв), використовуються відомі стандарти та діапазони частот стільникового зв’язку, що дозволяє забезпечити розвідзахищеність мереж. Таким чином, розгорнуті мережі можуть стати незамінним інструментом для забезпечення передачі інформації в прифронтових територіях, створення інфраструктури в непідготовлених (у відношенні зв’язку) районах виконання завдань.

З урахуванням вищезазначеного, за результатами проведених практичних досліджень обладнання, розроблено наступні пропозиції щодо розвитку (удосконалення) мереж, побудованих за принципом стільникових:

1. Для забезпечення зв’язком в наступальних (контрнаступальних) операціях сил оборони України під час визволення тимчасово окупованих територій, а також проведення операцій на окремих напрямках – сформувати мобільні підрозділи для розгортання базових станцій мережі на мобільній базі (автомобілі підвищеної прохідності з телескопічними щоглами, антенні машини з секційними щоглами). Базові станції на мобільній базі використовувати додатково до розгорнутої стаціонарної інфраструктури.

На зазначені мобільні підрозділи покласти завдання оперативного виходу та розгортання у визначеному районі базових станцій мережі для забезпечення управління передовими Силами оборони України.

2. Для підвищення стійкості роботи мережі доцільно впроваджувати резервне ядро мережі (територіально рознесене, підключене до іншого оператора по іншій фізичній лінії зв’язку, на іншій лінії електроживлення), яке повністю дублюватиме можливості основного ядра та постійного знаходитись в режимі “гарячої” заміни. Крім того, для забезпечення автономності кожної окремої базової станції доцільно використовувати в якості резерву ядро мережі на тактичному рівні в інтересах визначеної військової частини (тактичної групи).

3. Для забезпечення більш якісного покриття базових станцій мережі доцільно використовувати обладнання з випромінюванням в декількох діапазонах частот (від 700 МГц до 2100 МГц), що також надасть можливість адаптованої зміни робочих частот при подавленні певних ділянок частот засобами радіоелектронної боротьби противника.

4. В місцях нестійкого прийому сигналу мережі доцільно використовувати додаткове обладнання типу точок доступу та/або антенного обладнання з направленими антенами.

Одним із **напрямів подальших досліджень** є практичні випробування різних стандартів стільникового зв’язку з метою формування пропозицій щодо вибору та забезпечення стійкості роботи мережі в умовах навмисних радіоперешкод.

Перспективними також є дослідження у напряму розробки базових станцій повітряного базування на базі безпілотних літальних апаратів – ретрансляторів з обов’язковою перевіркою їх функціональних можливостей і тактико-технічних характеристик мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лаврут О. О., Климович О. К., Тарасюк М. Л., Антонюк О. Л. Стан та перспективи застосування сучасних технологій та засобів радіозв’язку в Збройних Силах України. *Системи озброєння та військова техніка*. 2017. № 1 (49). С. 42–49.

2. Лаврут О. О., Лаврут Т. В., Климович О. К., Здоренко Ю. М. Новітні технології та засоби зв’язку у Збройних Силах України: шлях трансформації та перспективи розвитку. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. № 1 (34). С. 91–101. URL: https://doi.org/10.30748/nitps.2019.34.13.

3. Радзівілов Г. Д., Масесов М. О, Дєгтяр О. А. Світові тенденції зі створення та розвитку військової техніки. *Комп’ютерно-інтегровані технології: освіта, наука, виробництво*. 2024. Випуск № 56. С. 381–385. DOI: https://doi.org/10.36910/6775-2524-0560-2024-56-45.

4. Лазута Р. Р. та ін. Військова навчально-методична публікація щодо застосування технології LTE (4G) системи зв’язку у військових частинах Збройних Сил України. *Матеріали вивчення бойового досвіду застосування Збройних Сил України*. Київ: НЦЗІ ВІТІ. 20 с.

DOI: 10.58254/viti.6.2024.13.161

УДК 621.3:623.4:629.07-044.4

канд. техн. наук Панченко І. В. ORCID: 0000-0001-5690-3813 (ВІТІ ім. Героїв Крут)
Бернацький А. П. ORCID: 0000-0003-0379-075X (ВІТІ ім. Героїв Крут)
Сердюк П. Є. ORCID: 0000-0002-5497-456X (ВІТІ ім. Героїв Крут)

БАГАТОФУНКЦІОНАЛЬНИЙ ВІЙСЬКОВИЙ СИМУЛЯТОР КЕРУВАННЯ МОБІЛЬНИМ РОБОТОМ З FPV ТА СИСТЕМОЮ ЗВОРОТНОГО ЗВ'ЯЗКУ

Активний розвиток в останнє десятиліття мобільної та автономної робототехніки сприяє пошуку можливостей їх застосування та вирішення завдань у галузі "Військова справа, національна безпека, безпека державного кордону".

В дослідженні наведена класифікація, розглянуті сучасні аспекти та стан військових симуляторів в світі. Проведений аналіз використання технологій сучасних військових симуляторів, що застосовуються в Україні для забезпечення максимально реалістичного та ефективного навчання військовослужбовців, та наведені приклади використання військових симуляторів в Україні.

В процесі опису багатофункціонального військового симулятора керування мобільним роботом з FPV та системою зворотного зв'язку, надана цільова функція зворотного зв'язку, та визначена важливість використання математичного апарату для побудови пристрою симуляції.

В роботі надані схеми та режими роботи багатофункціонального військового симулятора керування мобільним роботом з FPV та системою зворотного зв'язку.

При написанні висновків вказані, що важливим фактором сучасності є, інтеграція нових технологій. Майбутні військові симулятори обов'язково можуть включати ряд нових технологій, які ще більше підвищать їхню ефективність та реалістичність.

Ключові слова: *автономний робот, військовий, дослідження, дрон, методи, симулятор, VR, FPV, БпНЗ, БпЛА.*

I. Panchenko, A. Bernatskyi, P. Serdiuk A multi-functional military simulator of controlling a mobile robot with FPV and a feedback system.

The active development of mobile and autonomous robotics in the last decade contributes to the search for opportunities for their application and solving tasks in the field of "Military Affairs, National Security, State Border Security".

The study provides a classification, considers modern aspects and the state of military simulators in the world. An analysis of the use of modern military simulator technologies used in Ukraine to ensure the most realistic and effective training of military personnel is carried out, and examples of the use of military simulators in Ukraine are given.

In the process of describing a multi-functional military mobile robot control simulator with FPV and feedback system, the target feedback function is provided, and the importance of using a mathematical apparatus to build a simulation device is determined.

The work provides schemes and modes of operation of a multifunctional military simulator of controlling a mobile robot with FPV and a feedback system.

When writing the conclusions, it is indicated that an important factor of modernity is the integration of new technologies. Future military simulators are sure to include a number of new technologies that will further enhance their effectiveness and realism.

Keywords: *autonomous robot, research, drone, methods, military, simulator, FPV, VR, UGV, UAV.*

Постановка завдання. Активний розвиток в останнє десятиліття мобільної та автономної робототехніки сприяє пошуку можливостей їх застосування та вирішення завдань у галузі "Військова справа, національна безпека, безпека державного кордону".

Симулятори є потужним інструментом для навчання та підготовки, забезпечуючи безпечне середовище для практики та розвитку навичок [1].

У військовій підготовці, симулятори відіграють критичну роль, забезпечуючи безпечне, ефективне та економічно вигідне середовище для навчання військовослужбовців. Вони дозволяють користувачам набувати практичних навичок і розвивати критичне мислення в безпечному та контрольованому середовищі. Застосування систем симуляції має важливі критерії такі як [2]:

Безпека. Симулятори дозволяють військовослужбовцям тренуватися в умовах, максимально наближених до бойових, без ризику для життя та здоров'я;

Ефективність навчання. Використання симуляторів дозволяє військовим отримувати реалістичний досвід, що сприяє кращому засвоєнню матеріалу та розвитку необхідних навичок.

Економія ресурсів. Симулятори дозволяють зменшити витрати на навчання, оскільки вони знижують потребу у використанні дорогого обладнання, боєприпасів та інших ресурсів;

Стандартизація процесів. Симулятори забезпечують стандартизоване навчання, що дозволяє всім військовослужбовцям отримувати однаковий рівень підготовки незалежно від місця проведення тренувань;

Моделювання складних сценаріїв. Симулятори дозволяють моделювати складні бойові сценарії, включаючи ті, що враховують політичні та соціальні фактори.

В сучасному вимірі систем симуляцій існує кілька основних типів симуляторів, кожен з яких має свої особливості та застосування:

Реальні симулятори (Live simulations). Включають реальних людей, які працюють з реальними системами. Цей тип симуляції використовується для відпрацювання реальних операцій в умовах, максимально наближених до реальних;

Віртуальні симулятори (Virtual simulations). Включають реальних людей, які працюють з віртуальними системами. Вони використовуються для відпрацювання моторних, комунікаційних та інших навичок у віртуальному середовищі;

Конструктивні симулятори (Constructive simulations). Включають віртуальних людей, які працюють з віртуальними системами. Реальні люди можуть робити вхідні дані, але не беруть участі у визначенні результатів. Цей тип симуляції часто використовується для моделювання великих систем або процесів.

Ігрові симулятори (Gaming simulations). Використовуються для навчання через ігрові сценарії, що дозволяють користувачам взаємодіяти з віртуальним середовищем у формі гри.

Задля військового застосування існує декілька базових типів симуляторів, кожен з яких має свої особливості. Наведемо загальну класифікацію військових симуляторів (рис. 1) [3].

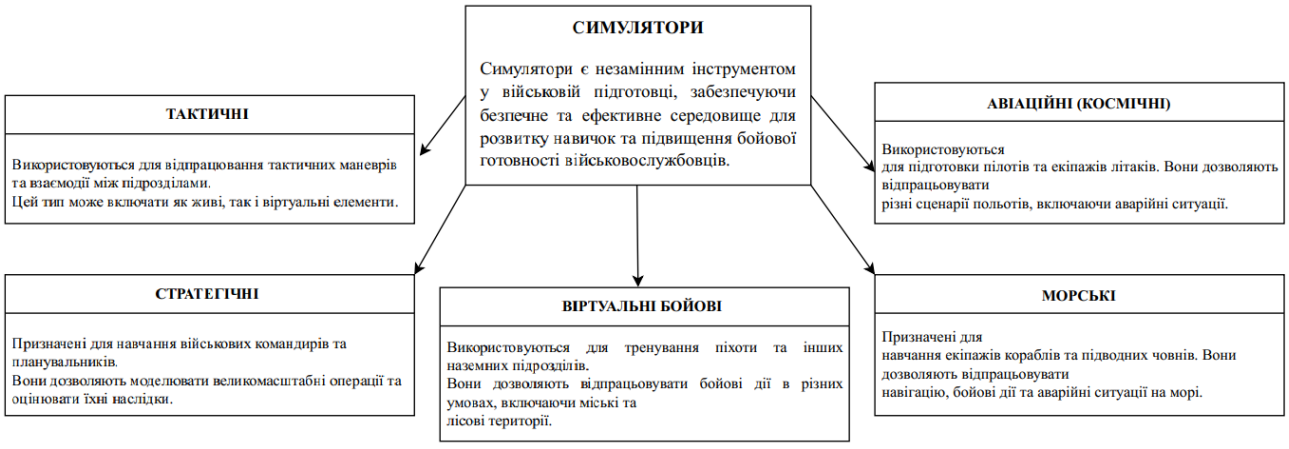


Рис. 1. Загальна класифікація військових симуляторів (адаптоване автором)

В Україні використовуються різноманітні військові симулятори для підготовки військовослужбовців. Наведемо декілька прикладів:

Віртуальний бойовий простір (Virtual Battlespace) використовується в навчальних центрах, таких як "Десна" та Центр імітаційного моделювання в Яворові. Він дозволяє від 10 до 200 осіб одночасно брати участь у віртуальних бойових діях, використовуючи комп'ютери або симулятори певного виду зброї;

Українська компанія Skiftech виробляє лазерні тактичні симулятори для піхоти, артилерії, мінометів, ПТРК, ПЗРК, а також військової техніки, включаючи танки, БТР та БМП. Ці симулятори дозволяють військовим відпрацьовувати різні бойові сценарії в умовах, максимально наближених до реальних [6];

Logics7 розробила понад 30 видів симуляторів для різноманітної зброї, включаючи Т-80 танк, БМП-2 бойову машину піхоти, РПГ-7 та РПГ-22 протитанкові гранатомети (рис. 2), а також пістолети Макарова та штурмові гвинтівки. Ці симулятори використовуються для навчання військових правильній виправки, диханню, поводженню зі зброєю, прицілюванню та плавному натисканню на спусковий гачок під час бойових маневрів [7]

В серпні 2023 року Чехія передала Україні симулятор для підготовки пілотів до роботи на літаках західного зразка F-16. Цей симулятор дозволяє українським військовим вивчати особливості та можливості сучасної техніки без необхідності використовувати реальні літаки [8];

Рис. 2. Симулятор UNITS для підготовки військових. (Фото: Компанія Logics7)

Українські військові використовують симулятори для навчання на протитанкових ракетних комплексах Javelin та переносних зенітно-ракетних комплексах Stinger. Ці симулятори дозволяють військовим відпрацьовувати навички стрільби та управління цими системами без використання дорогих боєприпасів [6];

Компанія "Інтерактивні системи плюс" пропонує інтерактивні лазерні стрілецькі тренажери, призначені для навчання військових із Збройних Сил України. Вони дозволяють відпрацьовувати стрільбу з різних видів зброї в умовах, максимально наближених до реальних [9].

Ці симулятори є важливим інструментом для підготовки українських військових, забезпечуючи безпечне та ефективне середовище для розвитку необхідних навичок та підвищення бойової готовності.

Розглядаючи технологічність сучасних військових симуляторів, що застосовуються в Україні, необхідно зазначити використання різноманітних передових технології для забезпечення максимально реалістичного та ефективного навчання військовослужбовців, а саме [10, 11]:

Технології *віртуальної реальності (VR)* дозволяють створювати повністю занурюючи середовища, де військові можуть тренуватися в умовах, максимально наближених до реальних бойових дій;

Застосування технологій лазерного променю в симуляторах для відпрацювання стрільби та тактичних маневрів. Вони дозволяють точно моделювати траєкторії куль та інші балістичні характеристики зброї. Як розширення лазерної технології, є системи M.I.L.E.S (Multiple Integrated Laser Engagement System): Такі системи використовують лазерні технології для моделювання двостороннього вогневого контакту, що дозволяє військовим відпрацьовувати тактичні маневри та взаємодію між підрозділами в умовах, максимально наближених до реальних бойових дій;

Для відтворення реалістичних характеристик зброї та бойових умов використовуються *складні математичні моделі*. Це дозволяє симуляторам точно відображати фізичні властивості та поведінку різних видів зброї;

Технології *доповненої реальності (AR)* використовуються для накладання віртуальних елементів на реальний світ, що дозволяє військовим тренуватися в реальних умовах з додатковими віртуальними об’єктами. Це може включати віртуальні мішені, індикатори та інші елементи, що підвищують ефективність навчання;

Системи моделювання бойових дій, використовуються для створення складних сценаріїв бойових дій, що включають різні види військової техніки та підрозділів. Це дозволяє військовим планувальникам розробляти та тестувати стратегії в умовах, максимально наближених до реальних;

Інтерактивні тренажери, дозволяють військовим взаємодіяти з симуляторами в режимі реального часу, що підвищує ефективність навчання. Наприклад, симулятори від "Інтерактивні системи плюс" дозволяють відпрацьовувати стрільбу з різних видів зброї в умовах, максимально наближених до реальних.

Ці технології забезпечують високий рівень реалістичності та ефективності військових симуляторів, що сприяє підвищенню бойової готовності та професійної підготовки українських військовослужбовців.

Кілька країн є лідерами у розробці військових симуляторів, завдяки своїм передовим технологіям, значним інвестиціям у дослідження та розвиток, а також активній участі у міжнародних військових альянсах. До світових лідерів у розробці військових симуляторів відносяться таки країни як, США, Канада Ізраїль, Велика Британія, Німеччина, Франція, Китай і Австралія.

США: США є безперечним лідером у розробці військових симуляторів. Управління перспективних досліджень Міністерства оборони США (DARPA) активно працює над створенням нових симуляційних технологій, включаючи глобальні комп’ютерні симуляції для військових навчань. Крім того, американські компанії, такі як Bohemia Interactive Simulations, є провідними виробниками військових симуляторів.

Канада: Канадські компанії активно розробляють та впроваджують нові симуляційні системи для військових навчань.

Ізраїль: Ізраїльські компанії розробляють високотехнологічні симулятори, які використовуються як всередині країни, так і експортуються до інших держав.

Велика Британія: Британські компанії та дослідницькі установи активно працюють над створенням нових симуляційних технологій, які використовуються як у національних збройних силах, так і в міжнародних військових операціях.

Німеччина: Німеччина має значний досвід у розробці військових симуляторів, завдяки своїм передовим технологіям та інноваційним підходам.

Франція: Французькі компанії розробляють та впроваджують нові симуляційні системи для військових навчань.

Китай: Китай активно розвиває свої можливості у сфері військових симуляторів, інвестуючи значні ресурси у дослідження та розробки. Китайські компанії та дослідницькі установи працюють над створенням нових симуляційних технологій, які використовуються як всередині країни, так і експортуються до інших держав.

Австралія: Австралійські компанії активно розробляють та впроваджують нові симуляційні системи для військових навчань.

Ці країни є лідерами у розробці військових симуляторів завдяки своїм передовим технологіям, значним інвестиціям у дослідження та розвиток, а також активній участі у міжнародних військових альянсах.

Військові симулятори мають потенціал значно покращити підготовку військовослужбовців, роблячи її більш ефективною, безпечною та адаптивною до сучасних викликів.

Аналіз останніх публікацій. Відомо багато досліджень та порівнянь проблематики, стосовно тренажерів та симуляторів у військовій справі. З урахуванням, що під час аналізу проблематики застосування тренажерів та симуляторів у військовій справі використовувалися ресурси всесвітньої інтернет бази даних Web of Science, Scopus, Googly Academy. тощо, а система пошукових запитів налаштована задля застосування спеціальних функцій пошукових ключів, з визначенням ключових термінів і комбінацій, що характеризують досліджувану область, результатом проведеного пошуку на момент дослідження, стали 572 різноманітних публікацій, у тому числі 39 монографій, 23 бібліографічних оглядів, 17 технічних стандартів. Велика різноманітність підходів до технічного опису зустрічається в спеціалізованій літературі, а саме в керівництвах до тренажерних комплексів в авіації, інженерії, військовій справі та інших галузях. Так, наприклад в роботі [3] Ганна Красота-Мороз надає загальні визначення, опис і класифікацію систем симуляції. Також дослідження [12] Бредфорда Белла (Bradford S. Bell) та співавторів надає важливий фундаментальний аналітичний опис таких систем. А Олександр Перемот, в блозі GameDev DOU, надає потужний опис застосування військового симулятора "Обрій" з розкриттям переваг і недоліків [13].

Але сучасні стан та реалії з урахуванням повномасштабного військового вторгнення рф, прискорило наповнення Сил оборони України різноманітною некодифікованою технікою та озброєнням, в тому числі і саморобними й експериментальними робототехнічними системами, в якості тренажерів використовуються звичайні ігрові пульти і комп'ютерна програма симулятор, отже є неприйнятні для роботи з реальними мобільними роботами.

Таким чином **метою статті** є вирішення наукової проблеми шляхом удосконалення засобів, що необхідні для вирішення прикладного завдання навчання оператора і здійснення керування мобільним роботом.

Викладення основного матеріалу: Поєднання матаналізу, теорії автоматичного управління та інших фундаментальних наук та симуляторів є критично важливим для військових з причин які впливають на [14]:

Точність моделювання. Математичні моделі дозволяють створювати точні симуляції різних військових сценаріїв. Використання математичних алгоритмів забезпечує високу точність і реалістичність симуляцій, що є критично важливим для ефективної підготовки військовослужбовців:

Оптимізація ресурсів. Використання математичного апарату, допомагає оптимізувати використання ресурсів під час військових навчань. Це включає планування логістики, розподіл ресурсів та управління часом. Математичні моделі дозволяють знаходити оптимальні рішення для складних задач, що допомагає знизити витрати та підвищити ефективність навчань.

Аналіз та прогнозування. Математичні методи дозволяють аналізувати результати симуляцій та робити прогнози щодо можливих результатів бойових дій. Це включає аналіз

великих обсягів даних, виявлення закономірностей та тенденцій, а також моделювання різних сценаріїв розвитку подій. Такий підхід допомагає військовим краще розуміти можливі ризики та приймати обґрунтовані рішення.

Розробка нових технологій. Наукова формалізація завдання є основою для розробки нових технологій, які використовуються у військових симуляторах. Це включає створення алгоритмів штучного інтелекту, машинного навчання, а також розробку нових методів моделювання та симуляції. Використання передових математичних методів дозволяє створювати більш ефективні та реалістичні симулятори.

Підвищення реалістичності. Математичні моделі дозволяють враховувати велику кількість змінних та факторів, що впливають на бойові дії. Це включає моделювання різних типів місцевості, погодних умов, а також поведінки противника. Використання математики забезпечує високу реалістичність симуляцій, що допомагає військовослужбовцям краще підготуватися до реальних бойових умов.

Інтеграція з іншими системами. Математичні моделі дозволяють інтегрувати симулятори з іншими військовими системами, такими як системи управління боєм, розвідки та зв’язку. Це забезпечує комплексний підхід до підготовки та планування військових операцій, що підвищує їх ефективність та координацію.

Навчання та розвиток навичок. Використання математичних моделей у симуляторах дозволяє створювати індивідуальні навчальні програми для військовослужбовців. Це включає адаптацію навчальних завдань до рівня підготовки кожного учасника, надання персоналізованих рекомендацій та зворотного зв’язку. Такий підхід допомагає більш ефективно розвивати навички та знання військовослужбовців.

В процесі симуляції бойових дій використовуються різні математичні моделі, що дозволяють аналізувати та прогнозувати результати військових операцій [15].

Зворотний зв’язок у системах симуляції керування роботом є критичним компонентом, який дозволяє системі коригувати свою поведінку на основі вихідних даних або продуктивності цієї системи. Це коригування є важливим для підтримання стабільності, покращення продуктивності та забезпечення того, щоб системи могли ефективно реагувати на зміни в їхньому середовищі.

Однією з найпоширеніших є передатна функція системи керування зі негативним зворотнім зв’язком, яка описує залежність вихідного сигналу від вхідного. Наведемо приклад такої функції для системи з зворотним зв’язком (рис. 3):

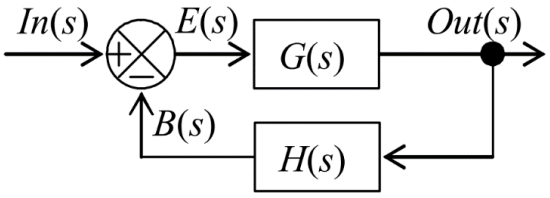


Рис. 3. Блок-схема загального замкнутого контуру
для системи зі зворотним зв’язком

Основні компоненти зворотного зв’язку

Зворотний зв’язок у системах керування роботом зазвичай включає наступні компоненти:

Контролер: Пристрій або алгоритм, що коригує вхідні дані на основі виміряних вихідних даних.

Основні компоненти системи:

1. Вхідні дані. Сигнали або дані, що надходять до системи.

Вхідний сигнал ($In(s)$): бажане значення або команда.

2. Процес, що контролюється. Система або процес, який підлягає контролю.

Передатна функція прямого каналу ($G(s)$): описує динаміку системи без зворотного зв'язку.

3. Вихідні дані. Результати або продуктивність системи.

Вихідний сигнал ($Out(s)$): фактичне значення, яке вимірюється.

4. Сенсори. Елементи, що вимірюють вихідні дані системи в тому числі оператор мобільного робота.

5. Компоненти зворотного зв'язку.

Передатна функція зворотного каналу ($H(s)$): описує динаміку зворотного зв'язку.

Передатна функція замкненої системи зі зворотним зв'язком визначається як:

$$T(s) = \frac{Out(S)}{In(s)} = \frac{G(s)}{1+G(s)H(s)}, \quad (1)$$

де $G(s)$ – передатна функція прямого каналу, а $H(s)$ – передатна функція зворотного каналу.

Зазвичай на практиці передатна функція прямого каналу $G(s)$ і зворотного каналу $H(s)$ розглядаються як:

$$G(s) = \frac{K}{s(T_S+1)}, H(s) = 1, \quad (2)$$

де K – коефіцієнт підсилення, T_S – постійна часу системи.

Тоді передатна функція замкненої системи буде:

$$T(s) = \frac{\frac{K}{s(T_S+1)}}{1+\frac{K}{s(T_S+1)}} = \frac{K}{s(T_S+1)+K}. \quad (3)$$

Ця передатна функція описує, як система реагує на вхідний сигнал з урахуванням зворотного зв'язку. Вона дозволяє аналізувати стабільність системи, її динамічні характеристики та ефективність керування [16].

6. Контролер: Пристрій або алгоритм, що коригує вхідні дані на основі виміряних вихідних даних.

Використання комунікаційних технологій дозволяє забезпечити ефективний зворотній зв'язок, та здійснення надійної передачі даних між компонентами системи. Поєднання математичних моделей та симуляторів дозволяє створювати ефективні системи керування зі зворотним зв'язком, що є критично важливим для сучасних робототехнічних застосувань.

Опис вирішення прикладного завдання. З урахуванням вище зазначеного, фахівцями кафедри Спеціальних інформаційних систем та робототехнічних комплексів, розроблений комплексний симулятор керування мобільним роботом рис. 4.

Для керування безпілотним мобільним роботом отримують у режимі реального часу інформацію про його фактичне положення та стан його руху, за допомогою використання каналу зворотного зв'язку VR FPV, на підставі чого оператор формує команду керування для управління безпілотним мобільним роботом. Будова пристрою керування (рис. 5) дозволяє його використовувати в якості доповнення до наземного пункту управління безпілотного мобільного робота , а також окремого віддаленого мобільного пункту керування.

Рис. 4. Зовнішній вигляд симулятора керування роботом з FPV
та каналом зворотного зв’язку

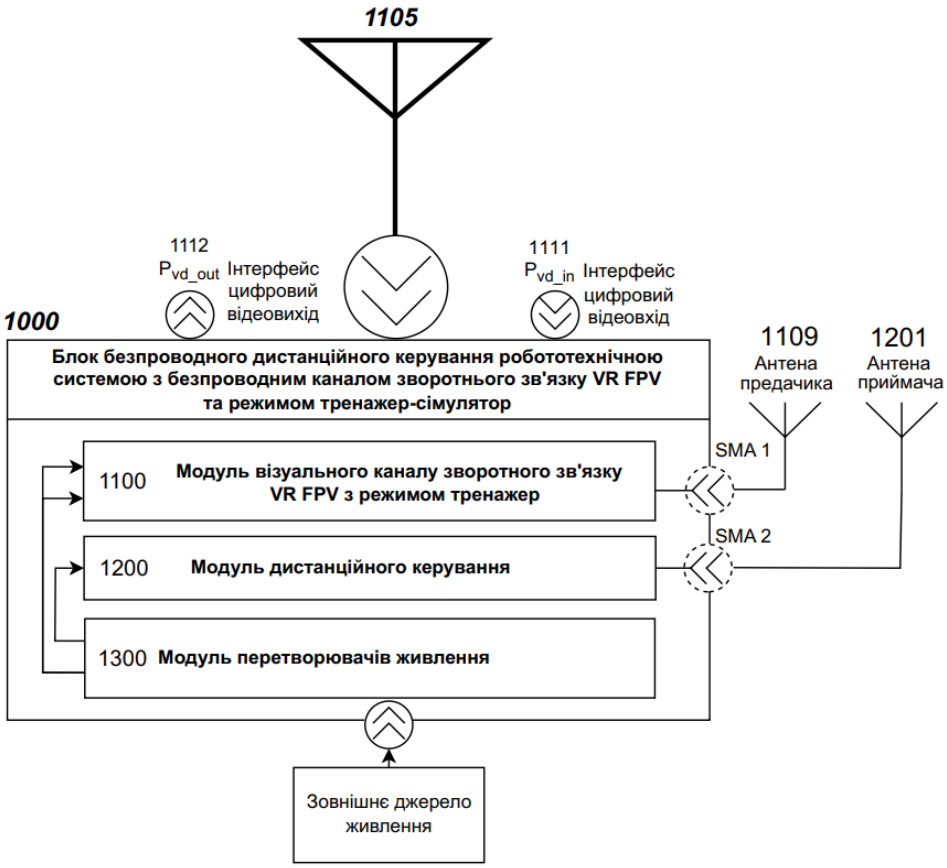


Рис. 5. Загальна функціональна схема будови симулятора керування
роботом з FPV та каналом зворотного зв’язку

В режимі тренажер, пристрій відтворює реальні умови використання й керування безпілотним мобільним роботом і надає можливість відпрацювання всіх без винятку режимів експлуатації безпілотного мобільного робота.

Пристрій містить модуль візуального каналу зворотного зв’язку VR FPV для отримання інформації про стан руху, модуль керування місії, модуль тренажерного перетворювання та критичної індикації. Забезпечений інтерфейсом підключення зовнішніх пристроїв та приймання-передачі даних, відеоокулярів, пульта керування оператора.

Забезпечується підвищення безпеки персоналу та розширення функціональних можливостей під час керування безпілотним мобільним роботом.

Симулятор керування безпілотним мобільним роботом (1000), складається з:

1100 модуль візуального каналу зворотного зв’язку VR FPV з режимом тренажер;

1200 модуль дистанційного керування;

1300 модуль перетворювачів живлення;

1105 антена-симулятор відеопередавача;

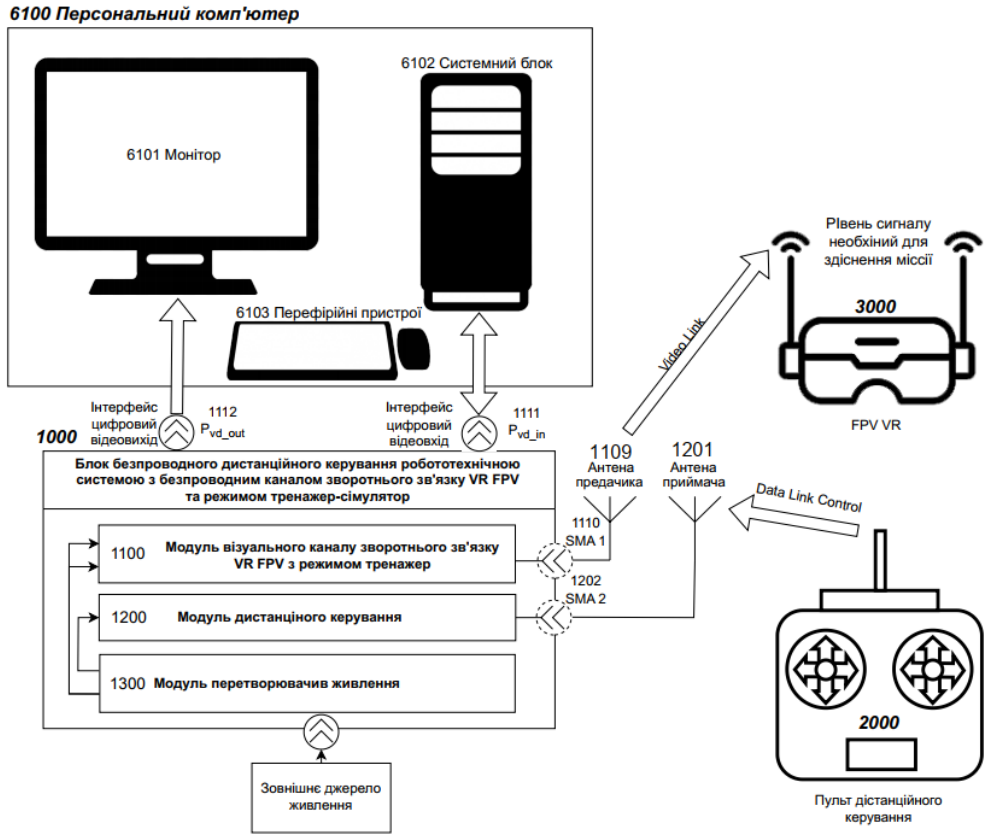
1109 антена відеопередавача;

1201 антена приймача.

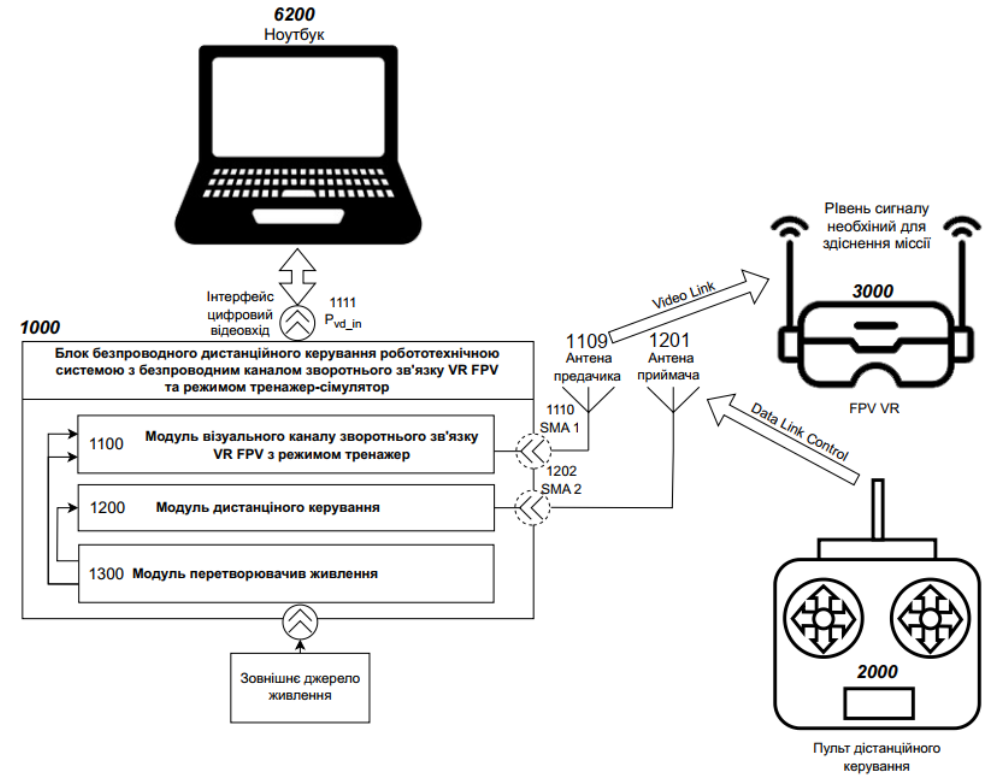
Режими роботи, які підтримує симулятор:

1. Режим "програмно-апаратний симулятор" (рис. 6, *а–в*).

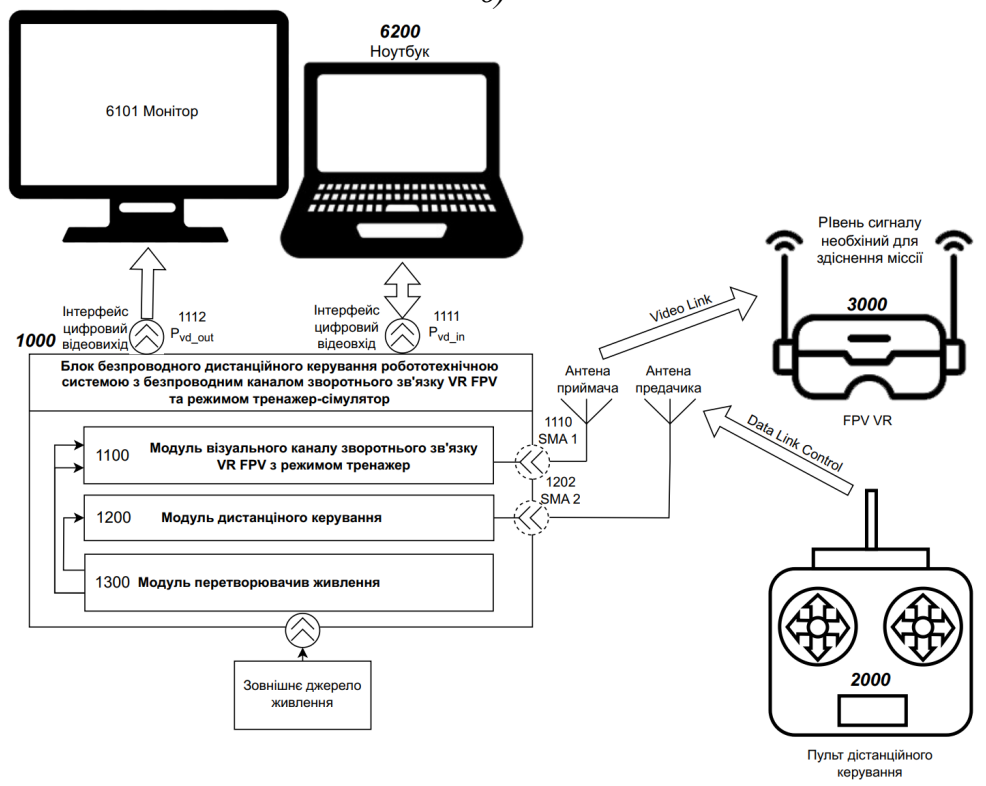
В цьому режимі апаратура працює з пониженою потужністю передавача відеоканалу. Відстань користувача близька до ПЕОМ (режим біля комп’ютера/ ноутбука)



а)



б)



в)

Рис. 6. Схема режим керування безпілотним мобільним роботом з застосуванням пристрою керування безпілотним мобільним роботом з каналом зворотного зв’язку VR FPV та режимом тренажер з ПЕОМ в режимі симуляції керування мобільним роботом:

а – із застосуванням ПЕОМ 6100 "Персональний комп’ютер";

б – із застосуванням ПЕОМ 6200 "Ноутбук";

в – із застосуванням і ПЕОМ 6200 "Ноутбук" та додатковим місцем спостерігача-інструктора

2. Режим "Виносна система керування FPV БпЛА" (рис. 7) Потужність і режим роботи всіх блоків повні. В цьому режимі такі фактори як потужність передавачів та відстань оператора залежать від тактичної і оперативної необхідності поставленого завдання.

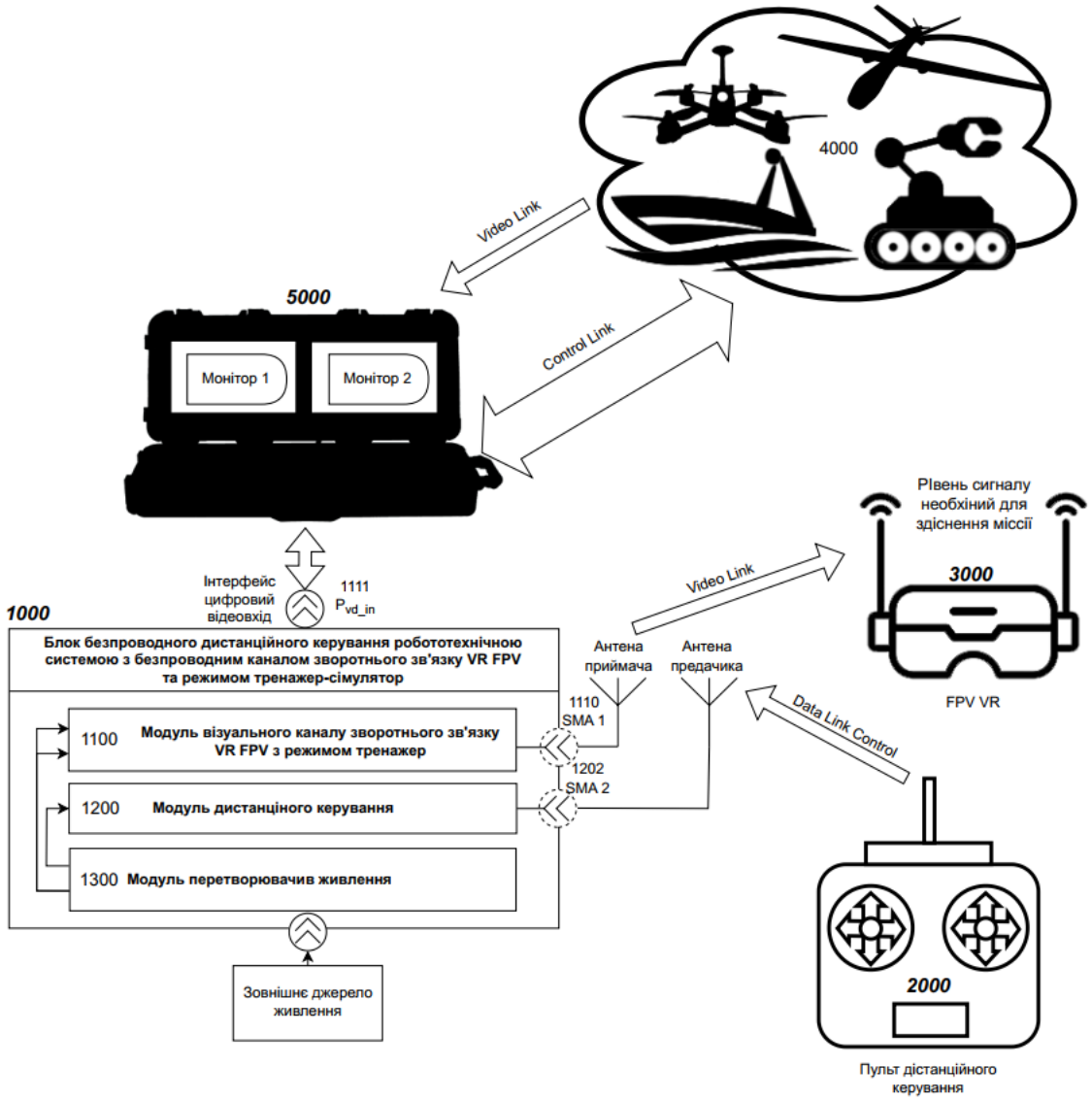


Рис. 7. Схема режим керування безпілотним мобільним роботом з застосуванням пристрою керування безпілотним мобільним роботом з каналом зворотного зв’язку VR FPV та режимом тренажер з наземною станцію керування мобільним роботом

Висновки

В роботі описана загальна складова і запропоновано варіанти використання багаторежимного симулятора мобільного робота. Зворотний зв’язок є невід’ємною частиною систем симуляції керування роботом, забезпечуючи їхню ефективність, стабільність і адаптивність. Застосування в системі зворотного зв’язку коригування в реальному часі дозволяє роботам коригувати свої дії на основі фактичного стану системи. Забезпечує точне керування рухом і виконання завдань. Дозволяє системам адаптуватися до змін у навколишньому середовищі. Така система симуляції з застосуванням комунікаційних технологій має важливу роль для Сил Оборони. Також в сучасному стані розвитку та застосування військових симуляторів відіграє вагомий вплив на підготовку сучасних військовослужбовців.

Сучасні симулятори здатні створювати надзвичайно реалістичні бойові умови, що дозволяє військовослужбовцям відпрацьовувати навички в умовах, максимально наближених до реальних. Використання симуляторів дозволяє значно знизити витрати на підготовку, оскільки не потребує використання реальної техніки, боєприпасів та інших ресурсів. Симулятори забезпечують безпечне середовище для відпрацювання складних та небезпечних маневрів, що знижує ризик травм та втрат під час навчання. Це особливо важливо для рекрутів та під час відпрацювання нових тактик та стратегій. Завдяки використанню сучасних технологій, таких як AI та машинне навчання, симулятори можуть адаптуватися до індивідуальних потреб кожного військовослужбовця, надаючи персоналізовані рекомендації та зворотний зв’язок. Симулятори дозволяють проводити тренування для великої кількості військовослужбовців одночасно, що особливо важливо для підготовки великих підрозділів та координації дій між різними військовими частинами. Сучасні військові та спеціальні симулятори дозволяють швидко створювати та тестувати нові бойові сценарії, що дає можливість військовим бути готовими до різних ситуацій та викликів.

Важливим фактором сучасності є, інтеграція нових технологій (рис. 8) [14].

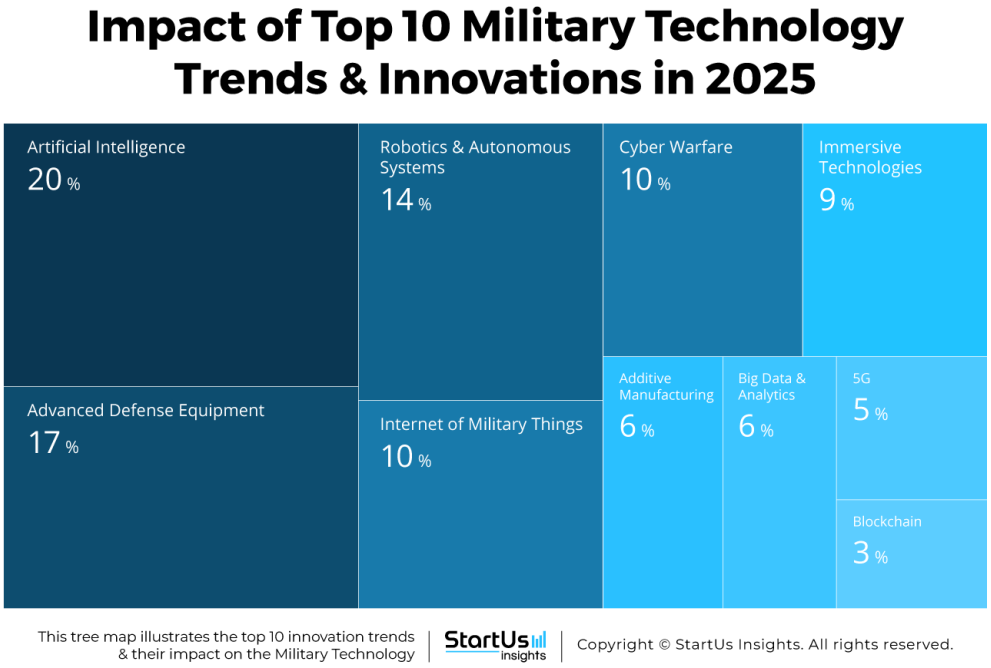


Рис. 8. Інфографіка прогноз-дослідження від аналітичного агентства StartUs, стосовно військових інноваційних технології в 2025 році

Майбутні військові симулятори обов’язково можуть включати ряд нових технологій, які ще більше підвищать їхню ефективність та реалістичність. В якості перспективних технологій, які можуть з’явитися в найближчому майбутньому можна зазначити такі як, штучний інтелект (AI), військовий інтернет речей (MIoT), 5G технології, розширена реальність (XR), адитивне виробництво (3D друк), робототехніка та автономні системи. Ці технології мають потенціал значно покращити військові симулятори, зробивши їх більш реалістичними, інтерактивними та ефективними для підготовки військовослужбовців до сучасних та майбутніх викликів.

Напрями подальших досліджень: Описаний в роботі симулятор поданий в органи патентного права на отримання патенту на корисну модель. Напрямками подальшого дослідження є вдосконалення апарату для застосування в якості універсального ретранслятора керування мобільними роботами, та впровадження системи зв’язку керування глибоководними апаратами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lateef F. Simulation-based learning: Just like the real thing [Electronic resource] / F. Lateef // Journal of Emergencies, Trauma, and Shock. 2010. Vol. 3, No. 4. P. 348. Mode of access: https://doi.org/10.4103/0974-2700.70743.

2. Hurrel S. Simulation-based learning benefits and challenges for eLearning [Electronic resource] / S. Hurrel // Helping You Be Powered By Knowledge | Neovation. Mode of access: https://www.neovation.com/learn/90-simulation-based-learning-benefits-and-challenges-for-elearning.

3. Красота-Мороз Г. Симуляційний тренінг як сучасна педагогічна технологія розвитку компетентностей військовослужбовців сил спеціальних операцій в системі професійної військової освіти [Електронний ресурс] / Г. Красота-Мороз, Д. Оленєв // Військова освіта. 2023. С. 186–195. Режим доступу: https://doi.org/10.33099/2617-1783/2023-47/186-195.

4. Петришин Б. Сучасні технології у підготовці військових: тактичні симулятори SKIFTECH [Електронний ресурс] / Б. Петришин // Рубрика. Режим доступу: https://rubryka.com/article/symulyatory-skiftech/.

5. The Critical Role of Virtual Reality & Simulation in Military Training Â» Karve [Electronic resource] // Karve â Your Strategic Growth Partner. – Mode of access: https://www.karveinternational.com/insights/the-critical-role-of-virtual-reality-simulation-in-military-training (date of access: 10.10.2024).

6. Які симулятори використовують бійці ЗСУ для навчання на Stinger, Javelin та навіть польський ПЗРК Grom | Defense Express [Електронний ресурс] // Військовий портал Defense Express - все про військову справу. Режим доступу: https://defence-ua.com/people_and_company/jaki_simuljatori_vikoristovujut_bijtsi_zsu_dlja_navchannja_na_stinger_javelin_ta_navit_polskij_pzrk_grom-13136.html.

7. Logics7 розробила понад 30 симуляторів зброї для підготовки ЗСУ [Електронний ресурс] // Militarnyi. Режим доступу: https://mil.in.ua/uk/news/logics7-rozrobyla-ponad-30-symulyatoriv-zbroyi-dlya-pidgotovky-zsu/.

8. Івахненко Д. Ігрові симулятори, на яких можна почати опановувати бойові навички [Електронний ресурс] / Д. Івахненко, Д. Гадомський // Texty.org.ua – статті та журналістика даних для людей Тексти.org.ua. Режим доступу: https://texty.org.ua/articles/111677/ihrovi-symulyatory-u-yakyh-mozhna-pochaty-opanovuvaty-bojovi-navychky/.

9. Симулятори бойових дій купити | ТОВ "Інтерактивні системи плюс" [Електронний ресурс] // ТОВ "Інтерактивні системи плюс". Режим доступу: https://isp.com.ua/.

10. Moiseienko O. How Virtual Reality Technologies in Ukraine are Enhancing Modern Warfare And Helping To Train Soldiers [Electronic resource] / O. Moiseienko // UNITED24 Media. Mode of access: https://united24media.com/war-in-ukraine/how-virtual-reality-technologies-in-ukraine-are-enhancing-modern-warfare-and-helping-to-train-soldiers-1466.

11. Система імітації бою MILES в ЗСУ [Електронний ресурс] // Militarnyi. Режим доступу: https://mil.in.ua/uk/systema-imitatsiyi-boyu-miles-v-zsu.

12. Bell, B. S. Current issues and future directions in simulation-based training in North America // B. S. Bell, A. M. Kanar, S.W.J. Kozlowsi - The International Journal of Human Resource Management, 19(8), 2008, pp. 1416–1434.

13. Перемот О. Що потрібно знати, як довго тренуватися та чи допоможе ігровий досвід. [Електронний ресурс] / О. Перемот // GameDevDOU. Режим доступу: https://gamedev.dou.ua/articles/fpv-simulator-steam-games/.

14. Top 10 Military Technology Trends for 2025 | StartUs Insights [Electronic resource] // StartUs Insights. Mode of access: https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022.

15. Forrester J. W. Industrial Dynamics / J. W. Forrester Massachusetts : MIT Press. 1996. 480 p.

16. Sterman J. Business Dynamics: Systems Thinking and Modeling for a Complex World with CD-ROM / J. Sterman. – London: McGraw-Hill Education, 2000. 1008 p.

DOI: 10.58254/viti.6.2024.14.174

УДК 004.9

д-р техн. наук, професор Пількевич І. А. ORCID: 0000-0001-5064-3272 (ЖВІ ім. С. П. Корольова)
Лобода Р. І. ORCID: 0000-0003-4010-0252 (ЖВІ ім. С. П. Корольова)
Мірошніченко С. І. ORCID: 0009-0007-2076-041X (ЖВІ ім. С. П. Корольова)
Остапчук Т. В. ORCID: 0009-0003-6689-3884 (ВІКНУ ім. Тараса Шевченка)

ІНФОРМАЦІЙНА СИСТЕМА ОЦІНЮВАННЯ НАДІЙНОСТІ ДЕШИФРУВАЛЬНИКА ПУНКТУ ДИСТАНЦІЙНОГО ПІЛОТУВАННЯ

В умовах збройної агресії з боку російської федерації проти України, яка переросла у повномасштабне військове вторгнення 24 лютого 2022 року, виникає найбільша загроза національній безпеці, оскільки мова йде про знищення української державності. Як засвідчив досвід підготовки та проведення розвідувальних операцій Збройними силами України під час широкомасштабного вторгнення збройних сил російської федерації на територію нашої держави, застосування безпілотних літальних апаратів І класу засвідчило ефективність їх використання, що актуалізувало питання підвищення ефективності збору розвідувальної інформації за їхньою допомогою.

Ключову роль в роботі безпілотного літального апарата першого класу відіграє дешифрувальник дистанційної пілотажної станції. Від його ефективності залежить якість роботи засобів повітряної розвідки. У статті розглянуто основні показники надійності оператора людино-машинної системи. Проведено аналіз існуючих методів контролю оператора людино-машинної системи, який показує, що показник його працездатності не вимірюється, а визначається шляхом моніторингу його функціонального стану з подальшою оцінкою показників працездатності.

Виходячи з результатів аналізу, встановлено, що застосування теорії нечітких множин та згортки за нелінійною схемою компромісу в задачах оцінки ефективності людино-машинних систем надає змогу ідентифікувати стан надійності дешифратора пункту дистанційного пілотування в реальному часі з урахуванням працездатності людини та ефективності роботи обладнання.

Розроблено інформаційну систему оцінювання надійності дешифрувальника пункту дистанційного пілотування, в основу якої покладена узагальнена математична модель у вигляді багаторівневого ієрархічного дерева логічного висновку, що відображає класифікацію показників та проміжні оцінки. Корінь дерева відповідає результату оцінювання, а вершина оцінювання – показникам надійності пункту дистанційного пілотування. Сам процес ґрунтується на математичному апараті нечіткої логіки та здійснюється з використанням доступної експертної інформації у вигляді логічних правил "ЯКЩО – ТО", що пов'язують нечіткі терми показників надійності пункту дистанційного пілотування і результат оцінювання.

Надійність отриманих даних досягається шляхом формування нечіткої бази знань з використанням нечітких термів, які враховують специфіку процесу отримання розвідувальної інформації на віддалених пунктах пілотування.

Ключові слова: *повітряна розвідка; безпілотні авіаційні комплекси; дешифрувальник; розвідувальна інформація; ефективність функціонування; віддалений пункт пілотування.*

I. Pilkevyc, R. Loboda, S. Miroshnichenko, T. Ostapchuk Information system for assessing reliability a decoder remote piloting station.

Under conditions of armed aggression by Russia against Ukraine, which escalated into a full-scale military invasion on February 24, 2022, national security is facing the greatest threat, as it is about destroying Ukrainian statehood. As experience in preparing and conducting intelligence operations by the Armed Forces of Ukraine during the large-scale invasion by the armed forces of the Russian Federation into your country has shown, using class I unmanned aerial vehicles has proven their effectiveness, which has raised issues of improving intelligence gathering with their help.

A key role in the operations of a first-class unmanned aerial vehicle is played by a remote pilot station decoder. Quality operation of airborne reconnaissance assets depends on its efficiency. The article considers main reliability indicators of a human-machine system operator. The analysis results of the existing methods for controlling the human-machine system operator, which shows that indicators of his performance are not measured, but are determined by monitoring his functional state with further evaluation of performance indicators.

Based on results of the analysis, it was found that using fuzzy set theory and convolution according to a nonlinear trade-off scheme in tasks of evaluating efficiency of human-machine systems makes it possible to identify reliability status of a remote piloting station decoder in real time, taking into account human performance and equipment efficiency.

The article develops an information system for assessing the reliability of a remote piloting station decoder based on a generalized mathematical model in the form of a multilevel hierarchical tree of logical inference that reflects

classification of indicators and intermediate estimates. The roots of the trees correspond to evaluation results, and tops correspond to reliability indicators of a remote piloting point. This process is based on mathematical apparatus of fuzzy logic and is carried out using available expert information in form of logical rules "IF - THEN" that link fuzzy terms of remote piloting point reliability indicators and the assessment result.

Reliability of the obtained data is achieved by forming a fuzzy knowledge base using fuzzy terms that take into account specifics of process obtaining intelligence information at remote piloting points.

Keywords: *aerial reconnaissance; unmanned aerial systems; decoder; intelligence information; performance; remote piloting point.*

Загальна постановка задачі. Аналіз організації та проведення операцій з добування розвідувальної інформації Збройними силами України у контексті широкомасштабного вторгнення збройних сил російської федерації в Україну, ілюструє високу ефективність застосування безпілотних авіаційних комплексів (БпАК) І класу [1].

БпАК І класу спроможні за короткий проміжок часу оглянути значну територію та оперативно передати здобуту інформацію. Під час обробки та аналізу матеріалів повітряної розвідки (ПР) головним є дешифрувальник, оскільки основне навантаження покладається саме на нього. Великий обсяг матеріалів ПР за умови швидкої зміни обстановки, складність виявлення та розпізнавання нових зразків озброєння і військової техніки спричиняє зниження рівня оперативності й достовірності виявлення та розпізнавання об'єктів дешифрувальником. Актуальним напрямком у вирішенні проблеми підвищення ефективності добування розвідувальної інформації (РІ) за допомогою БпАК є розроблення інформаційної системи оцінювання надійності дешифрувальника пункту дистанційного пілотування.

На надійність дешифрувальників пункту дистанційного пілотування (ПДП) впливають як його працездатність так і ефективність функціонування апаратури БпАК. Так як головне завдання ПДП це добування РІ шляхом спостереження та аналізу фотозображень в системі БпАК, то узагальнюючим показником ефективності функціонування системи розпізнавання зображення ПДП було обрано контрастність фотозображень, що сприймаються дешифрувальником з екрана ПДП [1]. Обраний показник дасть змогу врахувати технічний стан ПДП та умови приймання фотозображення, а також визначити вплив контрастності фотозображень на надійність дешифрувальника ПДП.

Таким чином для проведення оцінювання надійності дешифрувальника ПДП необхідно:

обґрунтувати комплексний показник надійності дешифрувальника ПДП;

вибрати та обґрунтувати показники, за якими буде здійснюватися контроль функціонального стану (ФС) дешифрувальника;

розробити інформаційну систему оцінювання надійності дешифрувальника ПДП за вектором виміряних показників.

Аналіз останніх досліджень та публікацій. Станом на сьогодні відсутній уніфікований методологічний підхід до формалізації так званих структурних помилок, ідентифікованих за допомогою методів статичного відлагодження, таких як надмірність, неповнота та суперечливість. Саме тому статично коректні бази знань не гарантують якості прийнятих рішень за рахунок помилок в самих знаннях, часто пов'язаних зі складністю окремої предметної області, що, наприклад, допускає дублювання логіки міркувань [6].

У [7] розглянуто інформаційний підхід до оцінки оперативно-технічних можливостей видових засобів розвідки, який ураховує не тільки просторове розрізнення засобу, але і його градаційні властивості. Запропоновано підхід, основою якого є використання критерію Джонсона, що дозволяє кількісно порівнювати межові зображувальні властивості видових засобів, які використовують однаковий набір розпізнавальних ознак. При цьому науковці під час розпізнавання зображення враховували наступні характеристики – яскравість, контрастність, роздільна здатність, інтервал оптичної щільності (фотографічна ширина), колірна гама, палітра, глибина кольору, насиченість кольору, а також просторова щільність [8]. Однак в жодній з цих робіт не врахована надійність роботи дешифрувальника ПДП.

Автори [9–11] розробили алгоритми оцінювання, методику та структуру комплексу оцінювання сенсомоторних реакцій операторів безпілотних літальних апаратів (далі – БпЛА). На основі проведених досліджень розробили та налагодили апаратно-програмний комплекс, впровадження якого дозволить автоматизувати процес оцінювання сенсомоторних реакцій операторів БпЛА, тим самим підвищити якість їх професійного психологічного відбору для потреб ЗС України. Однак автори залишили поза увагою питання впливу надійності дешифрувальника ПДП як оператора людино-машинної системи.

Метою статті є аналіз існуючих підходів до оцінювання людино-машинних систем та розробка інформаційної системи оцінювання надійності дешифрувальника ПДП.

Виклад основного матеріалу. Відповідно до ДСТУ 2860–94 Надійність техніки. Терміни та визначення (ДСТУ 2860–94), надійність це властивість об'єкта зберігати в часі у визначених межах значення всіх параметрів, які характеризують здатність виконувати необхідні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання і транспортування. Це визначення поширюється на будь-які технічні об'єкти. Для врахування людського фактора в системі машина-оператор, коли не всі властивості можуть бути охарактеризовані кількісно, ДСТУ 2860–94 визначає поняття надійності, як властивість об'єкта зберігати в часі здатність до виконання необхідних функцій в заданих режимах та умовах застосування [2]. Вибір показників та методів розрахунку надійності здійснюється відповідно до ДСТУ 2861–94 Надійність техніки. Аналіз надійності. Основні положення (ДСТУ 2861–94), залежно від виду об'єкта [3]. Види об'єктів, в свою чергу, встановлюються ДСТУ 2863–94 Надійність техніки. Програма забезпечення надійності. Загальні вимоги (далі – ДСТУ 2863–94), відповідно до якого пункт ПДП, як людино-машинну систему, віднесемо до об'єктів виду ІІ, які можуть знаходитися в проміжних станах працездатності та мають основний варіант застосування за призначенням [4]. Для таких об'єктів ДСТУ 2861–94 та ДСТУ 2863–94 визначає комплексний показник надійності $K_{\text{е}}$ – коефіцієнт зниження ефективності, який ставить кожному стану об'єкта певне значення міри зниження номінальної ефективності від 0 до 1. Крім того, вказаний показник надійності, зручно використовувати при розрахунках показників ефективності ПДП в довільний момент часу, так як він показує міру зниження ефективності добування РІ через погіршення надійності дешифрувальника ПДП: $K_{\text{е}} = 1 - \frac{\text{А}_{\text{р}}}{\text{А}_{\text{ном}}}$, де A_p – реальна ефективність добування РІ в ПДП в довільний момент часу, $A_{ном}$ – номінальна ефективність добування РІ у ПДП, за умови оптимального стану дешифрувальника та ефективного функціонування апаратури ПДП.

Таким чином, вихідним параметром інформаційної системи оцінювання надійності дешифрувальника ПДП повинен бути коефіцієнт зниження ефективності – $\text{К}_{\text{е}}$, який враховує обидві складові людино-машинної системи, тобто зниження працездатності дешифрувальника і погіршення ефективності функціонування апаратури ПДП. Як було відмічено [1], ефективність функціонування системи розпізнавання зображення можна оцінювати показником розпізнавання фотозображень, що сприймаються дешифрувальником на екрані ПДП – K_p. Це дасть змогу врахувати технічний стан засобу відображення цільової інформації БпАК та умови приймання відеосигналу, а також визначити вплив контрастності зображення на надійність дешифрувальника ПДП під час добування РІ шляхом пошуку, спостереження та аналізу зображень, що передаються БпЛА в реальному часі.

Основний напрям визначення надійності людино-машинних систем пов'язаний з оцінкою ФС оператора шляхом розрахунку узагальненого показника за вхідним вектором частинних показників з використанням різного виду згорток [5]. Застосування згорток вимагає знання чітких кількісних меж показників та їх оптимальних значень. В умовах індивідуального характеру та варіативності психологічних, фізіологічних і професійних можливостей та характеристик людини-оператора, його чутливості до впливу факторів зовнішнього та внутрішнього середовища визначення вказаних характеристик ускладнено та може привести

до значних похибок у визначенні рівня працездатності дешифрувальника [6]. Крім того, такий підхід не враховує ефективність функціонування техніки.

Таким чином, актуально постає питання розробки інформаційної системи оцінювання надійності дешифрувальника ПДП, з врахуванням вибраних параметрів, що характеризують ФС людини та ефективність функціонування апаратури, яка дозволить виявляти момент зниження надійності та попередити погіршення своєчасності і повноти добування РІ на ПДП. У такій постановці, завдання з оцінювання надійності зводиться до задачі ідентифікації ФС дешифрувальника та визначення розпізнавання зображень.

Під ідентифікацією ФС дешифрувальника ПДП будемо розуміти встановлення взаємозв'язку між вектором показників, отриманих інформаційно-вимірювальною системою в процесі чергування, і станом працездатності дешифрувальника з подальшим розрахунком рівня його надійності.

На рис. 1 представлена контекстна діаграма інформаційної системи оцінювання надійності дешифрувальника ПДП.

За показники ФС дешифрувальника ПДП було обрано такі характеристики: частота серцевих скорочень – X_1; стабільність серцевих скорочень – X_2; опір шкіри – X_3; температура тіла – X_4. Додаткові характеристики, що впливають на ефективність дешифрувальника, але не належать до його ФС: температура зовнішнього середовища – X_5; час доби – X_6; час безперервної роботи – X_7.

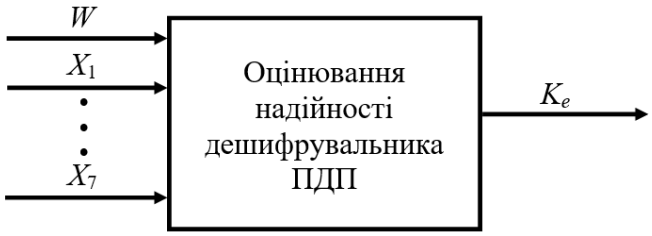


Рис. 1. Контекстна діаграма інформаційної системи

Для врахування впливу технічного стану засобу відеозображення на надійність дешифрувальника ПДП на вхід інформаційної системи надходить інформація про контрастність зображення W.

У зв'язку з індивідуальним характером, відсутністю чітких кількісних меж змін вхідних показників пропонуємо для ідентифікації ФС дешифрувальника ПДП за вибраними показниками використовувати теорію нечіткої логіки, а саме метод, суть якого полягає в проєктуванні та налаштуванні нечіткої бази знань, яка є сукупністю лінгвістичних висловлювань ЯКЩО$_{вх}$ – ТО$_{вих}$. Основна ідея полягає в тому, що налаштувавши нечітку базу знань можна виявити нелінійні залежності з необхідною точністю [7]. Для оцінювання надійності дешифрувальника необхідно побудувати математичну модель, яка встановлює взаємозв'язок між вхідними змінними (виміряні значення фізіологічних показників та зовнішнього середовища) та вихідними змінними (станом працездатності). Для побудови математичної моделі необхідно:

сформувати матрицю знань;

отримати нечіткі логічні рівняння;

визначити функції належності.

Відомо, що основним інструментом нечіткої логіки, яка дозволяє перетворити експертні знання "ЯКЩО-ТО" у жорсткі математичні моделі, є функція належності (ФН) [7]. Для даної задачі, вона характеризує ступінь впевненості експерта в тому, що деяка величина належить нечіткому поняттю (терму).

Методи апарата нечіткої логіки дозволяють зв'язати ФН показників ФС дешифрувальника зі станом працездатності останнього у вигляді правил "ЯКЩО-ТО" на основі нечіткого логічного висновку.

Отже, результат ідентифікації ФС дешифрувальника можна представити у вигляді:

$$y = f(x_1, x_2, \dots, x_n), \tag{1}$$

де $x_1, x_2, \dots, x_n$ – набір значень вхідних показників ФС дешифрувальника;

y – результат ідентифікації ФС.

З метою встановлення залежності (1) необхідно розглядати вхідні показники ФС дешифрувальника і вихідне рішення щодо стану працездатності, в якому знаходиться дешифрувальник, як лінгвістичні змінні, що задані на універсальних множинах:

$$X_i = \left[\underline{x_i}, \overline{x_i}\right], \tag{2}$$

$$Y = \left[\underline{y}, \overline{y}\right]. \tag{3}$$

Для оцінювання таких лінгвістичних змінних пропонується використовувати якісні терми, що складають терм-множину:

$A_i = \{a_i^1, a_i^2, \dots, a_i^{k_i}\}$ – терм-множина змінної x_i, $i = \overline{1,n}$;

$D_i = \{d_1, d_2, \dots, d_m\}$ – терм-множина змінної y,

де a_i^p – p-й лінгвістичний терм змінної x_i, $p = \overline{1,k_i}$, $i = \overline{1,n}$;

d_j – j -й лінгвістичний терм змінної y;

m – число різних рішень.

Назви термів $a_i^1, a_i^2, \dots, a_i^{k_i}$ можуть відрізнятися для різних лінгвістичних змінних x_i, $i = \overline{1,n}$.

Лінгвістичні терми $a_i^p \in A_i$ і $d_i \in D$, $p = \overline{1,k_i}$, $i = \overline{1,n}$, $j = \overline{1,m}$ необхідно розглядати як нечіткі множини задані на універсальних множинах X, Y за допомогою виразів (2) і (3).

Нечіткі множини a_i^p і d_i визначаються співвідношеннями:

$$a_i^p = \int_{\underline{x_i}}^{\overline{x_i}} \mu^{a_i^p}(x_i)/x_i; \tag{4}$$

$$d_j = \int_{\underline{d}}^{\overline{d}} \mu^{d_j}(d)/d, \tag{5}$$

де $\mu^{a_i^p}(x_i)$ – ФН значення змінної $x_i \in \left[\underline{x}, \overline{x}\right]$, $i = \overline{1,n}$ терму $a_i^p \in A_i$,$p = \overline{1,k_i}$;

$\mu^{d_j}(d)$ – ФН значення змінної $y \in \left[\underline{y}, \overline{y}\right]$ терму-рішенню $d_j \in D$,$j = \overline{1,m}$.

У співвідношеннях (4) і (5) знаки інтеграла позначають об'єднання пар $\mu(u)/u$.

Матриця знань сформована за такими правилами: розмірність такої матриці дорівнює $(n+1) \times N$, де $(n+1)$ – кількість стовпчиків, $N = k_1 + k_2 + \dots + k_m$ – кількість рядків; перші n стовпців відповідають вхідним показникам ФС дешифрувальника x_i, $i = \overline{1,n}$, а $(n+1)$-й стовпчик – значенням d_j вихідного рішення y, $j = \overline{1,m}$; кожен рядок матриці є деякою комбінацією значень вхідних показників ФС дешифрувальника, віднесену експертом до одного з можливих станів працездатності d_j, причому перші k_j рядків відповідають значенню d_1, а останні k_m рядків – значенню d_m; елемент a_i^{jp}, що стоїть на перетині i-го стовпця і jp-го рядка, відповідає лінгвістичній оцінці показника x_i у рядку нечіткої бази знань із номером jp, причому лінгвістична оцінка a_i^{jp} вибирається з терм-множини відповідного показника x_i, тобто:

$$\left(a_i^{jp} \in A_i, i = \overline{1,n}, j = \overline{1,m}, p = \overline{1,l_j}\right). \tag{6}$$

Для формування матриці знань перерахуємо можливі рівні стану надійності дешифрувальника ПДП. У чисельних дослідженнях встановлено, що надійність оператора людино-машинної системи нерозривно пов'язана з рівнем та динамікою його працездатності,

тому оцінювання надійності дешифрувальника будемо проводити шляхом визначення стану його працездатності, яка має низку рівнів $N_i, (i = 1 \dots 5)$ [8]: N_1 – впрацювання (ВП); N_2 – компенсації (К); N_3 – субкомпенсації (С); N_4 – декомпенсації (Д); N_5 – зрив (З).

Крім того визначимо межі, в яких змінюються показники, що вимірюються: X_1 – (45–180) уд/хв., X_2 – (0–5) уд/хв., X_3 – (10–30) кОм, X_4 – (35,5–40)°С, X_5 – (–20–+40)°С, X_6 – (0–24) год, X_7 – (0–6) год. Задача оцінки працездатності полягає в тому, щоб кожній комбінації показників поставити у відповідність одне з можливих рішень $N_i, (i = 1 \dots 5)$.

На рис. 2 представлена декомпозиційна діаграма інформаційної системи оцінювання надійності дешифрувальника ПДП, де T, P – проміжні змінні, $N \in (N_1, N_2, N_3, N_4, N_5)$ – стан працездатності дешифрувальника.

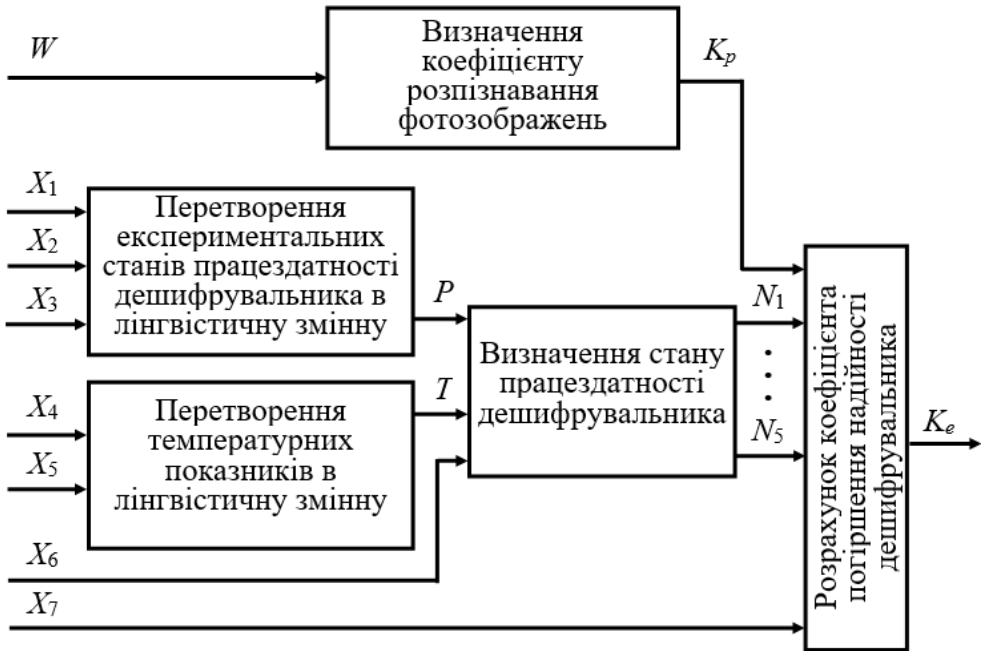


Рис. 2. Декомпозиційна діаграма інформаційної системи

Наведену модель описують рівняння:

$$T = f(X_4, X_5); \quad (7)$$

$$P = f(X_1, X_2, X_3); \quad (8)$$

$$N = f(X_6, X_7, T, P). \quad (9)$$

Показники $X_1 - X_7$ будемо розглядати як лінгвістичні змінні, а для їх оцінки будемо використовувати шкалу якісних термів. Для оцінки лінгвістичних змінних T та P будемо використовувати наступні терми: T={норма (Н), поза нормою (ПН)}; P={спокій (С), оптимальна робота (ОР), робота з максимальною мобілізацією сил (МС), стрес (СТ)}. Кожен із введених термів представляє собою нечітку множину.

Для визначення ФН вхідних параметрів $X_1 - X_7$ нечітким термам запропоновано метод рангових оцінок, для виставлення яких застосуємо 9-бальну шкалу Сааті.

Отримані значення ФН вхідних параметрів $X_1 - X_7$ представлені у вигляді графіків нечітких множин відповідних параметрів на рис. 3–9 [9].

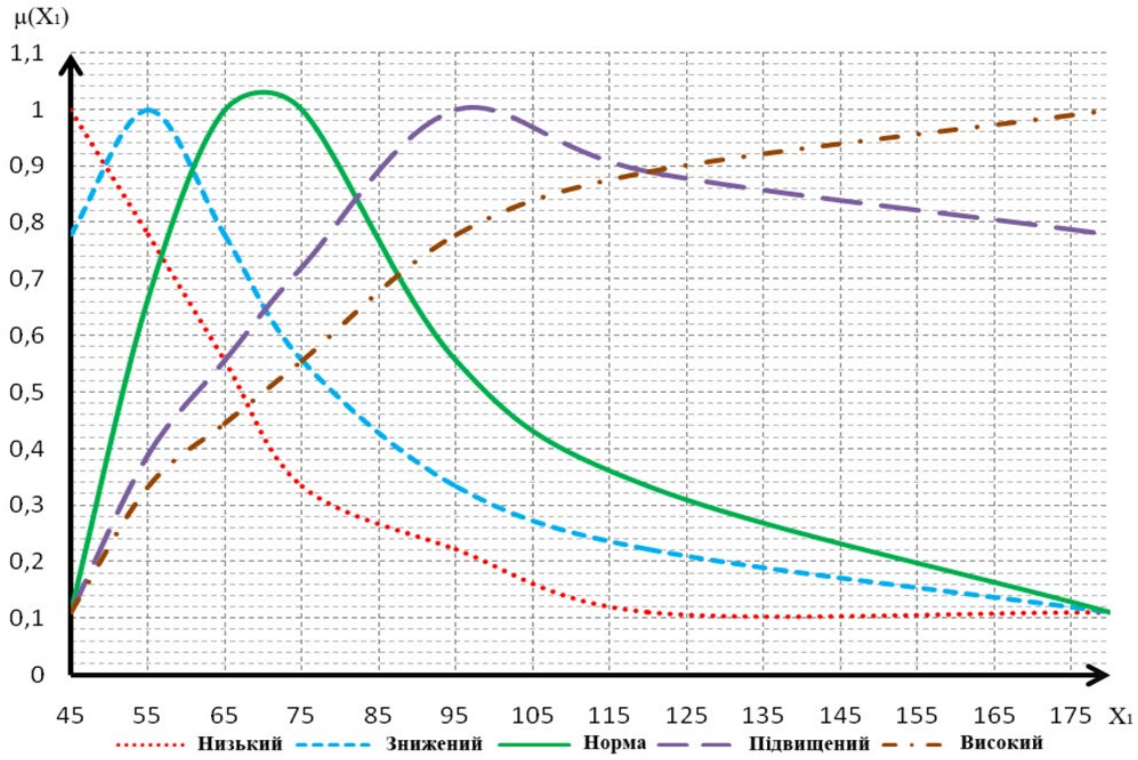


Рис. 3. Нечіткі множини параметра X_1

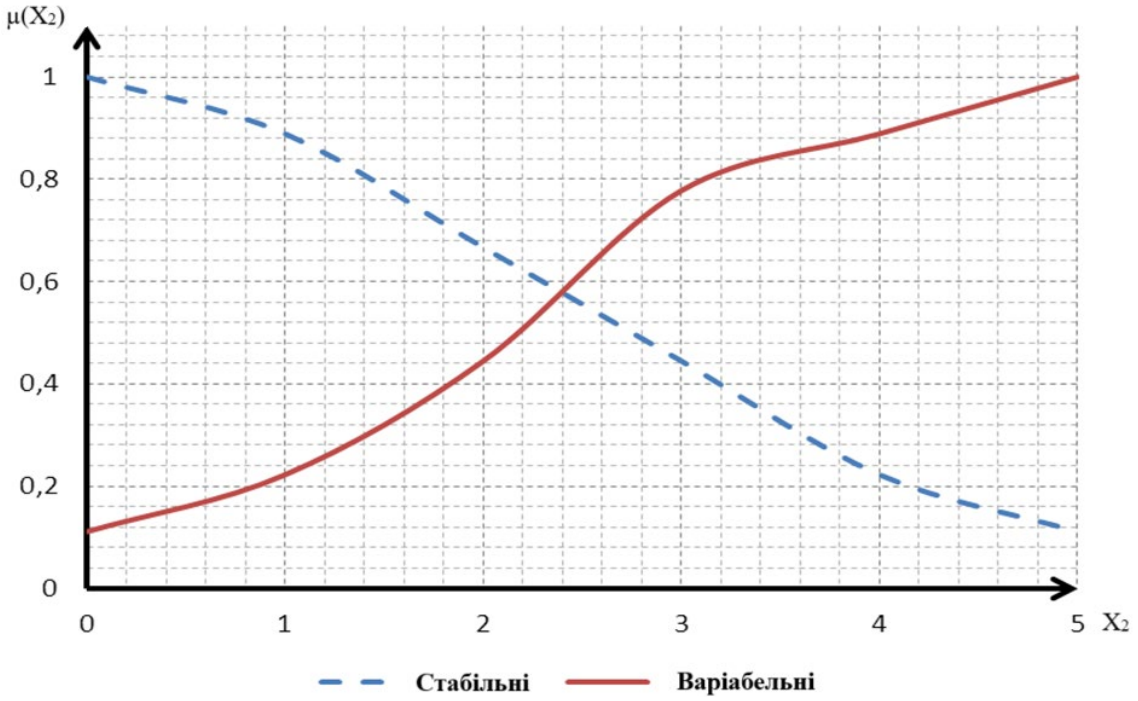


Рис. 4. Нечіткі множини параметра X_2

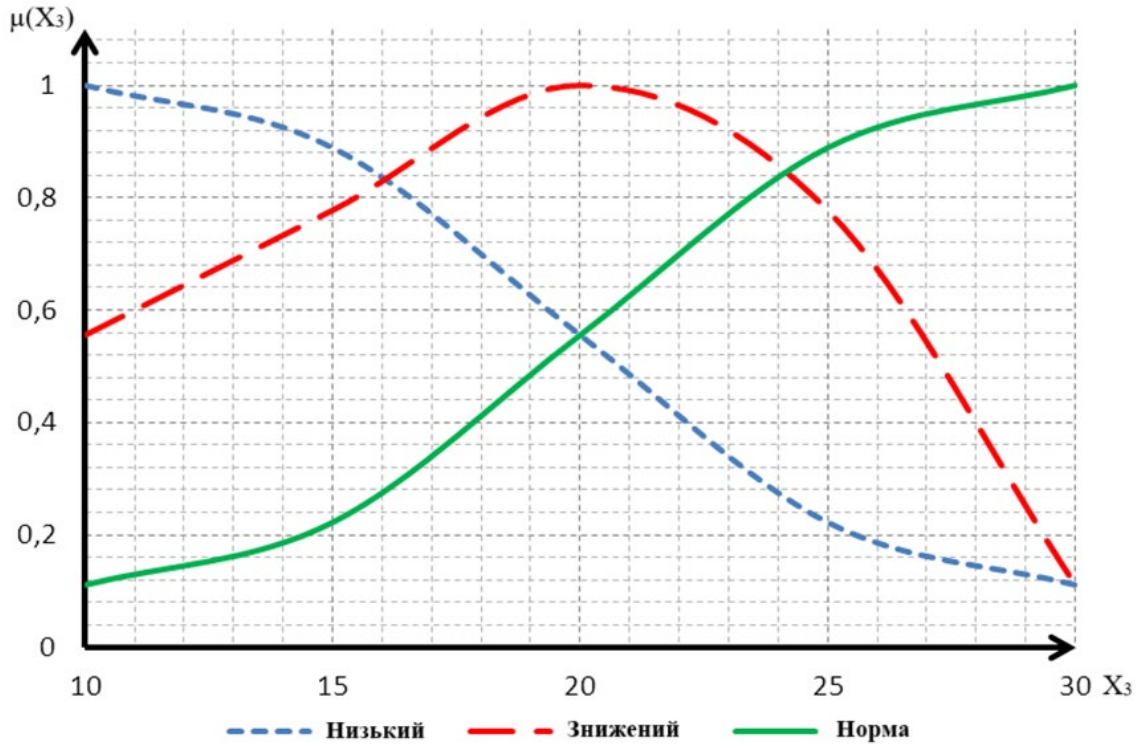


Рис. 5. Нечіткі множини параметра X_3

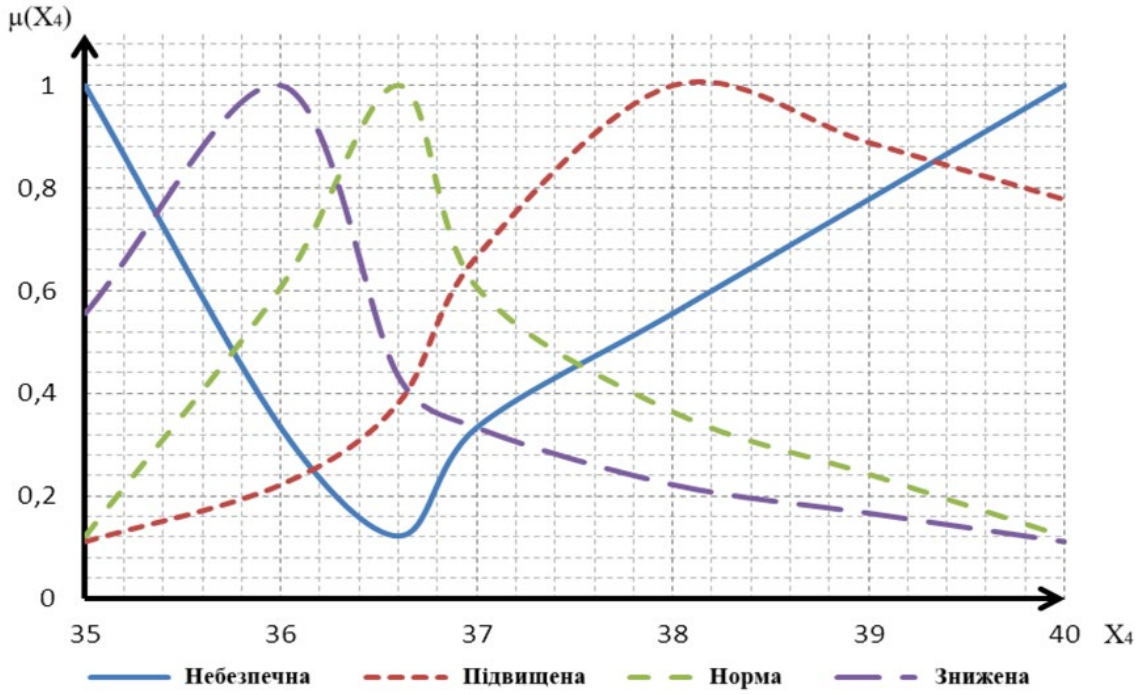


Рис. 6. Нечіткі множини параметра X_4

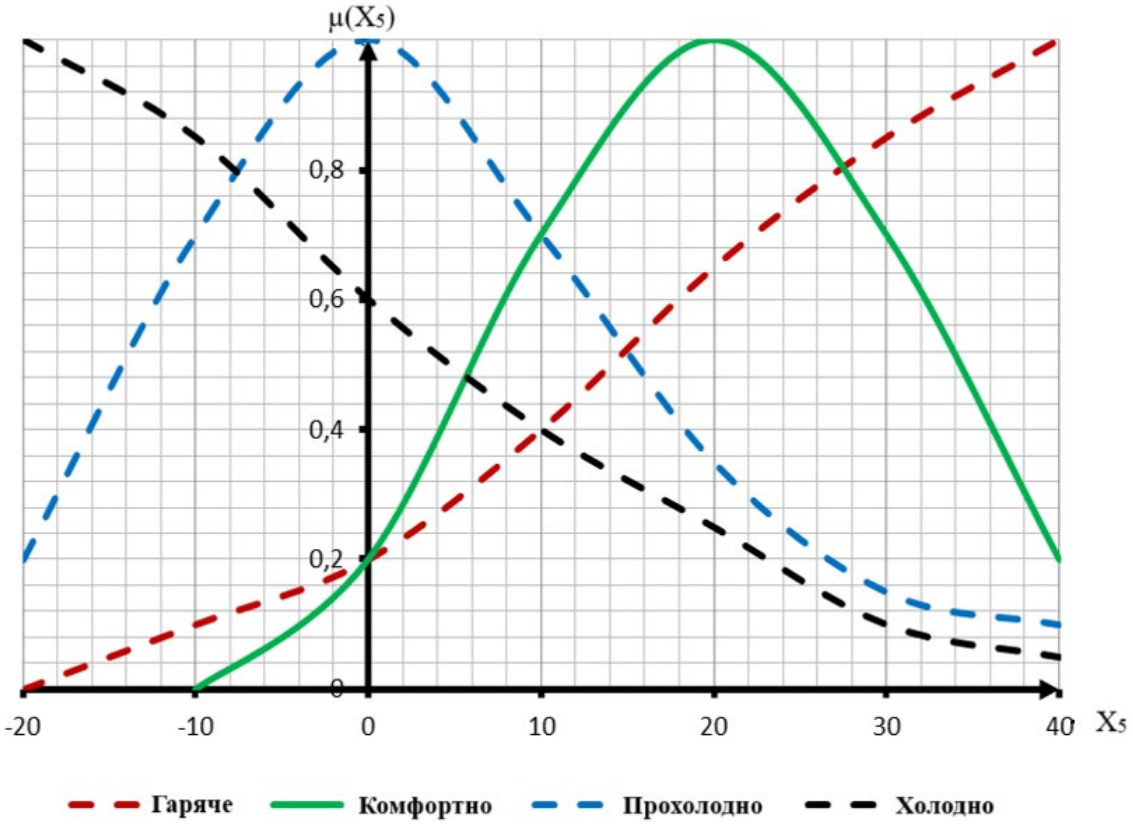


Рис. 7. Нечіткі множини параметра X_5

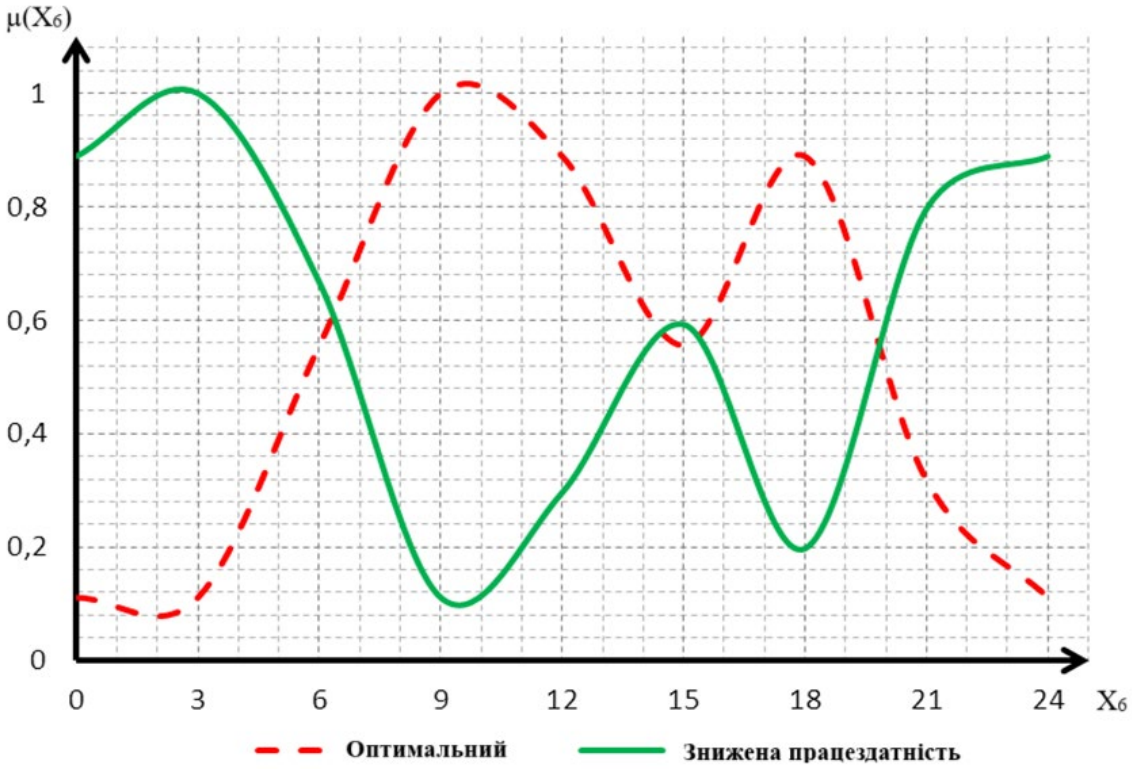


Рис. 8. Нечіткі множини параметра X_6

Для автоматизації процесу визначення ступеня належності показників ФС дешифрувальника до відповідних термів, було проведено апроксимацію нечітких множин параметрів $X_1 - X_7$ у середовищі Microsoft Office Excel, та отримані рівняння. Таким чином, знаючи ФН параметрів до оціночних термів, можна знайти ступінь належності стану дешифрувальника до кожного з рівнів працездатності $N_i, i = 1 \dots 5$.

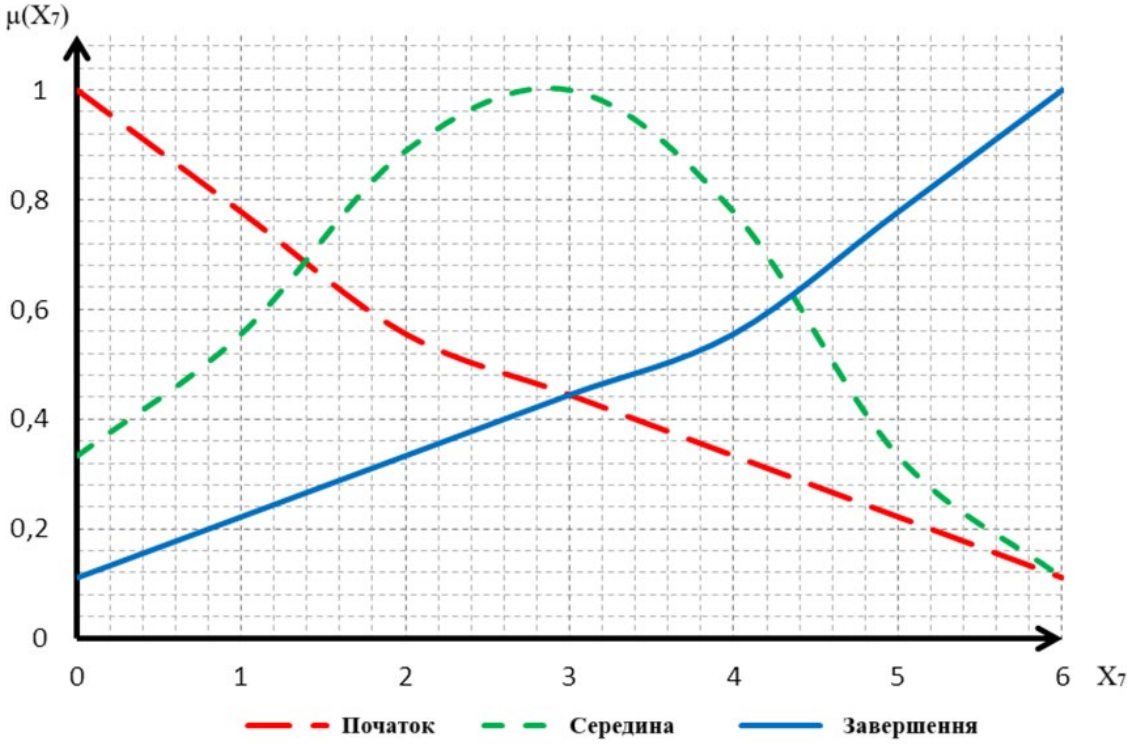


Рис. 9. Нечіткі множини параметра X_7

Для врахування в інформаційній системі якості обробки фотозображень в засобі відображення цільової інформації було використано формантний підхід до оцінювання розпізнавання зображень на фоні шуму. В результаті апроксимації залежності було отримано аналітичний вираз для обчислення коефіцієнта розпізнавання фотозображень залежно від контрастності:

$$K_{\text{р}} = \begin{cases} -0{,}428W + 1 \text{ якщо } W \le 0{,}7; \\ -1{,}19W + 1{,}54 \text{ якщо } 0{,}7 < W \le 0{,}94; \\ -83{,}3W^2 + 155W - 71{,}67 \text{ якщо } W > 0{,}94. \end{cases} \quad (10)$$

Отже, знаючи ФН параметрів $X_1«, \dots, » X_{»7«}$ до оціночних термів та коефіцієнт розпізнавання фотозображень – K_p, можна визначити коефіцієнт погіршення надійності дешифрувальника ПДП.

Для оцінювання надійності дешифрувальника пропонується застосовувати згортку за нелінійною схемою компромісів, якій притаманна висока чутливість до змін величин окремих частинних критеріїв та яка враховує компенсацію малої величини одного критерію надлишковою величиною іншого [10]

$$Y = \sum_{i=1}^{s} a_i [1 - y_i(x)],^{-1} \quad (11)$$

де a_i – вагові коефіцієнти, які характеризують ступінь впливу i-го показника на результат (ступінь впливу відповідного рівня працездатності на погіршення надійності дешифрувальника);

y_i – частинні показники.

Вагові коефіцієнти визначалися за виразом:

$$a_i = \frac{f_i}{\sum_{j=1}^{7} f_i}, \tag{12}$$

де f_i – коефіцієнт, який характеризує відносний вплив i-го показника на погіршення ефективності добування РІ на ПДП. Враховуючи кількість показників та їх вплив на зниження надійності дешифрувальника, було обрано наступні значення коефіцієнтів: $f_1 = 3$, $f_2 = 7$, $f_3 = 4$, $f_4 = 6$, $f_5 = 7$, $f_6 = 5$, $f_7 = 6$. Відповідно до виразу (12) були отримані значення вагових коефіцієнтів: $a_1 = »0{,}079»$, $a_2 = »0{,}184»$, $a_3 = »0{,}105»$, $a_4 = »0{,}158»$, $a_5 = »0{,}184»$, $a_6 = »0{,}131»$, $a_7 = »0{,}157»$.

Остаточний вираз для розрахунку коефіцієнта погіршення надійності дешифрувальника ПДП буде мати вигляд:

$$K_e = 1 - \frac{1}{\sum_{i=1,3,4,5} a_i \left[1-\mu^{N_i}\right]^{-1} + \frac{a_2}{\mu^{N_2}} + \frac{a_6}{1-K_\text{p}}}, \tag{13}$$

де μ^{N_i} – ФН до $N_i, i = 1 \ldots 5$ рівня працездатності.

Отже інформаційна система оцінювання надійності дешифрувальника ПДП працює за наступною послідовністю:

1. Зафіксувати вектор показників фізіологічних показників

$$X = \{X_1, X_2, X_3, X_4, X_5, X_6, X_7\}.$$

2. Визначити коефіцієнт розпізнавання фотозображень K_p за виразом (10).

3. Використовуючи логічні рівняння для температурних показників X_4, X_5, розрахувати багатомірну ФН вектора X_4, X_5 для всіх значень лінгвістичної змінної T, при цьому логічні операції (ТА)∧ і (АБО)∨ заміняються на операції min та max відповідно:

$$\mu(x) \wedge \mu(y) = \min\{\mu(x), \mu(y)\}; \qquad \mu(x) \vee \mu(y) = \max\{\mu(x), \mu(y)\}. \tag{13}$$

4. Використовуючи логічні рівняння для показників X_1, X_2, X_3 та правило (14), перетворити експериментальні стани працездатності дешифрувальника в лінгвістичну змінну P.

5. Визначити стан працездатності дешифрувальника ПДП N_i.

6. Використовуючи вираз (13), розрахувати коефіцієнт погіршення надійності дешифрувальника ПДП для вектора вхідних параметрів $X = \{X_1, X_2, X_3, X_4, X_5, X_6, X_7, W\}$.

Розроблена інформаційна система дозволяє визначити момент критичного зниження надійності дешифрувальника ПДП.

Висновок. Проведений аналіз показав, що застосування теорії нечітких множин та згортки за нелінійною схемою компромісів в задачах оцінювання надійності людино-машинних систем дозволяє здійснювати ідентифікацію стану надійності дешифрувальника ПДП в реальному масштабі часу з врахуванням працездатності людської компоненти та ефективності функціонування апаратури.

Розроблено інформаційну систему оцінювання надійності дешифрувальника ПДП, в основу якої покладена узагальнююча математична модель у вигляді багаторівневого ієрархічного дерева логічного висновку, що відображає класифікацію показників та проміжні висновки оцінювання. Корінь дерева відповідає результату оцінювання, а вершина показникам надійності дешифрувальника ПДП. Процес оцінювання надійності дешифрувальника ПДП ґрунтується на математичному апараті нечіткої логіки та здійснюється з використанням доступної експертної інформації у вигляді логічних правил "ЯКЩО-ТО", що пов'язують нечіткі терми показників надійності дешифрувальника ПДП і результат оцінювання. Науковий результат полягає у побудові ієрархічної системи відношень, яка дозволяє провести оцінювання надійність дешифрувальника ПДП і відслідковувати її

залежність від показників стану дешифрувальника та ефективності функціонування засобу відображення цільової інформації.

Напрямок подальших досліджень. Для продовження досліджень необхідно розробити алгоритм автоматичного моніторингу стану надійності оператора ПДП.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пількевич І. А., Лобода Р. І., Мірошніченко С. І. Аналіз шляхів забезпечення ефективності добування розвідувальної інформації за допомогою БпАК І класу // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. пр. Житомир: ЖВІ, 2023. Вип. № 25 (ІІ). С. 4–19. Інв. 5427 дск.

2. ДСТУ 2860–94 Надійність техніки. Терміни та визначення. Наказ Держстандарту України № 333 від 28 грудня 1994 р.

3. ДСТУ 2861–94 Надійність техніки. Аналіз надійності. Основні положення. Наказ Держстандарту України № 310 від 08 грудня 1994 р.

4. ДСТУ 2863–94 Надійність техніки. Програма забезпечення надійності. Загальні вимоги. Наказ Держстандарту України № 310 від 08 грудня 1994 р.

5. Дячук О. А., Фуртат Ю. О. Проблема надійності при участі людини-оператора в процесі прийняття рішень по керуванню об'єктами енергетики // Математичне та комп'ютерне моделювання. Серія: Технічні науки. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2020. Вип. 21. С. 61–75. URL: https://doi.org/10.32626/2308-5916.2020-21.61-75.

6. Пількевич І. А., Лобода Р. І., Дмитрук В. В., Лобода В. В. Перспективні напрями підвищення ефективності функціонування БпАК І класу // Збірник наукових праць "Труди університету". Київ: Національний університет оборони України ім. Івана Черняховського, 2021. № 2 (165). С. 42–49. Інв. 2574 т.

7. Осієвський С. В., Третяк В. Ф., Кулагін К. К., Власов А. В., Закіров З. З., Кривчун В. І. Метод підвищення ефективності функціонування людино-машинної системи за рахунок підвищення якості програмного забезпечення системи підтримки прийняття рішень. Грааль науки. № 6. С. 170–181. URL: https://doi.org/10.36074/grail-of-science.25.06.2021.029.

8. Філімонов В. І. Фізіологія людини: підручник. 4-е вид. / В. І. Філімонов. Київ: ВСВ «Медицина», 2021. 488 с. ISBN: 978-617-505-851-0.

9. Токар А. М. Удосконалене ергономічне забезпечення ефективності добування розвідувальної інформації на постах радіоперехоплення. Житомир: 20.02.14 – Озброєння і військова техніка. ЖВІ, 2013. 188 с. Інв. 262 т.

10. Засядько А. А. Способи спрощення задачі нелінійного програмування на основі класифікації обмежень // Системи обробки інформації. Харків: ХНУПС, 2020. Вип. 2 (161). С. 59–70. URL: https://doi.org/10.30748/soi.2020.161.07.

DOI: 10.58254/viti.6.2024.15.186

УДК 621.396.4

д-р техн. наук, професор Романюк В. А. ORCID: 0000-0002-6218-2327 (ВІТІ ім. Героїв Крут)
д-р філософії Гримуд А. Г. ORCID: 0000-0003-4012-5185 (НУОУ)

АЛГОРИТМИ ПОБУДОВИ ТРАЄКТОРІЇ КОМУНІКАЦІЙНОЇ АЕРОПЛАТФОРМИ ДЛЯ ЗБОРУ ДАНИХ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Пропонується рішення задачі побудови траєкторії польоту комунікаційної аероплатформи для збору даних моніторингу з вузлів незв’язної безпроводової сенсорної мережі великої розмірності для досягнення різних цільових функцій: мінімізація часу збору або максимізація часу функціонування мережі. Задача вирішується послідовно за застосуванням визначеної послідовності алгоритмів: кластеризації, пошуку найкоротшого шляху та його корегування за визначеними евристиками. Отримання допустимих рішень в реальному часі базується на застосуванні множини розроблених алгоритмів (евристик), які враховують взаємне розташування вузлів, наявність енергії їх батарей та об’єм трафіка моніторингу. Для оцінки ефективності застосування алгоритмів побудови траєкторії польоту та збору даних розроблена відповідна імітаційна модель. Отримані залежності показників ефективності (час збору даних, витрати енергії батарей, час функціонування мережі) на множині алгоритмів побудови траєкторії збору даних комунікаційною аероплатформою при різних вхідних даних. Результати імітаційного моделювання довели можливість зменшення часу збору даних до 20 % або підвищення часу функціонування мережі до 15 % порівняно з існуючими рішеннями.

Ключові слова: *безпроводова сенсорна мережа, комунікаційна аероплатформа, збір даних, траєкторія польоту, алгоритми побудови траєкторії.*

V. Romaniuk, A. Hrymud Algorithms for designing a trajectory of a communication aerial platform for collecting data from wireless sensor network nodes

Algorithms are proposed for solving the problem designing the flight path of a communication aerial platform for collecting monitoring data from the nodes of a large-scale disconnected wireless sensor network to achieve various objective functions: minimizing the collection time or maximizing the network operation time. To achieve the given objective functions, the problem is solved by applying a certain sequence of algorithms: clustering, finding the shortest path and its correction according to the defined heuristics. Obtaining admissible solutions in real time is based on the application of a set of developed algorithms (heuristics), which take into account the relative location of nodes, the energy level of their batteries, and the volume of monitoring data. In order to evaluate the efficiency of the application of flight path construction and data collection algorithms, a corresponding simulation model was developed. The obtained dependences of efficiency indicators (data collection time, battery energy consumption, network operation time) on a set of algorithms for building the spacecraft data collection trajectory with different input data. The results of simulations proved the possibility of reducing data collection time by up to 20 % or increasing network operation time by up to 15 % compared to existing solutions.

Keywords: *wireless sensor network, communication aerial platform, data collection, flight trajectory, algorithms for trajectory construction.*

1. Постановка завдання. Останні роки відбувається швидкий розвиток технологій безпроводових сенсорних мереж (БСМ). БСМ застосовуються для рішення багатьох задач моніторингу параметрів об’єктів (територій): спостереження за станом полів агрокультур, лісів, продуктопроводів, ліній електропередач, кордонів; пошуково-рятувальних та військових операцій тощо.

Особливістю БСМ [1–3] є обмеженість ресурсів сенсорних вузлів за енергією батареї, швидкодією процесора, обсягом пам’яті, потужністю передавача тощо. Сучасні БСМ налічують сотні (тисячі) сенсорних вузлів. Застосування класичної архітектури БСМ (передача даних моніторингу за маршрутами від вузлів до шлюзу) не завжди представляється можливим або економічно доцільним. Наприклад, у районах, які постраждали від надзвичайної ситуації, зайнятих противником, відсутня можливість використання комунікаційної інфраструктури загального користування для організації зв’язку зі шлюзом та немає можливості побудувати зв’язну топологію всієї мережі в умовах значної відстані між вузлами.

Для цих випадків для збору даних з вузлів доцільно застосовувати КА (комунікаційну аероплатформи, КА) в якості мобільного повітряного шлюзу [1–4]. При цьому виникає актуальна наукова задача підвищення ефективності алгоритмів побудови траєкторії обльоту КА вузлів мережі для збору даних з метою досягнення певних цільових функцій (ЦФ): мінімізації часу збору даних та/або мінімізації споживання енергії вузлів (максимізації часу функціонування мережі) [3–5, 21]. Розв'язання цієї задачі дозволить оптимізувати параметри системи управління процесом збору даних та в цілому покращити його ефективність.

2. Аналіз останніх публікацій. Використання КА для збору даних у видалених БСМ великої розмірності є відомим рішенням та розглядається з різних боків у багатьох публікаціях [1–16].

Перша група публікацій [5, 6] розглядає два способи рішення задачі побудови траєкторії польоту КА:

1. Обліт всієї території розміщення вузлів БСМ [5] за різними моделями – по горизонталі, спіраллю, зигзаґом, за кривою Гільберта тощо;

2. Обліт більшості території (кількості вузлів) з врахуванням обмеження на граничний час польоту КА (запропоновані тракторна, вуглова, кругова, квадратна моделі польоту КА [6]).

Основний недолік способу збору даних за обльотом території – значний час збору даних. Однак цей спосіб буде застосовуватися при первинному обльоті КА мережі для визначення фактичних параметрів вузлів (координати положення, рівень енергії батарей, обсяг даних моніторингу).

Наступна група публікацій [7–10] розглядає побудову траєкторії польоту КА при збиранні даних з вузлів лише як рішення класичної задачі комівояжера – пошук найкоротшого маршруту між початковою та кінцевою точкою польоту ТА з прольотом через вузли або точки збору даних (центри кластерів). Ця задача відноситься до класу NP-складних. Отримання точного рішення мережі значної розмірності проблематично. Тому на практиці пропонують евристичні алгоритми отримання наближеного рішення, які мають незначну обчислювальну складність: евристики Лин-Кернигана (Lin-Kernighan traveling salesman heuristic, LKH) [8], найближчого сусіда (Near Neighboring, NN) [9], за спіраллю (Spiral Decomposition) [10], за клітинками (Fast Path Planning with Rules, FPPWR) [11], випуклої оболонки (Convex Hull Insertion Heuristic, CHIH) [12], мурашиний алгоритм [13], генетичний алгоритм [14], алгоритм рою частинок [15] тощо. Однак за такою постановкою задачі обчислюється тільки найкоротший маршрут польоту, але не враховується стан параметрів вузлів, не здійснюється оптимізація енерговитрат вузлів. Тому застосування алгоритму пошуку найкоротшого шляху доцільно використовувати для початкового (базового) рішення та його подальшого покращення.

Третя група публікацій визначає [16–21] два основних підходи для підвищення ефективності збору даних КА з вузлів БСМ великої розмірності:

1. Збір даних КА безпосередньо з кожного вузла за рахунок створення віртуальних кластерів у місцях фактичного розташування вузлів;

2. Збір даних КА тільки з головних вузлів реальних кластерів мережі.

При першому підході (при відсутності зв'язності між вузлами) центр управління мережею розраховує тимчасові кластери (локальні радіомережі: КА-вузли кластеру) та в процесі польоту їх фактично формує КА (повітряний шлюз). При другому – при наявності радіозв'язності між сенсорними вузлами відбувається самоорганізація мережі та її розбиття на реальні фізичні кластери з визначенням головних вузлів кластерів (за відомими алгоритми кластеризації LEACH, HEED тощо) [16], які збирають дані з простих вузлів-моніторингу. КА облітає та збирає дані тільки з головних вузлів кластерів. Далі будемо враховувати обидва підходи.

В публікаціях [17–21] досліджуються особливості окремих етапів процесу збору даних та способи досягнення цільовими функціями: мінімум часу збору, максимум покриття площі (кількості вузлів) тощо.

В [17] досліджується задача зменшення час збору даних завдяки послідовному додаванню потенційно можливих точок зависання. Однак перебір варіантів точок зависання призводить до значної обчисленої складності, тому запропоновані рішення можуть бути використані в мережі малої розмірності.

В [18] досліджується декілька стратегій побудови точок збору даних з вузлів кластерів та траєкторії польоту КА в тимчасовій кластеризованій БСМ: через центр кластера, збір даних на траєкторії польоту на найближчій відстані від вузла до КА, політ через критичні вузли в кластерах, політ із зависанням в одній точці збору, яка мінімізує сумарну енергію витрат вузлів, тощо. Однак автори не розглядають можливість побудови декількох точок збору даних у кластері, оптимізацію інтервалів обміну, оптимізацію декількох цільових функцій.

В [19] розглядаються правила (евристики) скорочення траєкторії КА за рахунок врахування напряму переміщення КА та розташування вузлів у кластері. Подальші вдосконалення цих правил та оцінка їх ефективності будуть наведені далі в статті.

В [20] використовується глибока нейронна мережа для знаходження 3D-траєкторії польоту ТА з врахуванням якості радіоканалу, однак множина показників ефективності процесу збору не розглядається.

В [21] пропонується досягати цільової функції послідовно за рівнями ієрархії: мережа, кластер, КА, група вузлів, окремий вузол. На мережевому рівні оптимізація показників ефективності відбувається визначенням кількості кластерів та їх розмірів, побудовою найкоротшого маршруту обльоту. На рівнях КА-група вузлів та КА-вузол визначається відстань, яка дозволяє оптимізувати час обміну між ними та витрати енергії (запропоновані правила корегування точок (інтервалів) збору даних траєкторії). Для зменшення варіантів перебору та скорочення часу знаходження рішення по траєкторії обльоту вузлів та збору даних запропонована відповідна база правил прийняття рішень. Однак оцінка ефективності застосування правил та вагового визначення їх пріоритету не наведена.

Таким чином, невирішеним завданням при розгляді правил побудови траєкторії польоту КА, є оцінка ефективності їх застосування та визначення порядку (пріоритету) застосування для побудови траєкторії збору даних визначеної БСМ для досягнення двох основних критеріїв оптимізації: мінімізації часу зору даних та максимізації часу функціонування мережі.

Метою статті є аналіз ефективності та послідовності застосування алгоритмів (правил) побудови траєкторії польоту КА для збору даних з вузлів БСМ при досягненні визначених цільових функцій.

Виклад основного матеріалу. Розглядається стаціонарна безпроводова сенсорна мережа значної розмірності (сотні сенсорних вузлів) спеціального призначення. Кожен сенсорний вузол складається з наступних основних елементів: батарея, множина сенсорних датчиків (наприклад, вібраційний, магнітний, акустичний тощо), процесор, пам’ять, прийомопередавач, антена, система позиціонування, система управління.

В процесі свого функціонування кожний сенсорний вузол здійснює збір та зберігання параметрів навколишнього середовища (об’єктів спостереження) визначеної йому зони моніторингу. Кількість параметрів збору визначається типом сенсорних модулів, а частота та способи збору даних (за подіями, періодично, постійно) визначаються наземним центром управління мережею (ЦУМ).

Вузли БСМ випадковим чином розташовані на певній території та не мають можливості встановити зв’язну топологію для передачі даних до шлюзу з різних причин: значна відстань між ними, специфіка рельєфу місцевості, відсутність будь-якої комунікаційної інфраструктури загального користування, необхідність виконувати режим радіомовчання,

економічна недоцільність встановлення та експлуатації шлюзів тощо. Тобто в цих умовах топологія сенсорної мережі буде складатись з окремих незв'язних вузлів та/або окремих незв'язних фрагментів (кластерів) мереж. Вузли в зв'язних кластерах (при наявності у них відповідної системи управління, яка здатна реалізувати алгоритми самоорганізації) можуть вводити ієрархію управління: формувати головні вузли кластерів, які будуть збирати та зберігати дані з інших так званих простих вузлів кластера [16].

Для БСМ з незв'язною топологією роль мобільного шлюзу виконує безпілотний літальний апарат, оснащений додатковим обладнанням для реалізації процесу збору даних з сенсорних вузлів: процесор, пам'ять, прийомопередавач, антена, система позиціонування, відповідна система управління (комунікаційна аероплатформа).

На етапі планування ЦУМ розраховує траєкторію польоту КА та визначає на ній попередні точки (відрізки) збору даних з вузлів у просторі. В процесі польоту КА, завдяки спрямованій антені на висоті $h_k(t)$, формує тимчасові кластери (зони покриття та радіозв'язності) $C_k(t)$, $k = 1…K$ вузлів з радіусом $R_k(t)$, тобто створює тимчасові локальні радіомережі з повітряною точкою доступу (КА). Якщо в процесі польоту КА в поточну зону радіозв'язності потрапляють окремі вузли (головні вузли реальних кластерів фрагментів мережі), тоді вона встановлює з ними радіозв'язок (згідно з MAC-протоколом), визначає графік обміну та визначає (або корегує) точку (інтервал) траєкторії обміну. При підльоті КА до точки (інтервалу) збору даних на траєкторії відбувається процес обміну даними вузла-КА (рис. 1).

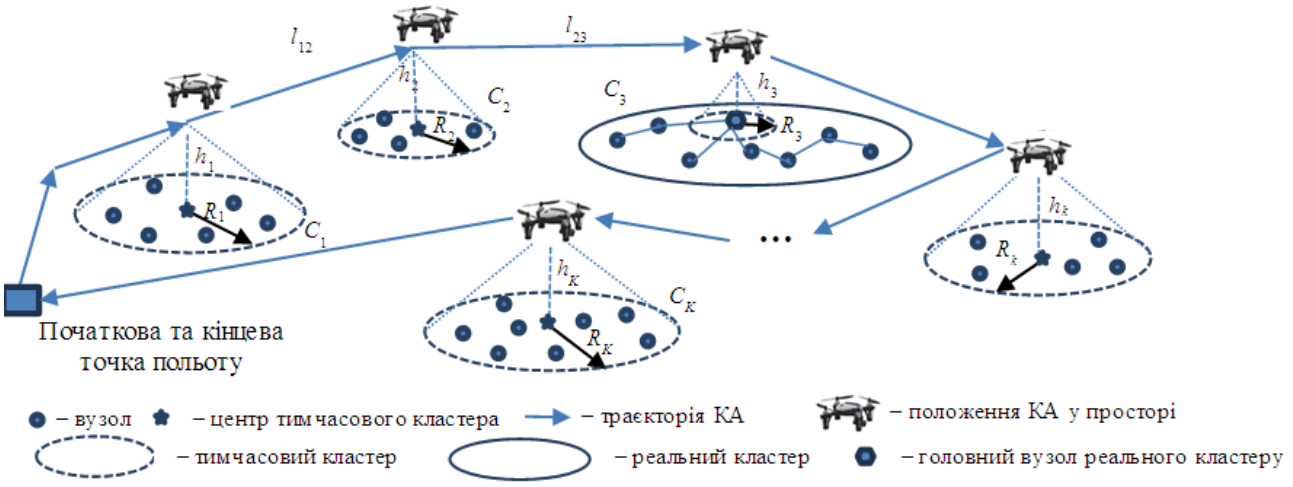


Рис. 1. Приклад траєкторії польоту КА для збору даних з вузлів (головних вузлів) кластерів

Задано:

1. Характеристики безпроводової сенсорної мережі:

– площа розташування БСМ (S) та вигляд її геометричної фігури (наприклад, прямокутна, смуга, коло, довільна тощо);

– кількість вузлів мережі (незв'язних та/або головних вузлів реальних кластерів), координати їх розміщення на місцевості (x_i, y_i), $i = 1... N$;

– щільність розміщення вузлів $\alpha = \bigcup_{k=1}^{K} \pi R_k^2 / S$ вузлів (де R_k – радіус k-ої зони покриття КА, $k = 1…K$) та тип їх розміщення (однорідний, з угрупованням тощо);

– обсяг зібраних даних моніторингу кожним i-м вузлом – V_{dmi}.

2. Характеристики вузла:

– технічні характеристики вузла – кількість та типи сенсорних датчиків, рівень енергії батареї, витрати енергії на моніторинг параметрів середовища для кожного типу датчика тощо;

– комунікаційні характеристики вузла – параметри антени, прийомопередавача, витрати енергії на біт прийому та передачі даних для обраного MAC-протоколу та типу обладнання тощо.

3. Характеристики комунікаційної аероплатформи:

– польотні характеристики – швидкість, висота, час польоту, енергія батареї, можливість зависання та переміщення у просторі з постійною або змінною швидкістю тощо;

– комунікаційні характеристики – MAC-протокол, параметри прийомопередавача тощо.

4. Цільові функції управління (1 – 4) збором даних, які реалізуються ЦУМ [21]:

– мінімізація часу збору даних T_{col}

$$T_{col} = \frac{L}{v} = \sum_{m=1}^{M} \frac{l_m}{v_m} \to \min \quad (1)$$

при забезпеченні заданого часу функціонування мережі $T_{fun} \geq T_{fungiv}$,

$l_m, v_m, m = 1 \dots M$ – інтервали траєкторії між точками збору даних та швидкість польоту;

– максимізація часу функціонування мережі T_{fun} за рахунок зниження (перерозподілу) витрат енергії вузлів e_{coni}

$$T_{fun} \to \max \quad (E_{con} = \sum_{i=1}^{N} e_{coni} \to \min) \quad (2)$$

при забезпеченні заданого часу збору даних $T_{col} \leq T_{co\,lg\,iv}$;

– оптимізація обох критеріїв $\begin{cases} T_{col} \to \min \\ T_{fun} \to \max \end{cases}$ або (3)

отримання допустимого рішення $T_{col} \leq T_{colgiv}$ та/або $T_{fun} \geq T_{fungiv}$, (4)

при обмеженнях Ω на:

– тип літального апарату (роторний); швидкість v=[$v_{\min}$, $v_{\max}$], висота h=[$h_{\min}$, $h_{\max}$], час $t_{fly} \leq t_{fly\max}$ та дальність його польоту $L \leq L_{\max}$;

– кількість кластерів у мережі – $1 \leq k \leq K$;

–початкову енергію батарей вузлів $e_i \leq e_{\max}$ та КА $e_{\text{КА}} \leq e_{\text{КА}\max}$;

– обсяг даних моніторингу кожного i-го вузла – $V_{dmi} \leq V_{dm\max}$;

– дальність радіозв'язності вузол-КА – $d_{i\text{-ТА}} \leq d_{\max}$ – розглядається поширення радіохвиль в умовах прямої видимості;

– радіус площі зони покриття (кластера) КА – $R_{\min} \leq R \leq R_{\max}$.

Час функціонування мережі T_{fun} може визначатися наступними показниками:

а) періодом стабільного функціонування мережі T_{pso} (5) – час функціонування мережі (моніторинг та передача даних в кожному раунді обльоту КА) до відмови першого вузла внаслідок виснаження його батареї:

$$T_{pso} = \min_{i \in N} t_{funi}(Nround), \quad (5)$$

де t_{funi} – час функціонування i-го вузла до його відмови, який визначається кількістю раундів обльоту ($Nround$);

б) відсотком вузлів, які відмовили (6) відносно кількості раундів обльоту КА

$$T_{fun} = \frac{N_{fail}(Nround)}{N} \text{ у відсотках,} \quad (6)$$

де $N_{fail}\,(Nround)$ – кількість вузлів, у яких енергія батареї менша допустимого рівня на $Nround$ раунді обльоту.

5. Множина способів (правил) побудови траєкторії польоту та збору даних КА з вузлів БСМ.

Обмеження та вимоги:

– площа обльоту КА немає заборонених зон, траєкторія її польоту формується у вигляді визначених координат точок у просторі, моделювання процесу польоту КА не розглядається;

– інформація про параметри стану вузлів (координати розміщення, рівень енергії батарей, обсяг даних моніторингу) збирається при первинному обльоті мережі КА, надалі інформація про стан вузлів оновлюється при кожному раунді обльоту;

– КА має можливість збору даних як при зависанні, так і в процесі польоту;

– КА і сенсорні вузли мають радіозасоби з однаковим MAC-протоколом, який дозволяє адаптувати швидкість передачі даних залежно від стану радіоканалу (співвідношення сигнал/шум) та регулювати потужність передачі (витрати енергії на передачу), наприклад, IEEE 802.11;

– обсяги пам'яті сенсорних вузлів, КА достатні для зберігання даних моніторингу;

– рівень енергії батареї КА достатній для здійснення раунду обльоту мережі;

– алгоритми управління процесом збору даних, які реалізуються системами управління вузлів та КА, повинні мати незначну обчислювальну складність через необхідність реалізації автономного польоту КА та забезпечення процесу збору даних у реальному часі.

Необхідно: провести аналіз ефективності застосування різних евристик (алгоритмів) побудови (корегуванні) траєкторії польоту КА для збору даних з вузлів БСМ при досягненні певних цільових функцій.

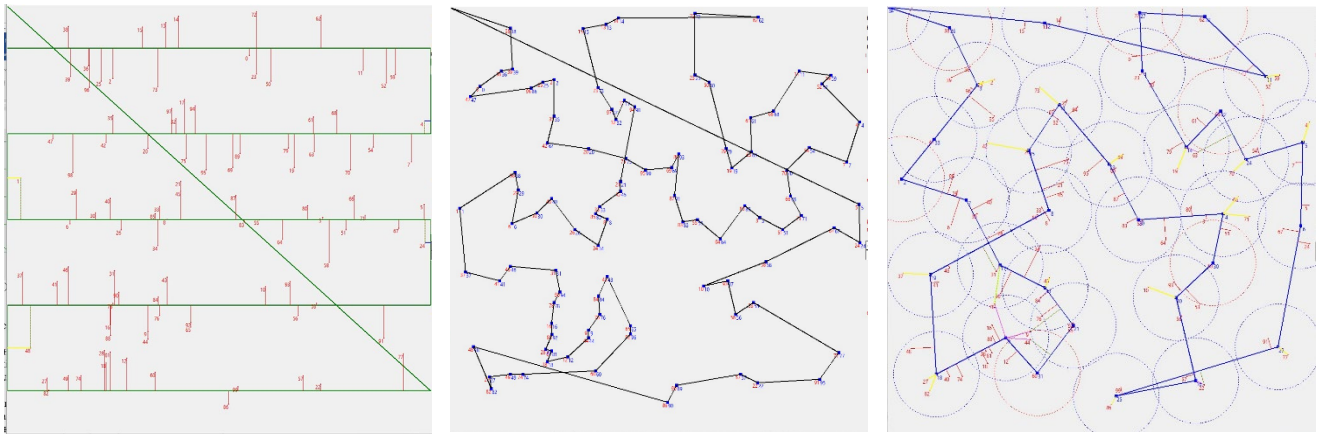
Рішення

Множина алгоритмів по досягненню цільових функцій (1)–(4) знаходиться між двома граничними: обліт КА всієї площі розміщення вузлів та обліт КА кожного вузла мережі.

Рис. 2. Взаємозв'язок алгоритмів побудови траєкторії польоту КА

1. **Алгоритми обльоту КА всієї території (площі), яку займають вузли БСМ**, з одночасним збором даних моніторингу з вузлів мережі. Так дослідження [5, 6] були присвячені аналізу різних варіантів обльоту всієї площі та збором даних з головних вузлів реальних кластерів: за смугами (рис. 3, *а*), за кутом, за квадратом, за кругом. Мета дослідження – знайти варіанти обльоту, які дозволяють скоротити довжину маршруту обльоту, або максимізувати кількість обслугованих (покритих) вузлів за обмежений час польоту КА. Показано, що не існує єдиного оптимального варіанта обльоту: варіант "за смугами" ефективний для максимізації площі покриття БСМ, варіант за колом більш ефективний за часом обльоту. Однак довжина маршруту та час обльоту за всією площею БСМ залишається дуже великим. Наприклад, за результатами проведеного авторами імітаційного моделювання для мережі з 100 вузлів довжина траєкторії КА при обльоті всієї площі по горизонталі при $R = 100$ складає $L = 7500$ ум. од., при сумарних витратах енергії вузлів $E_{con} = 4477$, при зменшенні радіуса покриття в два рази $R = 50$ довжина траєкторії вже становить $L = 11878$, при зменшенні в два рази витрат енергії до значення $E_{con} = 2115$ (рис. 2, *а*), що накладає додаткові вимоги до польотних характеристик літального апарата.

Обліт КА всієї мережі зазвичай буде використовуватися при первинному обльоті мережі для збору вихідної інформації про параметри вузлів мережі (координати положення, обсяг даних моніторингу, рівень енергії батареї тощо).



$L = 7232 \quad E_{con} = 4477\ (R = 100)$
$L = 11878 \quad E_{con} = 2582\ (R = 50)$
а) всієї площі БСМ ("за смугами")

$L = 8215\ E_{con} = 2000 \quad (R = R_{\min})$
б) кожного вузла

$L = 5987\ E_{con} = 3068\ (R = 100)$
$L = 7152 \quad E_{con} = 2114\ (R = 50)$
в) тимчасова кластеризація

Рис. 3. Моделювання алгоритмів обльоту КА вузлів БСМ

2. **Обліт кожного вузла на мінімальній висоті польоту КА**. В результаті моделювання цього способу отримуємо мінімальні витрати енергії вузлів на обмін даними $E_{con} = 2000$ (за рахунок ($R \leq R_{min}$) та значну довжину маршруту $L = 8215$ (рис. 3, *б*). Цей спосіб доцільно використовувати для мінімізації витрат енергії – ЦФ (2), але при цьому не гарантується виконання обмеження час польоту (збору даних) $L \leq L_{max}$. Для рішення задачі пошуку найкоротшого маршруту обльоту кожного з вузлів, можуть бути застосовані різні типи алгоритмів: повного перебору (для БСМ малої розмірності), евристичні (найближчого сусіда – рис. 2, *б*, за клітинками, зовнішньої оболонки тощо), генетичні, тощо. Кожний з них показує різні результати, залежно від параметрів мережі та особливостей реалізації (наведено далі в п. 3).

Результати моделювання показників оцінки ефективності перших двох способів є граничними та використовуються для порівняння з результатами застосування інших способів.

3. **Алгоритми кластеризації мережі.** Відбувається віртуальна кластеризація мережі, визначаються точки збору даних в кластерах (зазвичай в центрі кластеру) та побудова траєкторії польоту КА між точками збору. Тобто класична задача комівояжера перетворюється **на задачу пошуку найкоротшого маршруту (точніше траєкторії) переміщення зони покриття КА з начальної в кінцеву точку польоту, яка забезпечує покриття всіх вузлів (точок на площі) на мінімальній відстані обміну КА з вузлами.**

На першому етапі відбувається оптимізація кількості та розмірів кластерів мережі (шляхом визначення висоти польоту КА, діаграми спрямованості антени). Досягнення цільових функцій (1)–(2) має протилежну залежність. Зменшення кількості кластерів призводить до зменшення довжини траєкторії КА, але призводить до збільшення відстані між КА з вузлами кластеру та, відповідно, збільшення витрат енергії вузлів на передачу даних. І навпаки, в якості алгоритмів кластеризації можуть бути визначені FOREL (FORmal ELement), *к*-середніх та інші. На практиці доцільно використовувати алгоритм FOREL, який будує кластери, що фактично дорівнюють зоні покриття КА. Для отримання базового допустимого рішення пропонується ітераційний алгоритм адаптації розміру зони покриття КА.

ЯКЩО пріоритетна ЦФ T_{col}→min, ТОДІ визначити максимальне значення радіуса покриття R=Rmax та провести кластеризацію.

ЯКЩО пріоритетна ЦФ T_{op}→max, ТОДІ визначити мінімальне значення радіуса покриття R=Rmax та провести кластеризацію.

Для рішення двокритеріальної задачі оптимізації (3) пропонується використати лексикографічний метод. Для цього до моменту польоту КА наземний центр управління визначає пріоритет цільових функцій. Пропонується здійснювати пошук оптимального рішення за ієрархією згідно з пріоритетом ЦФ за наступними кроками [21]:

проводиться віртуальна кластеризація мережі згідно з визначеним алгоритмом кластерного аналізу – пропонується використовувати ітераційний алгоритм кластерного аналізу FOREL, який має певні переваги над іншими – мала обчислювальна складність, відповідність поняття кластера фізичному змісту зони покриття КА тощо;

будується найкоротший (або допустимої довжини) маршрут обльоту точок збору даних за певним алгоритмом рішення задачі комівояжера;

визначаються точки (інтервали) збору даних моніторингу КА в кластерах згідно з прийнятою стратегією обльоту кластерів та пріоритету цільових функцій (в простішому випадку точкою збору даних визначається центр кластера).

Відмітимо, що ефективність кінцевого рішення по досягненню цільових функцій та швидкість його отримання значною мірою визначається початковим рішенням по кластеризації (залежить від вибору початкової точки площі та радіусу покриття КА), алгоритму пошуку найкоротшого шляху обльоту, стратегією обльоту КА вузлів у кластері тощо.

Так час збору даних T_{col} КА з вузлів мережі залежить від наступних параметрів:

$$T_{col} = f(N, K, TR(St_k), v, V_{dmi}, Q_k, INT_i, s_{i-\text{КА}}(d_{i-\text{ТА}}, MAC), h_k, \Omega) \quad (5)$$

– кількості сенсорних вузлів s_i =1… N та координат їх розташування на місцевості (x_i, y_i);

– кількості $k = 1 \ldots K$ кластерів, їх площі, кількості вузлів у кластері n_k, взаємного розташування;

– траєкторії TR польоту КА в мережі, яка визначається стратегією St_k обльоту та збору даних з вузлів кожного k-кластера (збір даних у процесі польоту та/або при зависанні КА, одна або декілька точок зависання в кластері тощо);

– швидкості $v = \{v_m\}$ польоту КА на кожному з відрізків траєкторії $l_m, m = 1 \ldots M$;

– обсягу даних моніторингу V_{dmi} у вузлах мережі;

– кількості точок збору даних Q_k з координатами у просторі $(x, y, h)_k$ в кожному k-му кластері при зависанні КА;

– локації в просторі та часі інтервалів $INT_i = \{(x, y, h)_{begin}, (x, y, h)_{finish}, t_{begin}, t_{finish})\}_i$ траєкторії польоту КА, які визначені для збору (обміну) даних у русі з i-м вузлом;

– швидкості передачі MAC-протоколу $s_{i-TA}(d_{i-\text{КА}}, MAC)$, яка залежить від відстані d_{i-KA} та параметрів радіоканалу (співвідношення сигнал/шум), передавача, приймача, антен тощо;

– висоти польоту h_k, обмежень Ω ресурсів вузлів і КА тощо.

Збільшення часу функціонування мережі T_{fun} може досягатись:

зменшенням енерговитрат вузлів на прийом та передачу даних (зменшенням потужності передачі вузла) шляхом зменшення відстані КА-вузол

$$d_{i-TA} = g(K(R_k), n_k, TR_k, Q_k, INT_i),$$

яка досягається оптимізацією кількості кластерів K (розміром зони покриття R_k), кількістю вузлів у k-му кластері n_k, траєкторії TR_k, положенням точок Q_k (інтервалів INT_i) обміну в кластері;

перерозподілом витрат енергії між конкуруючими за передачу вузлами (якщо вузол має більший рівень енергії батареї, тоді він повинен витрачати більше енергії).

Крім того, при визначенні траєкторії обльоту вузлів кластера та обміну даними необхідно враховувати:

– взаємне розташування вузлів відносно траєкторії (обмін даними бажано робити в найближчих інтервалах траєкторії польоту КА від вузла);

– критичний рівень енергії батареї вузла (планувати обліт "виснажених" вузлів на мінімальній відстані);

– обсяг даних моніторингу вузла – вибір точки (інтервалу) збору траєкторії, які знаходяться ближче до цього вузла.

Для оцінки ефективності запропонованих різних способів (методів, алгоритмів, правил) процесу збору КА даних з вузлів БСМ була розроблена імітаційна модель. Вона написана мовою Python 3.11, має зручний інтерактивним інтерфейс, дозволяє візуально відслідковувати всі етапи процесу збору даних КА з вузлів мережі.

Вихідними даними для моделювання визначені наступні.

1. Характеристики мережі, вузлів, КА (згідно з постановкою задачі): S=1000×1000 умовних одиниць; N = 50…200; розміщення вузлів (однорідне, з групуванням), початкова енергія вузлів та обсяг даних моніторингу e_i; витрати енергії вузла на передачу (розраховуються за спрощеною формулою $e_{con} = c * d_{i-\text{КА}}^2$, де c =const, d – відстань між вузлом та КА); радіус покриття R; дальність радіозв'язності вузол-КА – $d_{i\text{-КА}}$; кількість раундів обльоту *Nround* тощо.

2. Способи (зі всієї площі, з кожного вузла, за кластерами), методи (безпосередньо з кожного вузла, з головних вузлів кластерів) збору даних.

3. Алгоритми тимчасової кластеризації мережі (FOREL, *k*-середніх тощо).

4. Алгоритми пошуку найкоротшого маршруту: евристичні (найближчого сусіда, клітинок, зовнішньої оболонки, тощо).

5. Правила кластеризації, визначення точок (інтервалів) збору даних на траєкторії польоту КА, правила обльоту кластера, правила побудови траєкторії КА тощо (таблиця 1) [21].

Таблиця 1

Ієрархія застосування алгоритмів по побудові траєкторії КА
для збору даних з вузлів БСМ

Етап рішення	**Алгоритми (параметри оптимізації)**	**Дія (алгоритм, правило)**	
		Цільова функція minT_{col}	**Цільова функція minE_{con}**
1. Віртуальна кластеризація БСМ (рівень мережі)	Алгоритми кластеризації Кількість та розмір однорідних кластерів R*, початкова точка кластеризації, кількість вузлів в кластерах, розмір кластера R_k	Зменшити кількість кластерів: збільшити R, визначити початкову точку кластеризації в місцях групування вузлів, перерозподіл вузлів між кластерами	Збільшити кількість кластерів: зменшити R зі збереженням зв'язності між вузлами кластера та КА
2. Пошук початкової траєкторії польоту КА (рівень мережі)	Алгоритм пошуку найкоротшого маршруту (траєкторії) обльоту центрів кластерів (первинних точок збору даних	Вибір кращого евристичного алгоритму з множини, оптимізація власних параметрів алгоритмів	–
3. Корегування точок збору даних в кожному кластері (рівень кластеру)	Положення точки (інтервалу) збору даних відносно траєкторії переміщення КА та розташування вузлів кластера	Правила скорочення траєкторії в кластері при забезпеченні радіозв'язності КА-найвіддаленіший вузол	–

Етап рішення	Алгоритми (параметри оптимізації)	Дія (алгоритм, правило)	
		Цільова функція minT_{col}	Цільова функція minE_{con}
4. Визначення стратегії збору даних в кластері (рівень кластеру)	Розташування траєкторії відносно положення вузлів в кластері, кількість та положення точок збору даних	Правила скорочення відстані КА-вузол, який має значний обсяг даних (зменшення часу обміну)	Правила зменшення відстані вузол-КА для витрат енергії батарей
5. Корегування точок (інтервалів) збору, розрахунок графіку обміну КА-вузли (рівень КА-вузол)	Кількість точок (довжина інтервалів) збору даних на відрізках траєкторії КА, швидкість польоту КА	Перерозподіл точок збору за відрізками траєкторії КА, вибір максимальної швидкості польоту при задоволенні часу обміну	Правила пріоритету обміну вузол-КА з меншим (малим) рівнем енергії батареї

Імітаційна модель надає можливість:

отримувати залежності показників ефективності – час збору даних (довжина траєкторії), витрати енергії батарей, час функціонування мережі) від множини керуючих параметрів (правил) побудови траєкторії польоту та збору даних КА при різних вхідних даних (розмірність мережі, тип розташування вузлів, кількість раундів обльоту тощо);

досліджувати параметри оптимізації – кількість та розміри кластерів, кількість та локація точок (інтервалів) збору даних на траєкторії польоту обльоту, стратегії обльоту кластерів; алгоритми пошуку найкоротшого маршруту тощо.

Проведемо моделювання та оцінку ефективності кожного з етапів рішення задачі побудови траєкторії КА для збору даних з вузлів та відповідних алгоритмів (правил) їх реалізації

1. Алгоритм кластеризації мережі – визначення розміру та кількості зон покриття КА

Зменшення кількості кластерів у мережі потенційно скорочує довжину маршруту польоту КА (відповідно час збору даних), але призводить до збільшення витрат енергії сенсорних вузлів (через збільшення відстані на передачу вузол-КА) та збільшення часу обміну вузол-КА (зменшується швидкість передачі MAC-протоколу). І навпаки. Тобто постає задача знаходження оптимуму кількості кластерів k^* та визначення їх розмірів R^*, визначення точок збору (Q_k) або інтервалів (INT_i) збору даних КА. Тому працюють наступні основні правила [21].

Правило з визначення кількості кластерів у мережі: ЯКЩО пріоритет ЦФ T_{col}→min (T_{fun}→max), ТОДІ збільшити (зменшити) розмір та кількість кластерів.

Результати дослідження запропонованого правила, при застосуванні різних евристичних алгоритмів пошуку найкоротшого шляху (найближчий сусід, за клітинками, випуклої оболонки) через центри кластерів представлені на рис. 3 та рис. 4 ($N = 100$, вузли мають координати, які вказані на рис. 2). Оптимізується розмір кластера R^* в межах значень $R = 50…100$ для кожного з алгоритмів. Відповідно до алгоритму кластеризації FOREL визначається кількість кластерів $k = 69…33$. Спостерігаємо, що для кожного алгоритму пошуку найкоротшого шляху існує оптимальне значення R^* ($R^*_{NN} = 94, R^*_{FPPWR}$=100, $R^*_{CHIH} = 100$), що дозволяє значно (більш ніж на 20 %) зменшити первинну довжину траєкторії польоту КА.

Для мережі з груповим розміщенням вузлів результати моделювання наведені на рис. 5.

Застосування інших мережевих правил (табл. 1) впливають на кількість кластерів та відповідно на довжину маршруту, витрати енергії на обмін даними КА з вузлами.

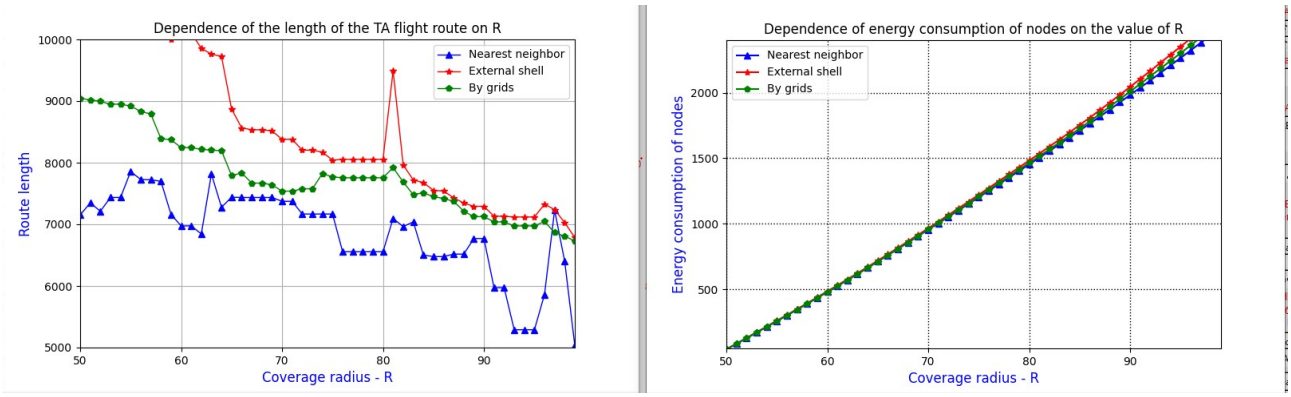


Рис. 4. Оцінка довжини траєкторії та витрат енергії вузлів від розміру зони покриття R при однорідному розміщенні вузлів при різних алгоритмах пошуку найкоротшого маршруту

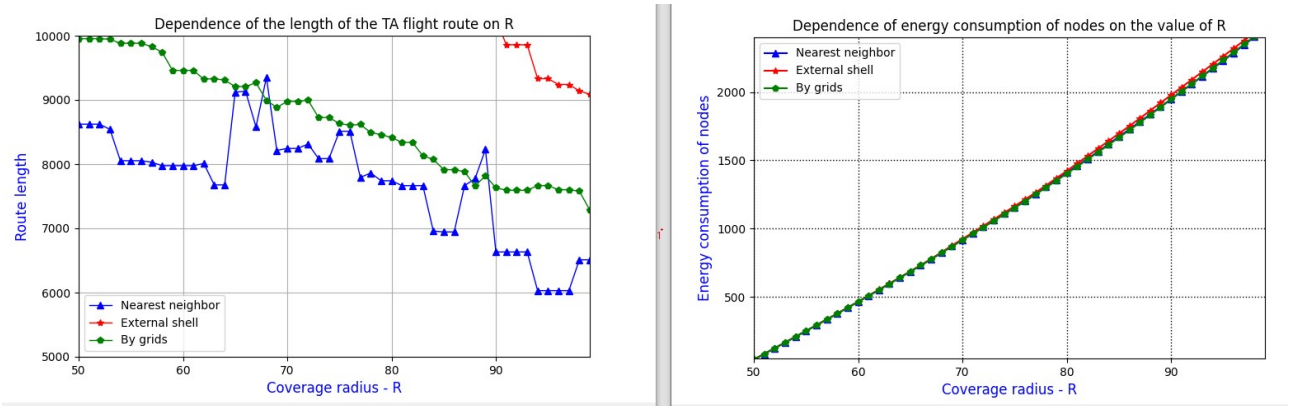


Рис. 5. Оцінка довжини траєкторії та витрат енергії вузлів залежно від розміру зони покриття R при груповому розміщенні вузлів

Правило вибору початкової точки кластеризації та порядку їх перебору: детермінований вибір та послідовний перебір; випадковий вибір та перебір; точку з максимальною кількістю вузлів в кластері та поступовим їх зменшенням.

Правило перерозподілу вузлів між кластерами: ЯКЩО в кластері незначна кількість вузлів ТОДІ за можливістю перерозподілити вузли цього кластеру по інших кластерах (тобто зменшити кількість кластерів).

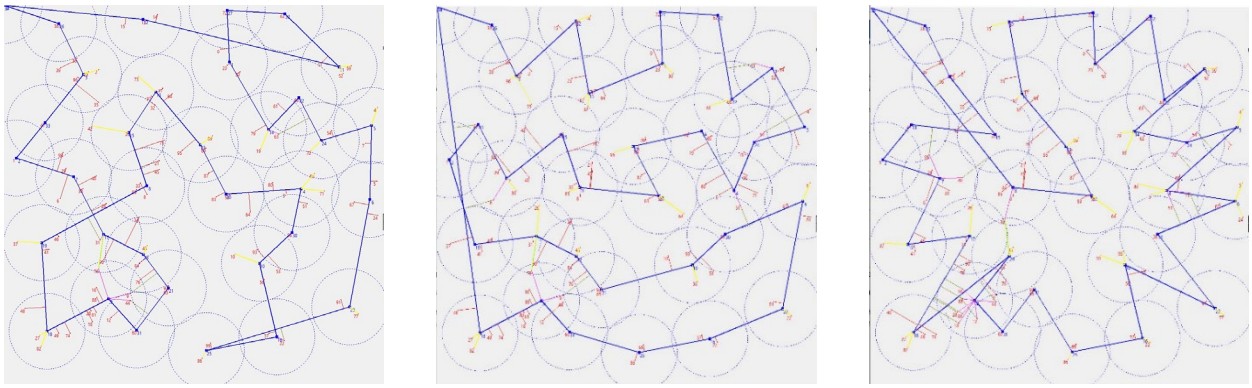
Правило адаптації розмірів кожного кластера: ЯКЩО ЦФ (2) ТОДІ зменшити R за рахунок зменшення висоти польоту КА зі збереженням зв’язності КА-вузлів кластеру.

Виграш застосування цих правил може досягати 5–7 %.

Тобто оптимізація радіуса зони покриття, застосування правил (вибору початкової точки кластеризації на етапі планування, перерозподіл вузлів між кластерами, адаптація розмірів кластерів) має суттєвий вплив на показники ефективності процесу збору даних при функціонуванні мережі.

2. Алгоритми пошуку найкоротшого маршруту (траєкторії) обльоту кластерів КА

Для рішення задачі пошуку найкоротшого маршруту обльоту кожного з кластерів також можуть бути застосовані різні відомі алгоритми: повного перебору (для малої кількості кластерів), евристичні, генетичні, тощо. Кожний з них показує різні результати залежно від параметрів мережі, вузлів та КА. На рис. 6–9 наведені показники ефективності (L, E_{con}, T_{fun}) при застосуванні трьох евристичних алгоритмів пошуку найкоротшого шляху (найближчого сусіда, за клітинками, зовнішньої оболонки) при однорідному та груповому розміщенні вузлів, розміру зони покриття (R = 50, 100), розмірності мережі (N = 100).



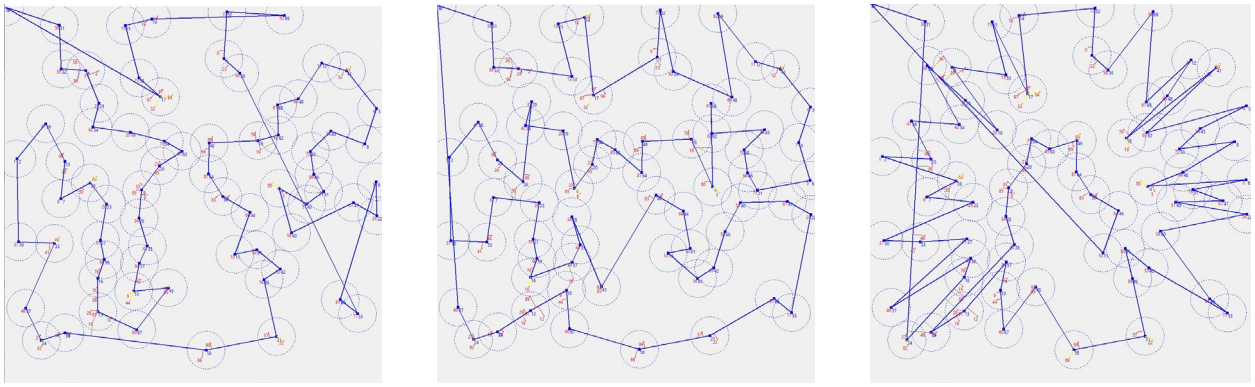
$L = 5987\ E_{con} = 3068\ (R = 100)$
а) найближчого сусіда

$L = 6596\ E_{con} = 3157\ (R = 100)$
б) за клітинками

$L = 6899\ E_{con} = 3290\ (R = 100)$
в) випуклої двошарової оболонки

Рис. 6. Результати моделювання траєкторії польоту КА в мережі з рівномірно розподіленими вузлами за різними алгоритмами пошуку найкоротшого маршруту (*N*=100, *R*=100)

Результати моделювання продемонстрували значну залежність показників ефективності від характеру розташування вузів на площі (однорідне, згрупуванням) та прийнятого алгоритму пошуку найкоротшого маршруту обльоту кластерів. В нашому випадку в більшості випадків перевагу з трьох визначених алгоритмів кращі показники ефективності має алгоритм найближчого сусіда.

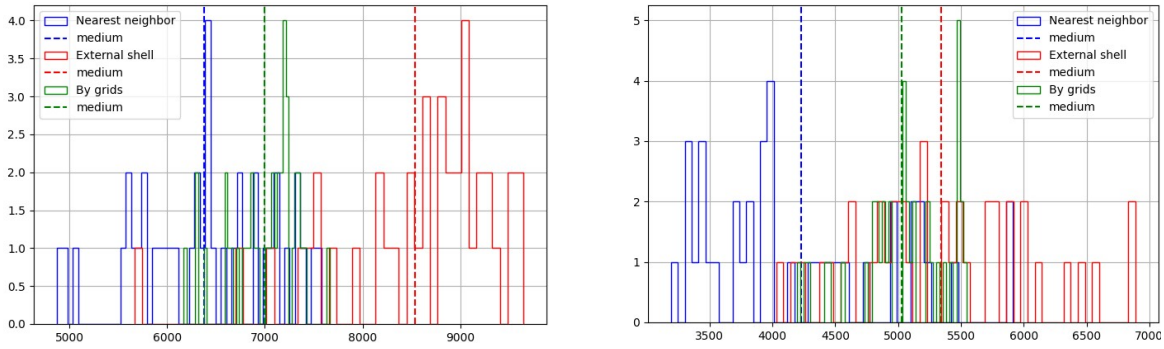


$L = 7153\ E_{con} = 2115\ (R = 50)$
а) найближчого сусіда

$L = 9042\ E_{con} = 2128\ (R = 50)$
б) за клітинками

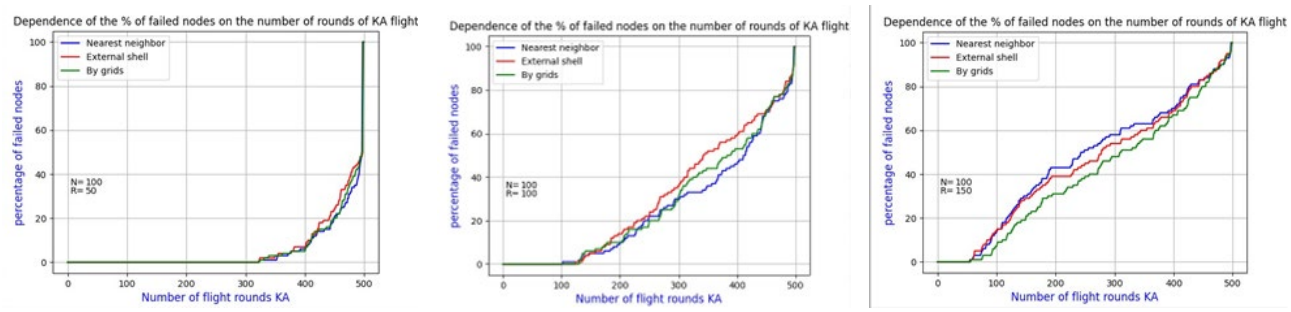
$L = 11844\ E_{con} = 2143\ (R = 50)$
в) випуклої оболонки

Рис. 7. Результат моделювання траєкторії обльоту КА кластеризованої БСМ з групуванням вузлів за різними алгоритмами пошуку найкоротшого маршруту (*N*=100, *R*=50)



а) рівномірне розміщення вузлів
б) групування вузлів

Рис. 8. Результати моделювання довжини маршруту польоту КА рівномірно розподілених та згрупованих вузлів в БСМ за різними алгоритмами пошуку найкоротшого маршруту (*R*=100, вибірка зі 100 випадкових розміщень вузлів на площі)



а) $R = 50$ б) $R = 100$ в) $R = 150$

Рис. 9. Залежності часу функціонування мережі від кількості раундів обльоту КА та радіусу покриття ($N = 100$ при $R = 50, 100, 150$)

Крім того, для кожного з алгоритмів існує додаткова можливість оптимізації за внутрішніми параметрами самих алгоритмів пошуку найкоротшого шляху. Наприклад, за алгоритмом найближчого сусіда – підбір кількості кроків до наступного кластера (один, два, три тощо), за квадратами (оптимізація розміру квадрата решітки), випуклої оболонки (оптимізація розміру кожної оболонки). При цьому для конкретних параметрів мережі (площа, розміщення, параметри вузлів, КА тощо) перевагу може мати кожний з них.

3. Правила обчислення (корегування) точок збору даних в кластері з скороченням довжини маршруту для покращення базового рішення (через центри кластерів).

Задача пошуку найкоротшого маршруту обльоту КА відрізняться від класичної задачі комівояжера. В нашій постановці задачі достатньо попадання вузла в зону покриття КА. Тому розглянемо евристичні правила скорочення маршруту відносно початкового рішення (п. 1, 2) (рис. 10) [19, 21].

Правила з скорочення довжини траєкторії польоту КА в кластері (рис. 10).

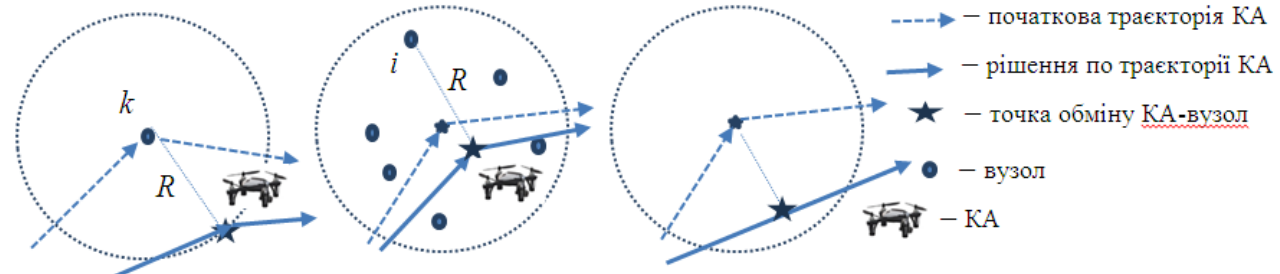


Рис. 10. Ілюстрація правил скорочення довжини траєкторії польоту та збору даних КА

ЯКЩО пріоритетна ЦФ $T_{col} \rightarrow \min$, початковий маршрут обльоту кластерів проходить через центр кластера з одним вузлом k, та наступний центр кластера не попадає в сектор напряму переміщення КА, ТОДІ в якості точки збору даних визначити точку на дотичній лінії, яка знаходиться на відстані R від нового маршруту в напряму переміщення КА (рис. 10, *а*).

ЯКЩО пріоритетна ЦФ $T_{col} \rightarrow \min$, початковий маршрут обльоту кластерів проходить через центр кластера, i-й вузол знаходиться на найбільшій відстані від траєкторії польоту КА, ТОДІ в якості точки збору даних визначити точку, яка знаходиться на відстані R від нового маршруту в напряму переміщення КА (рис. 10, *б*).

ЯКЩО пріоритетна ЦФ T_{col}→min, початковий маршрут обльоту кластерів проходить через центр кластера з одним вузлом k, та наступний центр кластера попадає в сектор напряму переміщення КА, ТОДІ траєкторію переміщення побудувати прямо до наступного центру кластера. в якості точки збору даних визначити точку на траєкторії, найближчу до центру кластеру (рис. 10в). За результатами моделювання застосування правил скорочення довжини маршруту можна зробити висновок: довжина траєкторії зменшується до 20 %, причому витрати енергії зростають не більш 10 %. За результатами моделювання (рис. 11) знову перемагає застосування евристики з алгоритмом найближчого сусіда, однак при інших параметрах мережі найкращі показники може показати будь-якій алгоритм пошуку найкоротшого маршруту.

4. Правила вибору точок (інтервалів) збору даних КА в кластерах (стратегії обльоту)

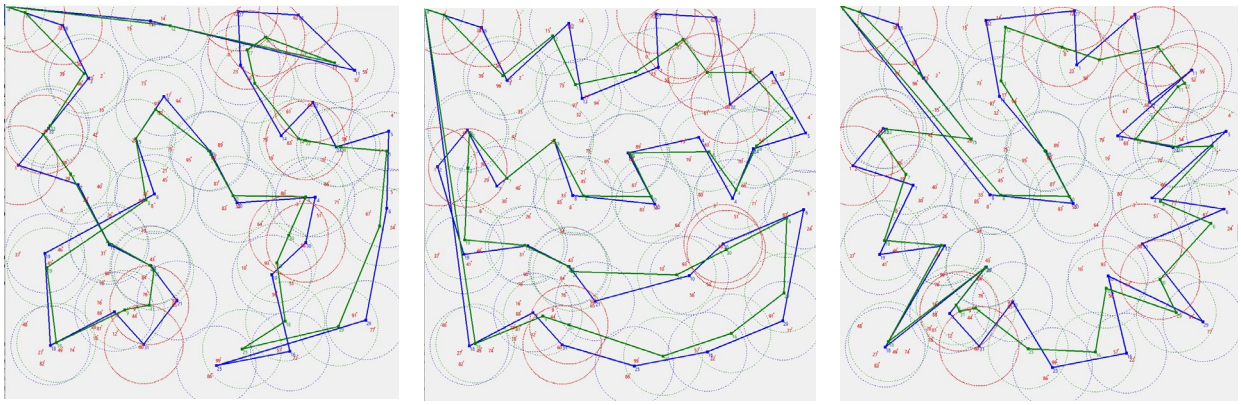
На рівні кластера визначається кількість та координати точок (інтервалів) збору даних КА (стратегія обльоту кластера). Можливі варіанти правил вибору точок показані на рис. 12 [18, 21]:

а – вибір точок обміну ближчих до траєкторії КА (через центр або центр «мас» кластера);

б – збір даних тільки при зависанні КА в центрі (центрі «мас») кластеру;

в – збір даних в процесі польоту з додатковою кластеризацією, якщо є групи вузлів;

г – збір даних в польоті з врахуванням малого рівня енергії батарей окремих вузлів.



$L = 5987$ $E_{con} = 3068$
$L_{\text{пр}} = 4999$ $E_{con\text{пр}} = 3212$
а) найближчого сусіда

$L = 6596$ $E_{con} = 3157$
$L_{\text{пр}} = 5117$ $E_{con\text{пр}} = 3244$
б) за клітинками

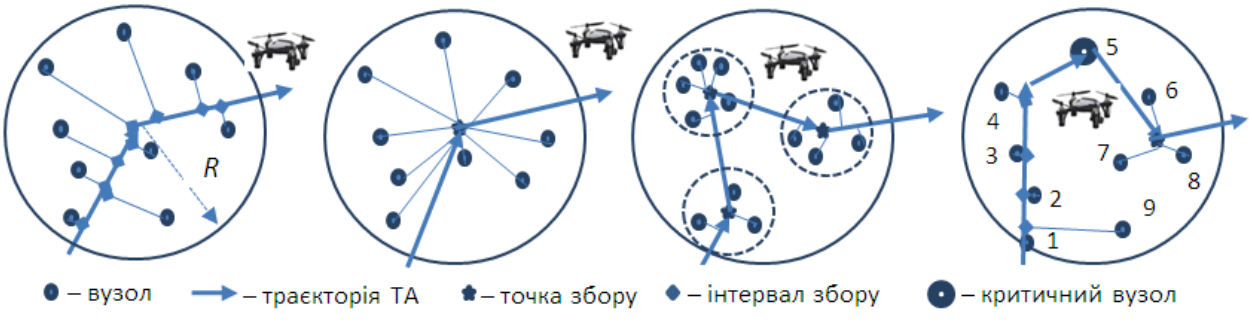
$L = 6899$ $E_{con} = 3290$
$L_{\text{пр}} = 5337$ $E_{con\text{пр}} = 3302$
в) випуклої двошарової оболонки

Рис. 11. Результати моделювання застосування правил по скороченню маршруту (*N*=100, *R*=100)

Результат кожної стратегії в k-му кластері оцінюється сукупністю параметрів:

– енергія витрат вузла кожного вузла кластера на збір (передачу та прийом) даних, сумарна енергія витрат вузлів кластера $E_{con}^{k} = \sum_{i \in k} e_{coni}$;

– час збору даних у кластері t_{con}^{k}, який визначається часом польоту та часом зависання КА.



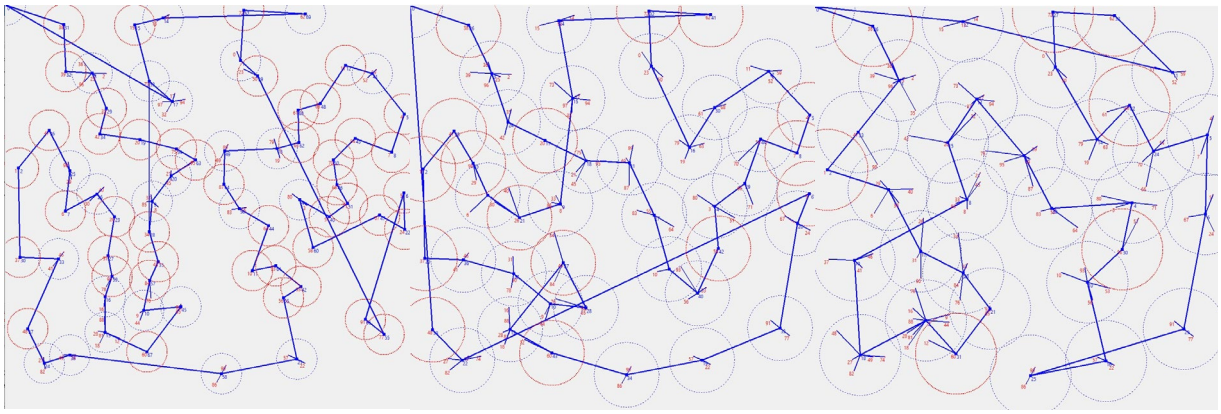
а) в процесі польоту б) тільки в центрі кластера в) з додатковою кластеризацією г) через критичні вузли

Рис. 12. Основні правила визначення точок (інтервалів) збору даних КА в кластері

Результати моделювання (рис. 13) показали зменшення витрат енергії вузлів при застосуванні стратегії збору даних у польоті (рис. 12, *а*) E_{contr} порівняно зі збором даних тільки в центрі кластеру E_{conz} (рис. 12, *б*) – до 20 % зниження витрат енергії вузлів на прийом та передачу (рис. 12). При наявності групування вузлів у кластері доцільно проводити їх додаткову кластеризацію з метою зменшення витрат енергії та зменшення часу обміну (рис. 12, *в*).

Правило з визначення точок зависання для збору даних: ЯКЩО в кластері є скупчення вузлів (навантажених або з малою енергією батарей), ТОДІ визначити точку зависання КА для збору даних з цих вузлів кластеру, яка мінімізує час обміну або витрати енергії цих вузлів.

Правило з корегування траєкторії польоту КА: ЯКЩО необхідно зменшити час передачі в радіоканалі вузол-КА та/або зменшити витрати енергії вузла, ТОДІ необхідно розмістити (перемістити) точки обміну на траєкторії КА ближче до вузла.



$E_{contr} = 2115\ (R = 50)$
$E_{conz} = 2210\ (R = 50)$
а)

$E_{contr} = 2512\ (R = 80)$
$E_{conz} = 2890\ \ (R = 80)$
б)

$E_{contr} = 3069\ (R = 100)$
$E_{conz} = 3841\ (R = 100)$
в)

Рис. 13. Результати моделювання двох стратегій збору даних
(по траєкторії та тільки в центрі кластера)

Правило зі зменшення та вирівнювання витрат енергії на передачу: ЯКЩО декілька вузлів конкурують за інтервали обміну з КА, ТОДІ визначити найближчий інтервал обміну *INT* на траєкторії польоту КА вузла з меншою енергією батареї.

Правила з визначення кількості та локації точок зависання, інтервалів обміну, стратегії обльоту та обміну в кластері: ЯКЩО ЦФ T_{col}→min, кількість вузлів в кластері

мала (середня) та обсяг даних незначний, ТОДІ визначити базову стратегію (прольот КА через центр кластера з визначенням інтервалів обміну на траєкторії польоту) (рис. 8, *а*);

ЯКЩО ЦФ T_{fun}→max, велика кількість вузлів в кластері, їхній обсяг даних значний, ТОДІ провести кластеризацію кластера з визначенням додаткових точок зависання (рис. 8, *г*).

5. ***Правило з перерозподілом вузлів за різними інтервалами траєкторії КА***

Кожна побудована траєкторія польоту КА складається з відрізків між точками збору, які можна оцінювати довжиною відрізка l_m та кількістю точок обміну. Якщо є інтервали траєкторії зі значною (дуже малою) кількістю точок збору, тоді намагаємось додати (забрати) до (від) неї вузли та повторно провести кластеризацію без врахування доданих (забраних) вузлів. Мета – скоротити довжину траєкторії або зменшити витрати енергії вузлів.

Правило перерозподілу точок збору даних: ЯКЩО відрізок траєкторії має значну (малу) кількість точок збору, ТОДІ зафіксувати цю ділянку траєкторії, викреслити (перерозподілити) вузли згідно з ЦФ та провести повторну кластеризацію мережі з метою досягнення певної ЦФ. Результати моделювання застосування запропонованого правила продемонстрували можливість отримання виграша за показниками ефективності до 8 %.

Інтервал обміну вузла і КА визначається з наступних міркувань: час польоту вузла КА повинен бути не меншим за час обміну КА-вузла [21].

Так як кожне правило орієнтовано на досягнення певної цільової функції та має різний результат її досягнення, тому запропонована їх ієрархія в вигляді метаправил. Наприклад [21].

Метаправило 1: ЯКЩО ЦФ T_{col}→min, ТОДІ (однокритеріальна оптимізація) знайти:

– максимальну (задану) кількість кластерів мережі;

– встановити базову траєкторію КА через центр кластерів, знайти найкоротший шлях (використати один алгоритм з множини для пошуку найкоротшого шляху) обльоту центрів;

– застосувати правила скорочення довжини маршруту, визначити можливі додаткові точки збору (зависання) КА відповідно до положення та обсягу даних у вузлах кластерів (групування вузлів зі значним обсягом даних);

– визначити стратегію обльоту вузлів кластерів;

– встановити максимальну швидкість руху КА в кластері, яка відповідає вимогам обміну даними КА з вузлами кластеру;

– розрахувати інтервали та графік передач вузлів під час польоту КА з врахуванням стану вузлів із застосуванням правил, які орієнтовані на збільшення швидкості передачі в радіоканалі.

Метаправило 2: ЯКЩО T_{col}→min та T_{fun}→max, перша ЦФ має пріоритет над другою, ТОДІ (лексикографічний метод оптимізації):

– знайти максимальну (визначену) кількість кластерів мережі;

– визначити точки збору (зависання) КА згідно з пріоритетом ЦФ;

– визначити стратегію обльоту вузлів кластерів;

– розрахувати траєкторію ТА через точки збору;

– розрахувати інтервали та графік передач вузлів під час польоту на мінімальній відстані з застосуванням правил, які враховують наявну енергію вузлів.

Оцінка ефективності застосування метаправил показала можливість скорочення до 20 % часу збору даних та збільшення до 15 % часу функціонування мережі в порівнянні з раніше запропонованими рішеннями. Важливо зазначити, що запропонована модель ситуаційного управління [21] може бути використана в спеціальному програмному забезпеченні системи управління збором даних ЦУМ та КА. Незначна обчислювальна складність моделі дозволяє застосовувати КА в автономному режимі та приймати (корегувати) рішення в реальному часі.

Висновки. Єдиним рішенням для збору даних з вузлів БСМ з незв'язною топологією є застосування КА. При цьому виникає задача побудови траєкторії польоту КА з визначенням

точок (інтервалів) збору даних для забезпечення основних цільових функцій: мінімум часу збору даних та/або максимум часу функціонування мережі.

Конкретна БСМ визначається багатьма параметрами: розміром площі та її формою; кількістю, координатами та щільністю розміщення вузлів, їх взаємним розміщенням; енергією батарей, обсягом даних моніторингу; обмеженнями параметрів вузлів та КА тощо. За допомогою розробленої імітаційної моделі проведені дослідження залежності показників ефективності збору даних від застосування різних алгоритмів (правил) побудови траєкторії польоту КА при визначених параметрах мережі, вузлів та КА. Доведено, що єдиного алгоритму (сукупності правил) пошуку траєкторії польоту КА, який забезпечує отримання оптимального рішення, для всіх варіантів БСМ та можливих ситуацій на мережі не існує.

Для оптимізації рішення по траєкторії польоту для збору даних КА запропонована база правил, яка реалізує ієрархію правил досягнення цільових функцій. Проведені дослідження дозволили визначити пріоритет та порядок застосування правил у базі (метаправил). Результати імітаційного моделювання довели, що застосування бази правил дозволяє зменшити час збору даних до 20 % або підвищити час функціонування мережі до 15 % в порівнянні з існуючими рішеннями. **Напрямом подальшого дослідження** є вдосконалення бази правил з побудови траєкторії польоту та збору даних КА з вузлів БСМ для інших цільових функцій управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Amodu, O.A.; Nordin, R.; Jarray, C.; Bukar, U.A.; Raja Mahmood, R.A.; Othman, M. A Survey on the Design Aspects and Opportunities in Age-Aware UAV-Aided Data Collection for Sensor Networks and Internet of Things Applications. Drones 2023, 7, 260. URL: https://doi.org/10.3390/ drones7040260.

2. Minh T. Nguyen, Cuong V. Nguyen, Hai T. Do, Hoang T. Hua, Thang A. Tran, An D. Nguyen, Guido Ala, and Fabio Viola. (2021). UAV-Assisted Data Collection in Wireless Sensor Networks: A Comprehensive Survey. Electronics. 10, 2603. DOI: 10.3390/electronics10212603.

3. Imad Jawhar, Nader Mohamed, Jameela Al-Jarood (2015) UAV-based data communication in wireless sensor networks: Models and Strategies. International Conference on Unmanned Aircraft Systems (ICUAS). DOI: 10.1109/ICUAS.2015.7152351.

4. V. Romaniuk, O. Lysenko, A. Romaniuk, O. Zhuk (2020). Increasing the efficiency of data gathering in clustered wireless sensor networks using UAV. Information and Telecommunication Sciences, 11 (1), 102–107. DOI: 10.20535/2411-2976.12020.102-107.

5. Zhiqing Wei, Mingyue Zhu, Ning Zhang, Lin Wang (2022). Zhiyong Feng UAV Assisted Data Collection for Internet of Things: A Survey. IEEE Internet of Things Journal 9(17): 1-1, DOI:10.1109/JIOT.2022.3176903.

6. Sarmad Rashedand Mujdat Soyturk (2017). Analyzing the Effects of UAV Mobility Patterns on Data Collection in Wireless Sensor Networks Sensors. 17, 413. DOI: 10.3390/s17020413.

7. Weihuang Huang, Jeffrey Xu Yu. (2017). Investigating TSP Heuristics for Location-Based Services Data Sci. Eng. 2: 71–93. DOI: 10.1007/s41019-016-0030-0.

8. Helsgaun K. (2017). An Extension of the Lin-Kernighan-Helsgaun TSP Solver for Constrained Traveling Salesman and Vehicle Routing Problems; Roskilde University: Roskilde, Denmark. DOI:10.13140/RG.2.2.25569.40807.

9. Hahsler M., Hornik, K. (2007). TSP – Infrastructure for the traveling salesperson problem. J. Stat. Softw., 23, 1–21.

10. Wu Yue, Zhu Jiang (2018). Path Planning for UAV to Collect Sensors Data Based on Spiral Decomposition. Procedia Computer Science 131, 873–879. DOI: 10.1016/j.procs.2018.04.29.

11. Chengliang W, Jun-hui Y (2015). Path Planning for UAV to Collect Sensor Data in Large-Scale WSNs. Transaction of Beijing Institute of Technology; 35: 1044–1049. DOI: 10.1016/j.procs.2018.04.291.

12. Kumar Nitesh, Prasanta K. Jana (2019). Convex hull based trajectory design for mobile sink in wireless sensor networks/International Journal of Ad Hoc and Ubiquitous Computing 30 (1): 26. DOI: 10.1504/IJAHUC.2019.097092.

13. Q. F., Yu W., Xiao K., Liu C., Liu W. (2022). Trajectory generation and optimization using the mutual learning and adaptive colony algorithm in uneven environments. Appl. Sci., 12, 4629. URL: https://doi.org/10.3390/app12094629.

14. Katoch S., Chauhan S.S., Kumar V. (2021). A review on genetic algorithm: past, present, and future. Multimed. Tools Appl., 80, 8091–8126. DOI: 10.1007/s11042-020-10139-6.

15. Emambocus B.A.S., Jasser M.B., Hamzah M., Mustapha A., Amphawan A. (2021). An enhanced swap sequence-based particle swarm optimization algorithm to Solve TSP. IEEE Access, 9, 164820–164836. DOI: 10.1109/ACCESS.2021.3133493.

16. Haider S.K., Jiang A., Almogren A., Rehman A.U., Ahmed A., Khan W.U., Hamam H. (2021). Energy Efficient UAV Flight Path Model for Cluster Head Selection in Next-Generation Wireless Sensor Networks. Sensors., 21, 8445. URL: https://doi.org/10.3390/s21248445.

17. Josiane da Costa Vieira Rezende, RoneIlídio da Silva and Marcone Jamilson Freitas Souza. (2020). Gathering Big Data in Wireless Sensor Networks by Drone. Sensors, 20, 6954. DOI: 10.3390/s20236954.

18. Dac-Tu Ho, EstenIngar Grotli, and Tor Arne Johansen (2013). Heuristic Algorithm and Cooperative Relay for Energy Efficient Data Collection with a UAV and WSN. International Conference Computing, Management and Telecommunications (ComManTel). DOI: 10.1109/ComManTel.2013.6482418.

19. Cariou, C., Moiroux-Arvis, L., Pinet, F., Chanet, J.-P. (2023). Evolutionary Algorithm with Geometrical Heuristics for Solving the Close Enough Traveling Salesman Problem: Application to the Trajectory Planning of an Unmanned Aerial Vehicle. Algorithms, 16, 44. URL: https://doi.org/10.3390/a16010044.

20. Nguyen, K. K., Duong, T. Q., Do-Duy, T., Claussen, H., & Hanzo, L. (2022). 3D UAV Trajectory and Data Collection Optimization via Deep Reinforcement Learning. IEEE Transactions on Communications. DOI: 10.1109/TCOMM.2022.3148364

21. Hrymud A., Romaniuk V. (2023). A model of situational control of the telecommunication aerial platform flight trajectory to collect data from nodes of a wireless sensor network. Communication, informatization and cyber-security systems and technologies, № 3. p. 88–100. DOI: 10.58254/viti.3.2023.12.101.

DOI: 10.58254/viti.6.2024.16.204

УДК 621.391

д-р техн. наук Сайко В. Г. ORCID: 0000-0002-3059-6787 (ВІТІ ім. Героїв Крут)
Романов Д. О. ORCID: 0009-0008-5522-7591 (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)

МЕТОД ВИЗНАЧЕННЯ КООРДИНАТ МАЛОВИСОТНОГО ОБ'ЄКТА ЗА УМОВИ ВИКОРИСТАННЯ ДЕКІЛЬКОХ ПРОМЕНІВ РАДІОСИГНАЛІВ

Нині у великих містах спостерігається стійка тенденція до збільшення просторової щільності телекомунікаційних систем. Насиченість радіоспектра аналоговими та цифровими системами, що використовуються для вирішення завдань радіозв'язку та телебачення, дозволяє на їх основі удосконалювати технології напівактивного радіолокаційного виявлення та визначення координат маловисотного об'єкта.

Здійснення радіолокаційного спостереження з використанням передавачів нерадіолокаційного призначення часто називають напівактивною радіолокацією з використанням сторонніх або паразитних джерел випромінювання.

Перевагами таких систем є мінімізація витрат на розгортання, незначні експлуатаційні енерговитрати, низька ймовірність встановлення завад, скритність факту роботи, екологічність та відсутність вимог до виділення радіочастотного ресурсу. Відносно великі висоти піднятя антен зв'язкових і телевізійних передавачів за наявної випромінюваної потужності створюють сприятливі умови виявлення маловисотних об'єктів.

Цифрові сигнали сучасних телекомунікаційних систем мають ширину спектра, що забезпечує прийнятну роздільну здатність та точність вимірювання сумарної дальності та кутових координат [20; 21]. Загалом системи такого типу являють собою багатопозиційну систему, що складається з одного або декількох джерел випромінювання та однієї або кількох приймальних позицій, рознесених у просторі [22; 23].

У роботі наведено загальну характеристику запропонованого методу визначення координат повітряного об'єкта на малій висоті за умов розповсюдження декількох променів радіосигналів.

Визначено метод і його технічне рішення щодо здатності визначати координати несанкціонованого маловисотного об'єкта за умов існування декількох променів розповсюдження радіосигналу та представлено алгоритм його функціонування, необхідний для технічної реалізації запропонованого методу.

У роботі розглянуто варіанти визначення координат повітряних об'єктів при різному складі первинних вимірювань координат і кількості приймальних пунктів.

Здійснено оцінку точності визначення місця розташування об'єкта для багатопозиційних радіосистем такого типу за умов існування декількох променів розповсюдження радіосигналу в розробленій моделі з врахуванням кількості сигналів, що приймаються, та помилки їх вимірювання.

Ключові слова: *приймальний пункт, визначення координат, станція радіолокації, маловисотний об'єкт, супровід до виявлення, багатопозиційні радіосистеми, терагерцовий діапазон.*

V. Saiko, D. Romanov, G. Radzivilov, V. Komarov, M. Fomin. Method of determining the coordinates of a low-altitude object under the conditions of using several radio signals

Currently, in large cities, there is a steady tendency to increase the spatial density of telecommunication systems. The saturation of the radio spectrum with analog and digital systems used to solve the problems of radio communication and television allows to improve the technologies of semi-active radar detection and determination of the coordinates of a low-altitude object on their basis.

Conducting radar surveillance using non-radar radar transmitters is often called semi-active radar using extraneous or parasitic radiation sources. The advantages of such systems are the minimization of deployment costs, low operating energy costs, low probability of malfunctioning, stealth of the fact of operation, environmental friendliness, and the absence of requirements for the allocation of radio frequency resources. Relatively high heights of antennas of communications and television transmitters with the existing radiated power create favorable conditions for detecting low-altitude objects. Digital signals of modern telecommunication systems have a spectrum width that provides acceptable resolution and accuracy of measuring the total distance and angular coordinates [20; 21]. In the general case, systems of this type are a multi-position system consisting of one or more radiation sources and one or more receiving positions spread in space [22; 23].

The paper gives a general description of the proposed method of determining the coordinates of an aerial object at low altitude under the conditions of propagation of several beams of radio signals. The method and its technical

solution capable of determining the coordinates of an unauthorized low-altitude object under the conditions of the existence of several rays of radio signal propagation are defined, and the algorithm of its operation necessary for the technical implementation of the proposed method is presented.

The paper considers options for determining the coordinates of aerial objects with different composition of primary coordinate measurements and the number of receiving points. The accuracy of determining the location of the object for multi-position radio systems of this type was evaluated under the conditions of the existence of several beams of radio signal propagation in the developed model, taking into account the number of received signals and their measurement errors.

Keywords: *reception point, determination of coordinates, radar station, low-altitude object, tracking to detection, multi-position radio systems, terahertz range.*

Постановка завдання у загальному вигляді

Особливості маловисотних об'єктів (МВО), що розглядаються як об'єкти радіолокаційного спостереження, до яких можна віднести екстремально низькі значення ефективної поверхні розсіювання (ЕПР) порядку 0,01…0,001 м^2, малі висоти та швидкості польоту до 50 м/с, викликають необхідність коригування традиційних підходів до вибору параметрів, а також алгоритмів функціонування пристроїв первинної та вторинної обробки радіолокаційної інформації.

Автори вважають, що необхідно застосувати сучасні наукові розробки, в яких застосовують додаткові радіосигнали від побутових передавачів FM-діапазону і DAB – радіо, цифрового телебачення (DVB-T, DVB-T2) та сигналів базових станцій (БС) стільникового зв'язку, корисних для виявлення та фіксації координат МВО [1–5]. Наразі такі відомі компанії, як Lockheed Martin (США), Thales (Франція), Leonardo (Італія), ERA (Чеська Республіка) та ін., проводять ефективні спроби створення спеціальних радіолокаційних комплексів, які одночасно використовують декілька додаткових передавачів різних діапазонів частот. Автори вважають, що утворення та використання низьковисотного радіолокаційного простору поширить можливості штатних засобів радіоконтролю та суттєво покращить точність, надійність та достовірність радіолокаційного моніторингу повітряного простору на малій висоті [3; 4].

Важливою умовою реалізації ефективної обробки радіолокаційної інформації в системах подібного типу є визначення координати на МВО за умови існування та розповсюдження декількох променів радіосигналів.

Аналіз публікацій за темою досліджень

У роботі [1] описана експериментальна багатопозиційна радіолокаційна система, яка виявляє та відстежує цілі на дальностях більше 150 км від приймача, використовуючи ехосигнали радіопередавача FM.

У роботі [4] обґрунтовано використання телевізійного передавача в багатопозиційній радіолокаційній системі, що дозволяє виявляти МВО в діапазоні до 260 км, оцінювати їхні декартові координати з використанням розширеного фільтра Калмана.

У роботі [5] представлено дослідження та дані щодо використання радіолокаційних систем стандарту LTE, здатних бути корисними для виявлення рухомих БпЛА.

Варто зазначити, що перелічені роботи, по суті, є розвитком досліджень, проведених з урахуванням специфіки розвитку радіолокаційної техніки та сучасних вимог, що висуваються до радіотехнічних систем.

Відомий метод зменшення помилок багатопроменевості при визначенні координати джерела випромінювання за допомогою далекомірних вимірювань полягає в тому, що координати джерела визначають за допомогою алгоритму зважених залишків координатних оцінок, отриманих на основі вимірювань від використання даних від різних комбінацій приймальних станцій [6]. Недоліком цього методу є те, що для оцінки координати джерела випромінювання потрібен значний час, оскільки необхідно накопичувати й зважувати

проміжні оцінки протягом певного періоду, що робить його непридатним для визначення координат рухомих джерел випромінювання.

Існує також метод зменшення багатопроменевих помилок при визначенні координати джерела випромінювання різницево-далекомірним способом, де обробка даних здійснюється на основі різницевих вимірювань після призначення ваг для приймальних станцій, які є ймовірними джерелами віддзеркалених сигналів [7]. До недоліків цього підходу належать:

залежність достовірності визначення ваги від вибору проміжної оцінки координат для заданого набору;

ризик помилкового вибору проміжної оцінки (наприклад, завдяки усередненню оцінок у межах певної комбінації або завдяки усередненню по всіх можливих комбінаціях), що може призвести до зміщення ваг;

можливість помилкового призначення ваги в ситуаціях, коли є більше одного приймального пункту (ПП) з віддзеркаленими сигналами, що може призвести до значної помилки у визначенні координати.

В роботі [8] представлено відомий спосіб визначення координат повітряного об'єкта різницево-далекомірним методом в умовах декількох променів розповсюдження радіосигналу, який полягає в тому, що:

координати об'єкта знаходять шляхом виявлення дії декількох радіопроменів;

здійснюється виключення з обробки частини сигналів згідно з різницею часу приходу сигналів (TDOA – *Time Difference of Arrival*), що мають найбільший розкид багатопроменевої затримки часу приходу сигналу (TOA – *Time of Arrival*);

враховуються показники рівня прийнятого сигналу (RSSI – *Received Signal Strength Indication*);

враховуються співвідношення сигнал/шум (SNR), коли коефіцієнт виявляється нижче за певний поріг.

До недоліків відомого способу визначення координати повітряного об'єкта різницево-далекомірним методом в умовах існування декількох променів розповсюдження сигналу є наступні особливості:

тривалий час оцінювання координат, викликаний необхідністю прийому та вимірювання часу приходу послідовності сигналів в невизначеному інтервалі часового періоду;

відсутність можливості застосування вищевказаного метода для визначення місцезнаходження рухомого повітряного об'єкта.

Тому авторами було обрано найбільш близький метод і технічне рішення, що за своєю суттю та вирішуваною задачею є найближчим аналогом (прототипом), цє спосіб визначення координати МВО в умовах існування декількох променів розповсюдження сигналів/у.

Ідея запропонованого методу полягає в наступному:

від кожного з ПП, координати яких відомі, приймають віддзеркалений від МВО радіосигнал;

надалі вимірюють час приходу радіосигналу;

формують набір проміжних оцінок координат МВО різницево-далекомірним методом для кожної можливої комбінації з трьох або більше ПП;

на основі проміжних оцінок формують підсумкову оцінку координат МВО;

остаточне визначення місцезнаходження МВО здійснюють на основі підсумкової оцінки координат.

Цей метод має деякі вади, наприклад, те, що при пошуку сигналів не враховується взаємний вплив компонент декількох променів радіосигналу, що підвищує ймовірність застосування хибних радіопроменів. Крім того, метод не оптимізує кількість променів під час використання терагерцового діапазону хвиль, що збільшує вимоги до апаратури без поліпшення точності визначення координат. Також для досягнення заданого порога

використовують емпіричну залежність дисперсії розрахунків координат від співвідношення сигнал/шум, що потребує великої кількості попередніх вимірювань і значного часу для реалізації розрахунків.

Постановка завдання

Метою цієї статті є розробка інноваційного способу та технічного рішення визначення координат МВО за умов існування декількох променів розповсюдження радіосигналу, достатніх для покращення достовірності розрахунків відстані щодо однопозиційних радіолокаційних ПП, а також забезпечення можливості прийому радіосигналів невеликого рівня у віддзеркаленому багатопроменевому радіопросторі.

Виклад основного матеріалу

1. Загальна характеристика розробленого методу визначення координати МВО за умов існування декількох променів розповсюдження сигналу.

В основу розробленого методу визначення координати МВО за умови існування декількох додаткових променів радіосигналу покладено завдання використання деяких технологічних операцій, які передбачають наступне:

оперативне розгортання мережі ПП на базі приймально-передавальних цифрових радіорелейних систем (ЦРС) терагерцового діапазону;

інтегрування ПП ЦРС в діючу мережу БС мобільного зв’язку;

проведення постійного сканування зон обслуговування БС мобільного зв’язку системами сканування, які побудовані на основі ЦРС терагерцового діапазону;

формування тимчасового кластеру збору даних вимірювань із семи груп ПП для передачі даних сканування до пункту обробки вимірювань (ПОВ) цього кластеру;

періодичне визначення на приймальних пристроях усіх груп ПП числа і часових затримок різних компонент віддзеркалених променів радіосигналу;

забезпечення підвищення ефективності мережі ПП на базі приймально-передавальних ЦРС терагерцового діапазону;

використання спільних часових, спектральних ресурсів й апаратних компонентів, підвищення точності вимірювань дальності щодо однопозиційних радіолокаційних систем;

можливості прийому променів низького рівня у віддзеркаленому багатопроменевому сигналі.

Ключовою відмінністю технічного рішення (що заявляється) від традиційних сучасних рішень є те, що для забезпечення визначення координати МВО за умов існування декількох променів розповсюдження радіосигналу розгортається мережа ПП, яка виконує функції сканування і функції мобільних гетерогенних шлюзів [9–11].

Для екстрених служб на основі групи БС з ЦРС для кожного кластеру створюється безпроводова мережа, що швидко розгортається та дозволяє скоротити час, необхідний для виявлення несанкціонованого МВО. Також передбачається можливість зменшити кількість персоналу, що залучаються для операції з виявлення координат МВО. Крім того, у технічному рішенні (що заявляється) на усіх ПП періодично визначають число і часові затримки компонент декількох променів радіосигналу. Це дозволяє ефективно забезпечити прийом слабких променів у багатопроменевому радіосигналі шляхом їх адаптації до умов розповсюдження, що змінюються, в каналі зв’язку, завдяки періодичному відділенню/виокремленню області багатопроменевості, періодичному пошуку і використанню у кожному періоді різних радіопроменів.

Завдяки використанню у технічному рішенні (що заявляється) більш широкої смуги пропускання в терагерцовому діапазоні, роботі з декількома діапазонами та збільшеній апертурі антенної решітки забезпечується високоточна роздільна здатність для поділу декількох променів розповсюдження та використання інформації про багатопроменеве розповсюдження для кращої локалізації та визначення координат МВО.

2. Алгоритм функціонування розробленого способу визначення координати МВО за умов розповсюдження декількох променів радіосигналу.

Етап 1: спочатку розгортають мережу ПП на основі приймально-передавальних ЦРС терагерцового діапазону, інтегровану в існуючу мережу БС мобільного зв’язку з ПОВ даних.

Етап 2: синхронізують роботу всіх ПП у зонах обслуговування БС мобільного зв’язку через механізм синхронізації.

Етап 3: здійснюють безперервне сканування зон обслуговування БС мобільного зв’язку за допомогою систем сканування на основі ЦРС терагерцового діапазону.

Етап 4: приймають віддзеркалений радіосигнал від МВО на кожному з ПП з відомими координатами.

Етап 5: після фіксації радіосигналу першим ПП від МВО передають інформацію про виявлення невідомого об’єкта через канали сигналізації або оповіщення.

Етап 6: формують тимчасовий кластер для збору даних із семи груп ПП і передають ці дані на ПОВ.

Етап 7: за допомогою передавача першого ПП випромінюють радіосигнал зондування на МВО для подальшого збору даних.

Етап 8: приймають віддзеркалений радіосигнал одночасно першим та іншими шістьома ПП, що генерують запитні радіосигнали з цих пунктів.

Етап 9: активують механізм сканування прийому і випромінювання радіосигналів іншими шістьма групами ПП, що дозволяє отримати додаткові вимірювання.

Етап 10: визначають кількість і часові затримки компонентів/компонент декількох променів радіосигналу на всіх ПП.

Етап 11: вимірюють час приходу радіосигналів.

Етап 12: комбінують всі можливі пари ПП із семи груп для отримання проміжних оцінок координат МВО.

Етап 13: вимірюють різницю часу приходу декількох променів радіосигналу від МВО до кожної пари ПП.

Етап 14: на основі різниці часу приходу радіосигналу обчислюють різницю відстаней від МВО до кожної пари ПП.

Етап 15: формують набір проміжних оцінок координат МВО різницево-далекомірним методом для кожної можливої комбінації з трьох ПП, використовуючи дані кластера.

Етап 16: на основі проміжних оцінок формують підсумкову оцінку координат МВО.

Етап 17: після отримання сигналів від усіх груп ПП кластеру, ці дані передають на пункт обробки через мережу БС, де відбувається накопичення та об’єднання даних. Остаточне визначення координати МВО здійснюється на основі підсумкової оцінки.

Технічний результат, як метод визначення координати МВО за умов існування декількох променів розповсюдження радіосигналу, полягає у підвищенні точності вимірювань відстані щодо однопозиційних радіолокаційних систем, а також забезпеченні можливості прийому радіопроменів низького рівня у віддзеркаленому багатопроменевому радіопросторі.

Зазначений результат досягається тим, що у запропонованому способі застосовуються ЦРС в терагерцовому діапазоні, які використовуються як високороздільні радари, що виявляють МВО, який швидко рухається. Також використання ЦРС терагерцового діапазону як систем сканування дозволить системі мобільного зв’язку мати функціональні характеристики систем сканування і забезпечити оптимізацію продуктивності мережі БС мобільного зв’язку, що включає в себе підвищення спектральної ефективності та надійності при мінімізації затримки. Для підвищення ефективності ці системи можуть використовувати такі спільні ресурси, як час, спектр і форму сигналів – безперервну хвилю з трапецеїдальною частотною модуляцією [10; 11], а також апаратні компоненти.

Крім того, використання терагерцових частот забезпечує високий рівень безпеки передачі даних в інтегрованій існуючій мобільній мережі для екстрених служб, яка включає в себе одну або кілька мобільних БС з ЦРС, оскільки цей діапазон частот мало використовується, що робить складним перехоплення сигналів і втручання в передачу [11; 12].

Технічне рішення (що заявляється) додатково дозволяє ефективно забезпечити прийом інформації слабких радіопроменів у багатопроменевому радіопросторі шляхом адаптації до умов розповсюдження, що змінюються, в каналі зв’язку, завдяки періодичному відділенню/виокремленню багатопроменевих областей, періодичному пошуку і використанню на кожному періоді оновлених радіопроменів.

Іншою важливою перевагою цього способу є те, що можливість високоточної оцінки координат, отриманої за один цикл обробки інформації в системі, дає суттєвий часовий виграш в загальному процесі визначення місцезнаходження МВО.

3. Технічні аспекти розробленого способу визначення координати на МВО за умов існування декількох променів розповсюдження радіосигналу для технічної реалізації запропонованого методу.

Суть способу визначення координати МВО за умов існування декількох променів розповсюдження радіосигналу для технічної реалізації запропонованого методу, що заявляється, пояснюється кресленнями, де на рисунку 1 зображено геометричний підхід до визначення координат МВО на основі нового створеного кластеру.

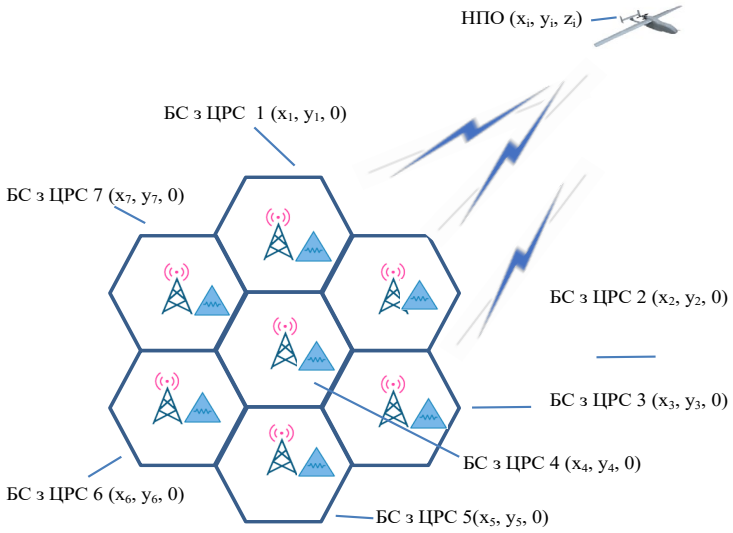


Рис. 1. Геометричний підхід до визначення координат МВО
на основі кластеру із семи груп ПП

Спосіб визначення координати несанкціонованого МВО за умов декількох променів розповсюдження радіосигналу, що заявляється, здійснюють наступним чином.

На першому етапі попередньо розгортають мережу ПП на базі ЦРС терагерцового діапазону, яка інтегрується в діючу мережу БС мобільного зв’язку з ПОВ, синхронізують роботу усієї множини ПП різних зон обслуговування БС мобільного зв’язку за допомогою механізму синхронізації, проводять постійне сканування зон обслуговування БС мобільного зв’язку системами сканування, які побудовані на основі ЦРС терагерцового діапазону, за допомогою механізму сканування.

Далі приймають віддзеркалений сигнал від МВО на кожному із множини ПП з відомими координатами, після приймання віддзеркаленого сигналу від першого ПП з загальної множини ПП. По каналах сигналізації передають інформацію про факт фіксації невідомого об’єкта

у зоні функціонування першого ПП, формують тимчасовий кластер збору даних вимірювань з семи груп ПП для передачі даних сканування до ПОВ цього кластеру, випромінюють передавальним пристроєм ЦРС першого ПП сигнал зондування до МВО.

Для збору й обробки даних зондування приймають ретрансляційний віддзеркалений сигнал від МВО одночасно першою та іншими шістьома групами ПП цього кластеру. Це призводить до генерації запитаних сигналів з ПП цього кластеру.

Із практичної точки зору, тимчасовий кластер БС з ЦРС у запропонованому способі складається з семи мобільних БС з ЦРС (див. рис. 1).

Далі запускають механізм процесу сканування випромінювання і прийому сигналів другою, третьою, четвертою, п'ятою, шостою та сьомою групами ПП, що дозволяє отримати додатково шість вимірювань похилої відстані і дванадцять вимірювань суми відстаней. Такий процес відбувається за алгоритмом, наведеним у [12; 13]. На приймальних пристроях усіх семи груп ПП періодично фіксують число і часові затримки компонентів декількох променів радіосигналу.

Для цього визначають часову область багатопроменевості, проводять пошук сигналу в області багатопроменевості та визначають оцінку числа і часових затримок компонент декількох променів радіосигналу, формують оновлені числа і часові затримки компонент різних променів радіосигналу. Знаходять часові затримки компонент променів сигналу поточного періоду, постійно уточнюючи оновлені часові затримки, а також визначають часовий термін обробки компонент променів радіосигналу на основі відповідних рівнянь, формують рішення по прийнятим компонентам багатопроменевого радіосигналу.

Далі вимірюють час приходу радіосигналу з семи груп ПП кластеру. Складають усі можливі пари ПП для формування набору проміжних оцінок координат МВО. Вимірюють для кожної пари ПП різницю часу приходу різних променів радіосигналу МВО до ПП цієї пари. Обчислюють по вимірюваній різниці часу приходу сигналу МВО у кожній парі різницю відстані від МВО до ПП цієї пари.

Після визначення відстані до МВО необхідно обчислити його координати. Для цього формують набір проміжних оцінок координат МВО різницево-далекомірним способом для кожної можливої комбінації з трьох ПП, при цьому формування набору проміжних оцінок координат МВО проводиться з урахуванням даних кластеру з семи груп ПП. Далі на основі набору проміжних оцінок координат МВО формують підсумкову оцінку його координат.

Закінчується технологічний процес формуванням підсумкової оцінки координат МВО ПОВ координат невідомого МВО, коли сигнали від усіх семи груп ПП кластеру прийняті та передаються на ПОВ по каналах діючої мережі БС мобільного зв'язку з подальшим їх накопиченням та комплексуванням, а визначення координати МВО здійснюють на підставі підсумкової оцінки його координат.

На рисунку 1 вищевказаний процес пояснюється наступним чином. Припустимо, що істинна позиція несанкціонованого МВО – p (x_i, y_i, z_i), а на землі БС з ЦРС отримують віддзеркалений від цього МВО сигнал позиції p_i (x_i, y_i, 0). Відстань між цими двома точками розраховується з урахуванням похибки вимірювання, що встановлюється під час сканування. Із кожним отриманим сигналом з несанкціонованого МВО, відстань від нього до мобільної БС з ЦРС визначається виразом (1):

$$d(p_i, p_o) = \sqrt{(x_i - x_0) + (y_i - y_0) + (z_0)^2} + \varepsilon, \quad (1)$$

де ε – похибка вимірювання.

Таким чином, кількість радіосигналів, що приймаються, і похибка вимірювання ε впливають на точність процесу позиціонування. Позиція p_k (x_k, y_k) визначається шляхом мінімізації виразу (2):

$$arg\ min\ \sum_{i=1}^{m}(\sqrt{(x_i - x_k) + (y_i - y_k) + (z_0)^2} - d(p_i, p_k)), \quad (2)$$

де m – кількість радіосигналів, що приймаються від несанкціонованого МВО.

В результаті мінімізації стає можливим обчислити координати МВО та їхні похибки.

Таким чином, для оцінки можливості визначення координат на основі радіосигналу, що приймається, в розробленій моделі враховується кількість радіосигналів, що приймаються, та помилки їх вимірювання.

Моделювання дозволяє визначити щільність помилки визначення координати при зміні кількості виявлених радіосигналів. На рисунках 2, 3 показано щільність імовірності помилки визначення координати при отриманні 40 та 5 сигналів відповідно з відносною похибкою вимірювання відстані 15 %.

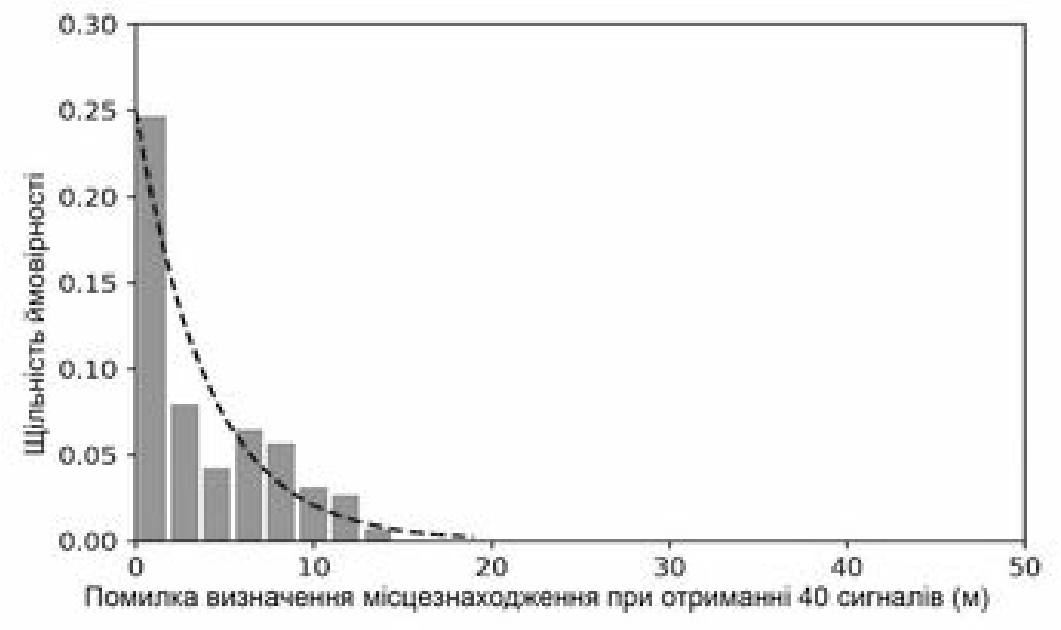


Рис. 2. Щільність ймовірності та гістограма помилки визначення координати при отриманні 40 сигналів

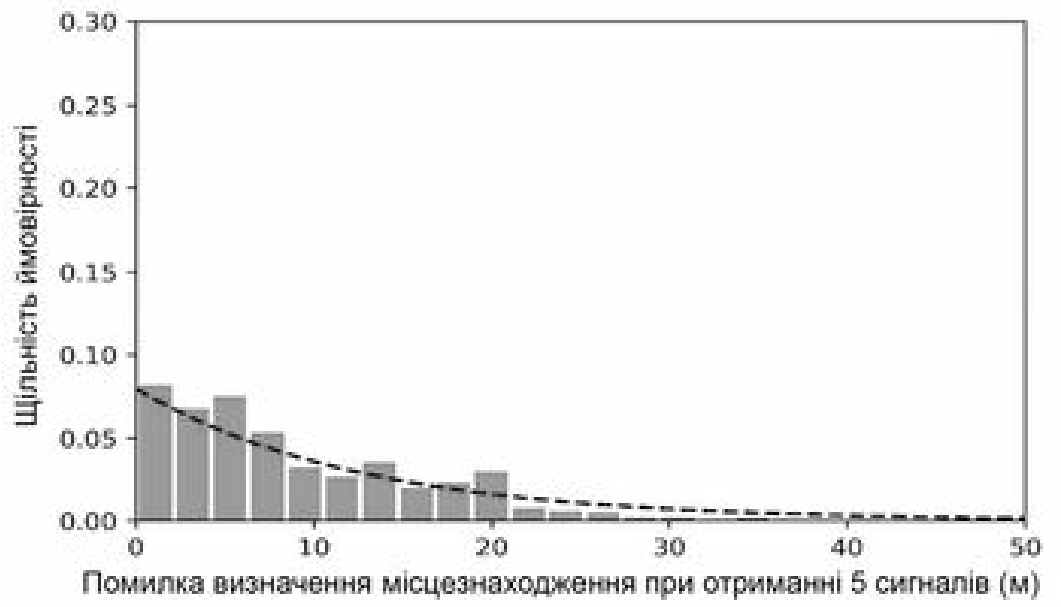


Рис. 3. Щільність ймовірності та гістограма помилки визначення координати при отриманні 5 сигналів

Результати моделювання показують, що помилка визначення координати збільшується, коли збільшується помилка вимірювання відстані. Враховуючи отримані залежності, точність визначення координати може бути досягнута шляхом підвищення якості вимірювання відстані та забезпечення виявлення обробки більшої кількості радіосигналів.

Неможливість успішного вирішення задачі виявлення малорозмірних цілей (зі значенням ЕПР порядку $10^{-3}…10^{-2}$ м^2) при використанні відомих методів виділення сигналів на фоні завад призвела до появи нових методів виявлення, що реалізують спільну обробку сигнальної та траєкторної інформації за кілька циклів огляду системою або скомпонованим кластером ПП.

Такі методи, що об'єднуються під загальною назвою «супровід до виявлення» або більш відомим англомовним варіантом «track-before-detect» (TBD), дозволяють досягти прийнятного рівня показників ефективності виявлення цілей при відношенні сигнал/шум менше 10 дБ.

Методи TBD, які для досягнення мети використовують сигнальну та траєкторну інформацію за кілька послідовних циклів огляду, в літературі згадуються давно [16–20].

Розробниками запропоновано безліч різних підходів, загальною рисою яких, як правило, є використання статистики на виході пристрою первинної обробки без порівняння з порогом виявлення, що є дуже продуктивним і при використанні, наприклад, методу перевірки множинних гіпотез або фільтра часток, який дозволяє стійко виявляти цілі при відношенні сигнал/шум менше 10 дБ [16].

Недоліком запропонованих алгоритмів є висока складність, яка навіть на сучасному етапі розвитку обчислювальних засобів робить їх практично нереалізованими для малогабаритних РЛС, які мають значні обмеження на масогабаритні характеристики та функціонують у режимі реального часу. Більш практичним підходом є використання розріджених даних (sparse data) у вигляді відміток, отриманих після первинного порівняння зі зниженим порогом виявлення [19].

Однак у публікаціях, наявних у відкритому доступі, автори в основному обмежуються використанням для виявлення 3…5 суміжних циклів огляду, що при забезпеченні гарної швидкодії та відносної простоті запропонованих алгоритмів не дозволяє досягти суттєвих виграшів у пороговому відношенні сигнал/шум понад 3…5 дБ [19].

При цьому питання вибору первинного порогу, який значно впливає на ефективність та швидкодію запропонованих алгоритмів, не розглядається. Тому з цієї точки зору, становлять інтерес недавні дослідження, де запропонована процедура TBD показала відносно високу ефективність виявлення малорозмірних цілей. Так, використання 3-4 циклів огляду дозволяє підвищити еквівалентний енергопотенціал РЛС на 2–3 дБ, а 5-6 циклів огляду на 4–5 дБ.

Але недоліком такого підходу є те, що підвищення практичності застосування запропонованого методу залежить тільки від підвищення темпу огляду до розумних значень, які не призведуть до значних втрат енергетики завдяки зниженню ефективності когерентного накопичення. При цьому комплексування вимірювань близько розташованими стільниками на основі запропонованого методу, наведеного вище, дозволяє зменшити вплив малої кількості точок вимірювань в певних областях і спрогнозувати траєкторію руху МВО.

Висновки

1. Таким чином, підвищення ефективності застосування способу визначення координати МВО за умов існування декількох променів розповсюдження радіосигналу, що заявляється, порівняно з прототипом, полягає в тому, що шляхом застосування радіорелейних систем терагерцового діапазона в інтегрованій існуючій БС мобільного зв'язку, що використовуються як високороздільні радари тимчасового кластеру збору даних вимірювань з семи груп ПП для передачі даних сканування до ПОВ, забезпечується виявлення МВО та більш висока точність вимірювання координат.

Також використання ЦРС терагерцового діапазону як систем сканування дозволить системі мобільного зв’язку мати функціональні характеристики систем сканування і забезпечити оптимізацію продуктивності мережі БС мобільного зв’язку, що включає в себе підвищення спектральної ефективності та надійності при мінімізації затримки.

Для підвищення ефективності ці системи використовують такі спільні ресурси, як час та спектр. Крім того, використання терагерцових частот забезпечує високий рівень безпеки передачі даних в інтегрованій існуючій мобільній мережі для екстрених служб.

2. Підвищення ефективності застосування способу визначення координати МВО за умов існування декількох променів розповсюдження радіосигналу, що заявляється, порівняно з прототипом, передбачає додаткові технологічні операції:

розгортання мережі ПП на базі радіорелейних систем терагерцового діапазону, яка інтегрується в діючу мережу БС мобільного зв’язку;

проведення постійного сканування зон обслуговування БС мобільного зв’язку системами сканування, які побудові на основі ЦРС терагерцового діапазону за допомогою механізму сканування;

формування тимчасового кластеру ПП для збору даних вимірювань із семи груп для передачі даних сканування до ПОВ цього кластеру;

періодичне визначення на приймальних пристроях усіх груп ПП кількості і часових затримок компонент віддзеркалених променів радіосигналу;

оцінювання підсумкової оцінки координат МВО ПОВ координати невідомого повітряного об’єкта, коли радіосигнали від усіх семи груп ПП кластеру прийняти;

підвищення ефективності мережі ПП на базі ЦРС терагерцового діапазону, яка інтегрується в діючу мережу БС мобільного зв’язку, шляхом використання спільних часових, спектральних ресурсів і апаратних компонентів;

підвищення точності вимірювань дальності щодо однопозиційних радіолокаційних систем, можливості прийому променів низького рівня у віддзеркаленому багатопроменевому радіосигналі.

3. Технічне рішення (що заявляється) може бути використано як фрагмент міської системи протиповітряної оборони, що забезпечує раннє попередження загрози від несанкціонованого МВО, що надходять, шляхом модифікації роботи БС мобільного зв’язку.

Подальшими напрямками наукових досліджень цієї роботи є:

оптимізація кількості радіопроменів при використанні терагерцового діапазону хвиль для зменшення вимог до апаратури;

подальший розгляд питань на основі запропонованої пропозиції і розробка удосконаленого методу TBD для поліпшення точності визначення координат.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Howland P. E., Maksimiuk D., Reitsma G. FM radio based bistatic radar. *IEE Proceedings – Radar, Sonar and Navigation*. 2005. P. 107–115. DOI: 10.1049/ip-rsn: 20045077.

2. Samczyński P., Wilkowski M., Kulpa K. Trial results on bistatic passive radar using non-cooperative pulse radar as illuminator of opportunity. *INTL – International Journal of Electronics and Telecommunications*. 2012. P. 171–176.

3. Honda J., Otsuyama T. Feasibility study on aircraft positioning by using ISDB-T signal delay. *IEEE Antennas and Wireless Propagation Letter*. 2016. P. 1787–1790.

4. Howland P. E. Target tracking using television-based bistatic radar. *IEE Proceedings – Radar, Sonar and Navigation*. 1999. P. 166–174.

5. Salah A. Experimental study of LTE signals as illuminators of opportunity for passive bi-static radar applications / Abdullah R.S.A. Raja, A. Ismail, F. Hashim, Aziz N.H. Abdul. *Electronics Letters*. 2014. P. 545–547. DOI: 10.1049/el.2014.0237.

6. Chen P. C. A non-line-of-sight error mitigation algoritm in location estimation. Proc. *IEEE Wireless Communications Networking Conference*. 1999. Vol 1. P. 316–320.

7. Cong L., Zhuang W. Non-line-of-sight error mitigation in TDOA mobile location. *Proc. IEEE Globecom*. Nov 2001. P. 680–684.

8. Європейський патент ЕР 3173809, ПМК кл. G01S 5/06, G0 5/02; опубл. 31.05.2017.

9. Сайко В. Г., Наритник Т. М. Безпроводові системи зв'язку терагерцового діапазону: монографія. Німеччина: Видавництво «LAP LAMBERT Academic Publishing RU», 2019. 68 с.

10. Сайко В. Г. Мережі мобільного зв'язку нового покоління 4G/5G/6G: монографія / В. Г. Сайко, Р. С. Одарченко, А. О. Абакумова, Т. М. Наритник, В. С. Наконечний, В. М. Домрачев, С. В. Толюпа, В. Ю. Заблоцький, П. Ф. Баховський. К.: ТОВ «Про формат», 2021. 200 с.

11. Saiko V., Odarchenko R., Zhurakovskyi B., Yevdokymenko M., Fesenko V., Tkachova O. A Model for Building a Wireless Terahertz Network for 5G NR. *Proceedings of the IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, IDAACS. 2023. P. 1071–1076.

12. Сайко В. Г., Радзівілов Г. Д., Комаров В. О., Фомін М. М., Солодовник В. І., Криволапов Я. В., Криволапов Г. Я. Алгоритм визначення координати несанкціонованого БпЛА за умов декількох променів розповсюдження сигнал // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. Том 35 (74). 2024. № 1. С. 74–80.

13. Zhu X., Feng Y. RSSI-based algorithm for indoor localization. *Communications and Network*. 2013. Vol. 5 (02). P. 37–42.

14. Tonissen S. M., Bar-Shalom Y. Maximum likelihood track-before-detect with fluctuating target amplitude. *IEEE Transactions on Aerospace and Electronic Systems.* 1998. № 34. P. 796–809.

15. Hadzagic M., Michalska H., Lefebrvre E. Track-Before-Detect Methods in Tracking Low-Observable Targets: A Survey. *Sensors & Transducers Magazine (S&T e-Digest).* 2005. Special Issue, August. P. 374–380.

16. Davey J. S., Rutten M. G., Cheung B. A. Comparison of Detection Performance for Several Track-before-Detect Algorithms. *EURASIP Journal on Advances in Signal Processing*. 2008. P. 1–10.

17. Orlando D., Venturino L., Lops M., Ricci G. Track-Before-Detect Strategies for STAP Radars. *IEEE Trans. Signal Process*. 2010. № 58. P. 933–938.

18. Nicomino F., Addabbo P., Clemente C., Biondi F., Giunta G., Orlando D. A Track-Before-Detect Strategy Based on Sparse Data Processing for Air Surveillance Radar Applications. *Remote Sensing*. 2021. № 13. P. 2–19.

19. Неуймин А. С., Жук С. Я. Обнаружение цели в импульсно-доплеровской РЛС на основе многообзорного накопления сигналов. *Вестник Национального технического университета Украины «КПИ». Серия: Радиотехника. Радиоаппаратостроение.* 2013. № 53. С. 89–97.

20. Saiko V., Toliupa S., Brailovskyi M., Narytnyk T., Nakonechnyi V., Shtanenko S.. Mathematical Simulation of FMCW Radar Operation: Simulation of the Normalized Signal at the Receiver Input. *5th IEEE International Conference on Advanced Information and Communication Technologies, AICT 2023 – Proceedings.* 2023. С. 140–146. DOI: 10.1109/AICT61584.2023. 21–25 Nov. 2023. URL: https://ieeexplore.ieee.org/xpl/conhome/10452416/proceeding.

21. Сайко В. Г., Романов Д. О., Наритник Т. М, Комаров В. О., Фомін М. М. Аналіз перспектив використання терагерцового діапазону частот для безпроводових мереж зв'язку спеціального призначення. *Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць ВІТІ.* 2024. № 5. С. 138–153.

22. Saiko V., Lukova-Chuiko N., Zhurakovskyi B., Nakonechnyi V., Brailovskyi M. A Method of Increasing the Reliability of Heterogeneous 5G/IoT Special Communication Networks when Using the Terahertz Wave Range. *CEUR Workshop Proceedingsthis.* 2022. 3384. P. 120–131.

23. Saiko V., Nakonechnyi V., Brailovskyi M., Toliupa S. Models of improving the efficiency of radio communication systems using the terahertz range. *2020 IEEE International Scientific-Practical Conference: Problems of Infocommunication Science and Technology. PIC S and T 2020* – Proceedings. P. 192–196.

DOI: 10.58254/viti.6.2024.17.215

УДК 623.4

Сорочкін О. М. ORCID: 0000-0001-8336-9978 (ХНУПС ім. Івана Кожедуба)
Сосулін М. В. ORCID: 0009-0003-0178-621x (ХНУПС ім. Івана Кожедуба)
Матвєєв Є. В. ORCID: 0000-0002-1582-7591 (ХНУПС ім. Івана Кожедуба)

ПЕРСПЕКТИВИ ВІЙСЬКОВОЇ АВІАЦІЇ ЧЕРЕЗ ІНТЕГРАЦІЮ БПЛА, ШІ ТА НОВІТНІХ ТЕХНОЛОГІЙ

Стаття присвячена аналізу перспектив розвитку військової авіації через інтеграцію безпілотних літальних апаратів (БПЛА), штучного інтелекту (ШІ) та новітніх технологій. Безпілотні літальні апарати стали невід'ємною частиною сучасних військових стратегій, виконуючи розвідку, спостереження, збирання розвідувальних даних (ІСР) та бойові операції. Висока ефективність БПЛА дозволяє Збройним Силам України використовувати ці системи для розвідки, радіоелектронної боротьби та ударів. Інтеграція автономних систем штучного інтелекту та сучасних сенсорів значно покращила можливості БПЛА, дозволяючи їм адаптуватися до динамічних ситуацій та приймати рішення в реальному часі. Розвиток технологій роїв, де кілька БПЛА діють злагоджено, є перспективним напрямом. Незважаючи на свої переваги, БПЛА стикаються з викликами у сфері радіоелектронної боротьби та кіберзагроз. Забезпечення безпечних каналів зв'язку та захист від радіоелектронних перешкод є критично важливими. Крім того, ефективне використання БПЛА вимагає спеціалізованої підготовки операторів. Штучний інтелект стає ключовим інструментом у військовій авіації, надаючи новітні можливості для автономного управління польотами, точного розпізнавання цілей та оперативного прийняття рішень. Інтеграція хмарних технологій дозволяє автономним літакам отримувати та обробляти дані в реальному часі, сприяючи злагодженій взаємодії та обміну інформацією між різними платформами. Кібербезпека стає ключовою для захисту автономних літаків від кібератак. Технології Інтернету речей (IoT) сприяють зв'язку між системами та сенсорами, покращуючи готовність та обслуговування автономних бойових літаків. Модернізація пілотів-солдатів також охоплює впровадження передових технологій для підвищення операційних можливостей.'

Ключові слова: *військова авіація, безпілотні літальні апарати, штучний інтелект, новітні технології, кібербезпека, інтеграція, автономні системи.*

O. Sorochkin, M. Sosulin, Y. Matvieiev Prospects of military aviation through the integration of UAVs, AI and the latest technologies

The article is devoted to the analysis of prospects for the development of military aviation through the integration of unmanned aerial vehicles (UAVs), artificial intelligence (AI) and the latest technologies. Unmanned aerial vehicles have become an integral part of modern military strategies, performing reconnaissance, surveillance, intelligence gathering (IGI) and combat operations. The high efficiency of UAVs allows the Armed Forces of Ukraine to use these systems for reconnaissance, electronic warfare and strikes. The integration of autonomous artificial intelligence systems and modern sensors has greatly improved the capabilities of UAVs, allowing them to adapt to dynamic situations and make decisions in real time. The development of swarm technologies, where several UAVs operate in concert, is a promising direction. Despite their advantages, UAVs face challenges in the field of electronic warfare and cyber threats. Ensuring secure communication channels and protection against radio-electronic interference are critical. In addition, the effective use of UAVs requires specialized training of operators. Artificial intelligence is becoming a key tool in military aviation, providing the latest opportunities for autonomous flight control, accurate target recognition and quick decision-making. The integration of cloud technologies allows autonomous aircraft to receive and process data in real time, facilitating harmonious interaction and information sharing between different platforms. Cybersecurity is becoming key to protecting autonomous aircraft from cyberattacks. Internet of Things (IoT) technologies facilitate communication between systems and sensors, improving the readiness and maintenance of autonomous combat aircraft. The modernization of soldier pilots also includes the introduction of advanced technologies to enhance operational capabilities.

Keywords: *military aviation, unmanned aerial vehicles, artificial intelligence, the latest technologies, cyber security, integration, autonomous systems.*

Вступ

У сучасних умовах розвитку військової авіації особливе місце займає інтеграція безпілотних літальних апаратів та новітніх технологій, що забезпечують їх ефективне функціонування. Військові конфлікти та війни останніх років підкреслюють необхідність використання автономних систем для виконання небезпечних та складних завдань, що знижує

ризики для людських життів та підвищує ефективність бойових операцій. Важливість використання таких технологій в умовах сучасної російсько-української війни важко переоцінити, оскільки вони дозволяють забезпечити високу ефективність і точність виконання завдань.

Безпілотні літальні апарати стали ключовими елементами сучасних військових стратегій завдяки своїй здатності виконувати різноманітні завдання – від розвідки до проведення бойових операцій. БПЛА можуть бути дистанційно керованими або повністю автономними, що дозволяє використовувати їх у різних умовах. Інтеграція штучного інтелекту значно розширює можливості цих систем, дозволяючи їм адаптуватися до змінних умов бойових дій, приймати рішення в реальному часі та виконувати складні координовані операції.

Інновації в сфері сенсорних технологій і систем прихованості дозволяють БПЛА виконувати широкий спектр місій з високою ефективністю. Крім того, розвиток технологій роїв, де кілька БПЛА діють злагоджено, відкриває нові можливості для проведення складних розвідувальних місій та ударних операцій. Впровадження нових технологій також дозволяє підвищити безпеку використання БПЛА, забезпечуючи захист від радіоелектронних загроз та кіберзагроз, що є критично важливим для їх ефективного функціонування.

Успішна інтеграція БПЛА з пілотованими літаками в бойових операціях демонструє їхню універсальність та важливість. Комбінований підхід, коли БПЛА виконують розвідку та придушення систем протиповітряної оборони ворога, а пілотовані літаки виконують точкові удари, максимально використовує сильні сторони обох платформ. Цей підхід дозволяє забезпечити високу ефективність та мінімізувати ризики для пілотованих літаків.

Незважаючи на значні переваги, БПЛА стикаються з викликами у сфері радіоелектронної боротьби та кіберзагроз. Забезпечення безпечних каналів зв’язку та захист від радіоелектронних перешкод є критично важливими для збереження їхньої цілісності. Досвід з поточних конфліктів підкреслює необхідність постійного вдосконалення захисту від БПЛА, що включає покращення радіолокаційних систем та електронних контрзаходів. Ефективне використання БПЛА також вимагає спеціалізованої підготовки операторів, що включає комплексні програми підготовки з технічних навичок, тактичного застосування та стратегії протидії радіоелектронній боротьбі.

Актуальність дослідження

Актуальність дослідження зумовлена стрімким розвитком технологій, що забезпечують можливість створення та використання автономних бойових систем. Російсько-українська війна демонструє високу ефективність безпілотних літальних апаратів, які виконують різноманітні завдання, зокрема розвідку, спостереження, збирання розвідувальних даних та проведення бойових операцій. Інтеграція штучного інтелекту дозволяє підвищити ефективність цих систем, роблячи їх більш адаптивними та автономними.

Аналіз останніх досліджень та публікацій

Розвиток сучасних інформаційних технологій та автоматизації, зокрема технологій штучного інтелекту, значно вплинув на ефективність та можливості використання безпілотних літальних апаратів у військових операціях.

В роботі [1] розглянуто застосування ШІ для групових дій БПЛА. Автори детально аналізують використання штучного інтелекту для координації та управління групами БПЛА під час виконання бойових завдань. Вони підкреслюють важливість розробки ефективних алгоритмів для автономної роботи БПЛА, що дозволяє знизити залежність від людського фактора та підвищити загальну ефективність бойових операцій.

Дослідження [2] присвячено ролі та викликам спільного застосування пілотованої та безпілотної авіації у військових операціях. Автори підкреслюють необхідність комбінованого використання пілотованих літаків і БПЛА для досягнення максимального ефекту в бойових умовах. Основну увагу приділено викликам, які пов’язані з інтеграцією цих систем, а також

розробці стратегій для забезпечення ефективної взаємодії між пілотованими та безпілотними платформами.

Робота [3] розглядає застосування безпілотних авіаційних систем у сфері цивільного захисту. Автори досліджують можливості використання БПЛА для виконання завдань, які пов'язані з ліквідацією надзвичайних ситуацій, наданням допомоги в зонах катастроф та моніторингом екологічної ситуації. Вони наголошують на важливості розвитку технологій БПЛА для підвищення ефективності системи цивільного захисту.

У дослідженні [4] розглянуто таксономію поведінки та ієрархічну модель управління роями БПЛА для виконання бойових та спеціальних місій. Автор аналізує різні підходи до управління роями БПЛА, підкреслюючи важливість розробки ефективних моделей для координації дій великої кількості безпілотних апаратів. В роботі також розглянуто виклики, пов'язані з інтеграцією БПЛА у бойові дії, та пропонуються шляхи їх вирішення.

Дослідження [5] присвячено авіаційній техніці четвертого і п'ятого поколінь, їх історії та напрямах подальшого розвитку. Автори аналізують сучасні тенденції розвитку авіаційної техніки, включаючи інтеграцію новітніх технологій та систем управління. Вони підкреслюють важливість розвитку технологій ШІ та БПЛА для підвищення ефективності військових операцій.

У статті [7] розглянуто вплив електрифікації літаків на майбутнє військової авіації. Автор аналізує переваги та виклики, пов'язані з впровадженням електричних систем у військові літаки, підкреслюючи важливість інтеграції новітніх технологій для підвищення ефективності та зниження витрат на військові операції.

Ці дослідження підкреслюють важливість інтеграції БПЛА, ШІ та новітніх технологій для розвитку військової авіації, а також вказують на виклики та перспективи їх використання у сучасних військових умовах.

Постановка задачі. Задача цього дослідження полягає у визначенні основних напрямків розвитку військової авіації через інтеграцію безпілотних літальних апаратів, штучного інтелекту та новітніх технологій, а також у виявленні викликів та перспектив використання цих систем у сучасних військових конфліктах.

Мета. Метою дослідження є аналіз основних тенденцій розвитку військової авіації через інтеграцію БПЛА, ШІ та новітніх технологій, а також оцінка їх впливу на сучасні військові стратегії.

Основна частина. Безпілотні літальні апарати стали невід'ємною частиною сучасних військових стратегій, оскільки їх можна розділити на дистанційно керовані літальні апарати та повністю автономні системи. Нині, БПЛА використовуються для розвідки, спостереження, збирання розвідувальних даних та бойових операцій, часто виконуючи завдання, небезпечні для пілотованих літаків, що дозволяє Збройним Силам України ефективно використовувати БПЛА у війні з Росією, застосовуючи ці системи для розвідки, радіоелектронної боротьби та ударів. Здатність БПЛА діяти у зонах бойових дій без ризику для пілотів є надзвичайно цінною.

Розвиток автономних систем, штучного інтелекту та інтеграції сучасних сенсорів значно покращив можливості БПЛА, що оснащені ШІ, дозволяє їм адаптуватися до динамічних ситуацій та приймати рішення в реальному часі, підвищуючи їх ефективність і дозволяючи проводити координовані операції, збільшуючи їх вплив на полі бою. Крім того, вдосконалення технологій прихованості, систем радіоелектронної боротьби та універсальності бойового навантаження дозволяє БПЛА виконувати широкий спектр місій.

Успішна інтеграція БПЛА з пілотованими літаками в бойових операціях демонструє їхню універсальність та важливість, комбінований підхід, коли БПЛА виконують розвідку та придушення систем протиповітряної оборони ворога, а пілотовані літаки виконують точкові удари, максимально використовує сильні сторони обох платформ. Розвиток технологій роїв,

де кілька БПЛА діють злагоджено, є перспективним напрямом, і такі рої можуть перевантажувати оборону ворога, проводити складні розвідувальні місії та виконувати координовані удари з високою ефективністю. Автономні рішення в роєвих системах підвищать їх ефективність у динамічних бойових сценаріях [4].

Незважаючи на свої переваги, БПЛА стикаються з викликами у сфері радіоелектронної боротьби та кіберзагроз, оскільки забезпечення безпечних каналів зв’язку та захист БПЛА від радіоелектронних перешкод є критично важливими для збереження їхньої цілісності, і досягнення у сфері антизаглушення та надійного шифрування мають вирішальне значення. Іншим викликом є розробка заходів протидії ворожим БПЛА, що включає покращення радіолокаційних систем та електронних контрзаходів, досвід з поточних конфліктів підкреслює необхідність постійного вдосконалення захисту від БПЛА.

Ефективне використання БПЛА вимагає спеціалізованої підготовки операторів, тому комплексні програми підготовки, що охоплюють технічні навички, тактичне застосування та стратегії протидії радіоелектронній боротьбі, є важливими, а тренування на симуляторах та реальні навчання допомагають операторам розвивати необхідні навички для максимізації ефективності БПЛА в бойових умовах [5].

Штучний інтелект стає ключовим інструментом у військовій авіації, надаючи новітні можливості для автономного управління польотами, точного розпізнавання цілей та оперативного прийняття рішень (Decision-Making Model) (1):

$$R=f(D, S, T, A), \quad (1)$$

де R – прийняття рішення;

D – дані (інформація про ситуацію);

S – стратегія (план дій);

Т –технології (включаючи ШІ);

A – аналіз (оцінка ризиків та можливостей).

Ці системи здатні аналізувати великі масиви даних в реальному часі, що значно підвищує ефективність та ситуаційну обізнаність під час виконання місій автономними бойовими літаками. Сполучені Штати та Китай активно розширюють свої можливості використання ШІ для різноманітних військових цілей, при цьому ключові компанії оборонної індустрії, такі як BAE Systems, Boeing, Elbit Systems, Leidos, Lockheed Martin та Raytheon, розробляють свої ШІ-технології самостійно або через аквізиції [2].

Застосування ШІ охоплює широкий спектр оборонних систем, включаючи автономні транспортні засоби та озброєння, що забезпечує підвищену точність, ефективність та зниження витрат військових операцій. Інтеграція хмарних технологій дозволяє автономним літакам отримувати та обробляти дані в реальному часі, що сприяє злагодженій взаємодії та обміну інформацією між різними платформами, підвищуючи загальну продуктивність місій. Серед інновацій, що знаходяться на стадії розвитку, варто відзначити антени з формуванням променя, мережі датчиків для моніторингу та V2V підтримку в автономних транспортних засобах, тоді як технології запуску безпілотників, інтелектуальні електромережі для заряджання електромобілів та мережеві сервіси, що базуються на геолокації, переживають період інтенсивного зростання.

З урахуванням високої залежності військової авіації від цифрових технологій, кібербезпека стає ключовою для захисту автономних літаків від кібератак, що є вирішальним для збереження недоторканності та конфіденційності військових дій. Зростання загрози кібератак пов’язане зі збільшенням взаємодії між фізичними та цифровими системами, а слабкі захисні механізми, агресивні тактики зловмисників, дефіцит кваліфікованих фахівців з кібербезпеки та недостатньо ефективне управління захистом підвищують ризики для оборонних підприємств. Тому кібербезпека є критично важливою для всіх секторів, зокрема для оборонної промисловості через секретність її даних [2].

Технології Інтернету сприяють зв'язку між системами та сенсорами, забезпечуючи ефективне моніторингу та управління, що покращує готовність та обслуговування автономних бойових літаків. На початковому етапі розвитку перебувають технології для керування трансмісіями літаків, дрони з дистанційним управлінням та системи уникнення зіткнень літаків, в той час як інтенсивно розвиваються технології для керування групами БПЛА, лідари для запобігання зіткненню на транспорті та методи виправлення супутникових зображень.

Робототехнічні системи відіграють важливу роль у розвитку автономних літаків, дозволяючи виконувати складні маневри та оптимізацію траєкторії польоту без людського втручання, включно з БПЛА та координованими місіями дронів (2):

$$\min \int_{t_0}^{t_f} L\big(x(t), u(t)\big)dt, \tag{2}$$

де L – функція втрат (наприклад, витрати пального);

$x(t)$ – стан системи в момент часу t;

$u(t)$ – управлінські рішення (включаючи рішення, підтримані ШІ);

t_0, t_f – початковий і кінцевий час.

Новітнім напрямкам розвитку належать алгоритми машинного навчання для прогнозування (3), системи уникнення зіткнень та автономні системи керування, тоді як технології радарів для уникнення зіткнень і LiDAR для зображень активно розвиваються, а також з'являються акустичні сигнали для автономних транспортних засобів (3):

$$y = f(x; \theta) + \epsilon, \tag{3}$$

де y – вихід (наприклад, ймовірність успішного завершення місії);

x – вхідні дані (характеристики місії);

θ – параметри моделі;

ϵ – похибка.

Впровадження передових технологій для підвищення операційних можливостей, застосування генетичних алгоритмів для оптимізації бойових стратегій (4), включаючи системи доповненої реальності для збільшення ситуаційної обізнаності та мобільні пристрої для моніторингу здоров'я та продуктивності (4):

$$P(t+1) = f(P(t), R, C), \tag{4}$$

де $P(t)$ – популяція рішень в момент часу t;

R – операції вибору;

C – кросовер та мутація.

Прорив у цих напрямках значно вплине на майбутнє оборонної промисловості, де модернізація солдатів стане одним із ключових факторів.

Висновки. Висновки цього дослідження підкреслюють важливість інтеграції безпілотних літальних апаратів, штучного інтелекту та новітніх технологій для розвитку військової авіації. Ці системи дозволяють підвищити ефективність бойових операцій, знизити ризики для людських життів та забезпечити більш ефективне виконання складних завдань. Незважаючи на значні переваги, виклики, пов'язані з кібербезпекою та протидією радіоелектронним загрозам, залишаються актуальними і потребують подальшого дослідження та вдосконалення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білозьоров О. С., Кадук С. О., Кривенков М. В., Беспалько О. В. Застосування штучного інтелекту для групових дій БПЛА // Тези доповідей науково-практичної конференції інженерно-авіаційного факультету Харківського національного університету Повітряних Сил ім. Івана Кожедуба

"Безпілотна авіація у сучасній збройній боротьбі", 7 грудня 2023 року, Харків: Харківський національний університет Повітряних Сил імені Івана Кожедуба, 2023. С. 45–50.

2. Герасименко В. В., Блискун О. Є., Печененко О. М., Гончаренко Є. В. Роль та виклики спільного застосування пілотованої та безпілотної авіації у військових операціях // Тези доповідей науково-практичної конференції інженерно-авіаційного факультету Харківського національного університету Повітряних Сил імені Івана Кожедуба "Безпілотна авіація у сучасній збройній боротьбі", 7 грудня 2023 року, Харків: Харківський національний університет Повітряних Сил ім. Івана Кожедуба, 2023. С. 60–65.

3. Застосування безпілотних авіаційних систем у сфері цивільного захисту: монографія / Д. В. Бондар, А. В. Гурник, А. О. Литовченко, В. В. Хижняк, В. Л. Шевченко, Д. М. Ядченко. Київ, 2022, 312 с.

4. Компанієць О. М. Таксономія поведінки та ієрархічна модель управління роями БПЛА для виконання бойових та спеціальних місій // Тези доповідей науково-практичної конференції інженерно-авіаційного факультету Харківського національного університету Повітряних Сил імені Івана Кожедуба "Безпілотна авіація у сучасній збройній боротьбі", 7 грудня 2023 року, Харків: Харківський національний університет Повітряних Сил імені Івана Кожедуба, 2023. С. 25–30.

5. Рєзнік В. І., Постольник М. М., Мосолов В. М., Сторожук С. М. Авіаційна техніка четвертого і п’ятого поколінь: історія та напрями подальшого розвитку. DOI: 10.54858/dndia.2021-17-22.

6. Leading innovators in galvano-scanners for the aerospace and defense industry. https://www.army-technology.com/data-insights/innovators-galvanoscanners-aerospace-defence/.

7. Matt McLaughlin. How aircraft electrification is shaping the future of military aviation: Defense News Whitepaper. 2023. 6 p.

DOI: 10.58254/viti.6.2024.18.221

УДК 004.4

Усик А. А. ORCID: 0009-0009-1355-5826 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Симоненко О. А. ORCID: 0000-0001-8511-2017 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Троцько О. О. ORCID: 0000-0001-7535-5023 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Бєляков Р. О. ORCID: 0000-0001-9882-3088 (ВІТІ ім. Героїв Крут)

ОБҐРУНТУВАННЯ ДЕКЛАРАТИВНОГО ПІДХОДУ ПРИ РОЗРОБЦІ ТА УПРАВЛІННІ ІНФОРМАЦІЙНИМИ СИСТЕМАМИ З ВИКОРИСТАННЯМ ХМАРНИХ ТЕХНОЛОГІЙ

У сучасному світі стрімкого розвитку технологій та зростаючого значення інформаційних систем для великих організацій, включаючи Збройні сили України, актуальною стає потреба в оптимізації їх розробки та управління ними. У Збройних силах України переважає принцип ієрархічності при побудові інформаційно-комунікаційних систем, що накладає обмеження на процес впровадження нових гнучких рішень. Для процесу розробки та управління інформаційними системами здебільшого використовується імперативний підхід. Разом з тим використання декларативного підходу у цих системах відкриває широкі можливості для забезпечення їх ефективності, гнучкості та простоти у розробці та управлінні ними.

У статті розглядається можливість використання принципів декларативного підходу для оптимізації розробки та управління інформаційними системами з використанням хмарних технологій, переваги та приклади його застосування.

Проблематика дослідження полягає у необхідності оптимізації процесу розробки та управління інформаційними системами з використанням хмарних технологій в умовах швидкого темпу розвитку технологій та зростаючих потреб Збройних сил України у використанні цих систем для підвищення інформаційної обізнаності та прискорення прийняття рішень командирами під час ведення бойових дій.

Метою дослідження є аналіз принципів декларативного підходу та визначення його можливостей для оптимізації розробки та керування інформаційними системами з використанням хмарних технологій. Для досягнення мети використовуються методи аналізу сучасного стану і тенденцій розвитку хмарних технологій, а також аналізуються приклади реалізації декларативного підходу у різних IT-проєктах.

Проведений аналіз показує важливість декларативного підходу для підвищення ефективності розробки та управління інформаційними системами з використанням хмарних технологій. Результати дослідження можуть бути корисні для підрозділів, що розглядають можливість впровадження декларативного підходу у свої проєкти. Декларативний підхід може бути застосовано у новітніх розробках інформаційних систем для підвищення рівня автоматизації та оптимізації процесів управління інфраструктурою Збройних сил України.

Ключові слова: *декларативний підхід, хмарні інформаційні системи, оптимізація, автоматизація, інфраструктура як код, Збройні сили України.*

A. Usyk, O. Symonenko, O. Trotsko, O. Bieliakov Substantiation of the declarative approach in the development and management of information systems using cloud technologies

In today's world of rapid technological development and the growing importance of information systems for large organizations, including the Armed Forces of Ukraine, the need to optimize their development and management is becoming urgent. In the Armed Forces of Ukraine, the principle of hierarchy prevails in the construction of information and communication systems, which imposes restrictions on the process of implementing new flexible solutions. The process of developing and managing information systems is mostly based on the imperative approach. At the same time, the use of the declarative approach in these systems opens up wide opportunities to ensure their efficiency, flexibility and simplicity in development and management.

The article discusses the possibility of using the principles of the declarative approach to optimize the development and management of information systems using cloud technologies, and also the advantages and examples of its application.

The research is concerned with the need to optimize the process of developing and managing information systems using cloud technologies in the context of the rapid pace of technology development and the growing needs of the Armed Forces of Ukraine to use these systems to increase information awareness and accelerate decision-making by commanders during combat operations.

The purpose of the study is to analyze the principles of the declarative approach and determine its capabilities for optimizing the development and management of information systems using cloud technologies. To achieve this goal, the author uses methods of analyzing the current state and trends in the development of cloud technologies, as well as analyzes examples of the declarative approach in various IT projects.

The analysis shows the importance of the declarative approach to improve the efficiency of development and management of information systems using cloud technologies. The results of the study may be useful for departments considering implementing the declarative approach in their projects. The declarative approach can be applied in the latest developments of information systems to increase the level of automation and optimize the infrastructure management processes of the Armed Forces of Ukraine.

Keywords: *declarative approach, cloud information systems, optimization, automation, infrastructure as code, the Armed Forces of Ukraine.*

Постановка задачі. Основним завданням функціонування інформаційно-комунікаційних систем є забезпечення стійкого, безперебійного управління військами та своєчасного надання інформаційних сервісів із заданою якістю та рівнем безпеки. Для ефективної діяльності розробників та посадових осіб, які імплементують розроблені рішення та здійснюють управління інформаційними системами впровадження новітніх механізмів є критично важливим.

Однак існуючі підходи щодо розробки та управління інформаційними системами є дещо застарілими, оскільки вони чітко регламентовані згідно з інструкціями. Хоча така регламентація має певні переваги, вона одночасно позбавляє систему необхідної гнучкості, не задовольняє принципам інтероперабельності та масштабованості. Імперативний підхід, який наразі переважає, створює значні обмеження при необхідності швидкої адаптації систем до змінних умов бойової обстановки та нових вимог командування.

У зв'язку з цим виникає необхідність пошуку нових підходів для гнучкого та адаптивного управління інформаційно-комунікаційними системами, зокрема їх розробкою та управлінням. Особливої актуальності набуває дослідження можливостей декларативного підходу в поєднанні з хмарними технологіями, що потенційно може забезпечити необхідний рівень гнучкості та ефективності управління військовими інформаційними системами.

Аналіз останніх публікацій

В останні роки спостерігається зростаючий інтерес до використання декларативного підходу в розробці та управлінні інформаційними системами з використанням хмарних технологій. Дослідження в цьому напрямку акцентують увагу на розвитку ефективних методів та інструментів, які дозволять спеціалістам описувати бажаний стан системи або результат, а не послідовність дій для досягнення цього стану [1]. Це підтверджується ґрунтовним дослідженням *Brown* і *Davis* [2], які провели всебічний аналіз декларативних підходів у контексті управління хмарними ресурсами.

Результати останніх досліджень свідчать про потенціал декларативного підходу для покращення ефективності розробки та управління інформаційними системами. Автори дослідження [3] у своєму порівняльному аналізі декларативної та імперативної парадигм демонструють значні переваги декларативного підходу в контексті масштабування та управління складними системами.

У дослідженні [4] автори розглядають гібридний підхід, тобто пропонують ефективні методи поєднання декларативних та імперативних парадигм для досягнення оптимального балансу між безпекою та продуктивністю. Існують напрацювання щодо поєднання декларативного та імперативного підходів у технологіях надання хмарних додатків [5].

У роботі [6] досліджуються сучасні підходи до створення SaaS-застосунків з використанням "cloud-native" технологій, що доповнюється дослідженням [7] щодо патернів інтеграції для декларативного та імперативного управління хмарними системами. Автори дослідження [11] представляють детальний аналіз продуктивності різних підходів у хмарних системах.

Зауважимо, що наразі фактично відсутні дослідження в питаннях хмарної декларативної інфраструктури в ЗСУ, тому що дана галузь тільки починає розвиватися, отже це може бути перспективною областю для наукових досліджень та розробки практичних рішень.

Метою статті є оцінка ефективності декларативного підходу відносно існуючих за розробленим показником IEDAMS, що є результатом розрахунку вагових коефіцієнтів за аналітично-визначеними критеріями.

Виклад основного матеріалу. Декларативний підхід зазвичай використовується в різних областях, таких як бази даних, конфігураційні файли, графічні інтерфейси користувача, обробка даних, обробка подій, інтеграція сервісів.

Прикладом застосування декларативного підходу є *GitOps,* основна концепція якого полягає в узгодженні бажаного і поточного стану системи. Таким чином, *GitOps* складається з Git-репозиторію з декларативними описами інфраструктури, які повинні привести до кінцевого бажаного стану розгорнутої інфраструктури. Як і у випадку з *Kubernetes* в *GitOps* (який сам по собі є декларативною системою), для забезпечення доступу до сервісів *Kubernetes* ззовні кластера *Kubernetes* необхідний декларативний, хмарний вхід. Цей декларативний підхід дозволяє *Kubernetes* пропонувати автоматизовані, спрощені та масштабовані додатки.

Інструмент IaC в *GitOps* автоматизує процес розгортання. Програмне забезпечення або дрейф-агенти попередять користувача у разі будь-якого відхилення від бажаного стану в поточному виробничому середовищі. Це забезпечить відповідність вимогам і, таким чином, також допоможе у впровадженні *Compliance as Code*. Ви зможете завантажити попередню версію свого середовища за допомогою контролю версій декларативної інфраструктури в *GitOps*. Декларативна інфраструктура також сприяє загальній безпеці, забезпечуючи підвищену стабільність та оптимізацію витрат.

Безпека на основі політик

Використовуючи підхід декларативної інфраструктури, можна кодифікувати власну безпеку на основі політик у вигляді *Policy as Code* (PaC). Політики безпеки, такі як протоколи автентифікації та авторизації, привілеї доступу, політики делегування тощо, можуть бути налаштовані за допомогою декларативного методу. Завдяки контролю версій також можна уникнути мануальних помилок, під час впровадження політики безпеки [17].

Інструменти IaC

При використанні декларативного підходу до розгортання додатків, необхідно лише визначити бажану версію програми та її конфігурацію у відповідному файлі специфікацій. Інструменти декларативного IaC автоматично виконають усі необхідні кроки для встановлення та налаштування додатку відповідно до заданих параметрів. Такий підхід значно спрощує роботу розробників, звільняючи їх від необхідності глибоко занурюватись у деталі процесу розгортання, як це відбувається в імперативній моделі.

Залежно від вимог організації та обраного підходу, можна обрати один з декількох інструментів IaC. Наприклад, *Chef*, якщо віддаєте перевагу імперативному підходу. Якщо є потреба реалізувати декларативну інфраструктуру, можна використовувати *Flux & Flagger*, *Terraform*, *Puppet* або *Cloudformation*. Такі інструменти, як *SaltStack* та *Ansible* є поєднанням обох підходів, але є переважно декларативними за своєю природою.

Доцільність використання декларативного підходу у військових структурах

Для математичного обґрунтування доцільності використання імперативного чи декларативного підходу у розробці та управлінні інформаційними системами, пропонується комплексний інструмент оцінки IEDAMS (*Index of Effectiveness of the Declarative Approach for use in Military Structures*), розроблений для кількісного визначення потенційних переваг впровадження певного підходу у військових IT-системах. Цей індекс враховує унікальні вимоги та обмеження військових підрозділів, забезпечуючи основу для прийняття обґрунтованих рішень щодо впровадження нових IT-підходів.

IEDAMS складається з восьми ключових факторів, кожен з яких відображає критичний аспект військових IT-операцій:

a) Операційна ефективність (*Operational Efficiency*, OE). Є метрикою швидкості та точності виконання завдань;

b) Оптимізація ресурсів (*Resource Optimization*, RO). Оцінка ефективності використання обчислювальних ресурсів та інфраструктури;

c) Адаптивність до змін (*Adaptability to Change*, AC). Метрика, що відображає здатність системи швидко пристосовуватися до нових вимог;

d) Зменшення помилок та надійність системи (*Error Reduction and System Reliability*, ER). Оцінка частоти помилок та підвищення загальної надійності;

e) Масштабованість та гнучкість (*Scalability and Flexibility*, SF). Оцінка здатності системи розширюватися та адаптуватися до різних масштабів операцій;

f) Підвищення безпеки (*Security Enhancement*, SE). Оцінка захищеності від кіберзагроз та вразливостей;

g) Інтероперабельність (*Interoperability*, IO). Метрика взаємодії системи з іншими військовими та взаємодіючими системами;

h) Навчання та передача навичок (*Training and Skill Transfer*, TST). Відображає рівень складності навчання фахівців та передачі знань між різними підрозділами.

Розрахунок показника IEDAMS пропонується здійснювати у два етапи:

Крок 1: Розрахунок окремих факторів.

Для кожного з факторів (OE, RO, AC, ER, SF, SE, IO, TST) обчислюється відносне покращення порівняно з імперативним підходом (1), а саме

$$Factor = \frac{(Mtrc\_declarative - Mtrc\_imperative)}{\max(Mtrc\_imperative, Mtrc\_declarative)}, \quad (1)$$

де *Mtrc_declarative* – значення метрики при використанні декларативного підходу;

Mtrc_imperative – значення метрики при використанні імперативного підходу.

Чисельник показує абсолютну зміну в метриці. У знаменнику використовується функція max(), що вибирає більше з двох значень, та гарантує, що знаменник ніколи не буде нулем.

Також це нормалізує результат, обмежуючи його діапазоном від –1 до 1.

Крок 2: Обчислення зваженої суми факторів (2):

$$IEDAMS = w1 \times OE + w2 \times RO + w3 \times AC + w4 \times ER + w5 \times SF + w6 \times SE + w7 \times IO + w8 \times TST, \quad (2)$$

де *w1–w8* – вагові коефіцієнти, що відображають відносну важливість кожного фактора значення відповідних факторів, обчислені на кроці 1.

Важливо зазначити, що сума всіх вагових коефіцієнтів (3) повинна дорівнювати 1:

$$w1 + w2 + w3 + w4 + w5 + w6 + w7 + w8 = 1. \quad (3)$$

Значення IEDAMS може варіюватися від –1 до 1.

Позитивні значення ($0 < IEDAMS \leq 1$) вказують на перевагу декларативного підходу. Чим ближче до 1, тим більша перевага.

Негативні значення ($-1 \leq IEDAMS < 0$) свідчать про перевагу імперативного підходу. Чим ближче до –1, тим більша перевага імперативного підходу.

Значення близькі до 0 ($-0{,}2 < IEDAMS < 0{,}2$) вказують на мінімальну різницю між підходами.

Для практичного застосування IEDAMS у військових структурах рекомендується проведення контрольованих експериментів або аналіз існуючих впроваджень для збору даних по кожному фактору, проведення консультацій з військовими IT-експертами для встановлення

відповідних вагових коефіцієнтів. Рекомендується застосування формули для обчислення індексу на основі попередньо зібраних даних, після чого здійснюється інтерпретація отриманого значення IEDAMS та його окремих компонентів для подальшого використання результатів IEDAMS для обґрунтування рішень щодо впровадження декларативних підходів у військових ІТ-системах.

Хоча IEDAMS надає структурований підхід до оцінки ефективності декларативних методологій, важливо враховувати його обмеження. Суб’єктивність вагових коефіцієнтів може призводити до неточних результатів, саме тому необхідно проводити збір даних. Наявна складність збору даних через наявність грифу секретності. Можливість неповного охоплення всіх аспектів військових ІТ-операцій, особливо у вузькоспеціалізованих сценаріях.

```
Import React from ‘react’;
import ( Radar, RadarChart, PolarGrid, Legend, PolarAngleAxis, PolarfadiusAxis, ResponsiveContainer } from 'recharts';
const data = [
        { factor: "Операційна ефективність, declarative: 0.8, imperativeive: 0.6, ful Mark: 1 },
        { factor: "Оптимізація ресурсіs, declarative: 0.75, imperative: 0.55, fullMark: 1},
        { factor: Адаптивність до змін, declarative: 0.85, imperative: 0.5, fullMark: 1 },
        { factor: Зменшення помилок, declarative: 0.9, imperative: 0.7, fullMark: 1 },
        { factor: Масштабованість та гнучкість", declarative: 0.85, imperative: 0.6, fullMark: 1},
        { factor: Підвищення безпеки, declarative: 0.8, imperative: 0.7, ful Mark: 1 },
        { factor: "Інтероперабельність, declarative: 0.75, imperative: 0.5, fullMark: 1},
        { factor: "Навчання та передача навичок", declarative: 0.7, imperative: 0.6, fullMark: 1 },
    ];
        const IEDAMSRadarChartUkrainian= () => (
        <ResponsiveContainer width="100%" height={400}>
          <RadarChart cx="50%" cy="50%" outerRadius="80%" data={data}>
            <PolarGrid  />
            <PolarAngleAxis dataKey="factor" />
            <PolarRadiusAxis angle={30} domain={[0, 1]} />
            <Radar name="Декларативний підхід" dataKey="declarative" stroke="#82ca9d" fill="#82ca9d" fillopacity=(0.6) />
             <Radar name="Імперативний підхід" datakey="imperative" stroke "#8884d8" fill="#8884d8" fillopacity {0.6} />
            <Legend />
          </RadarChart>
        </ResponsiveContainer>
);

export default IEDAMSRadarChartUkrainian;
```

Рис. 1. Код діаграми IEDAMS

Для полегшення інтерпретації пропонується використовувати радіальну діаграму (рисунок 2) для візуалізації багатовимірного характеру покращень, які пропонує IEDAMS. Діаграму було побудовано з використанням бібліотеки мови програмування *JavaScript* (рисунок 1), але дозволяється використовувати інші, більш зручні для окремих спеціалістів способи відображень покращень, вирахуваних за допомогою IEDAMS.

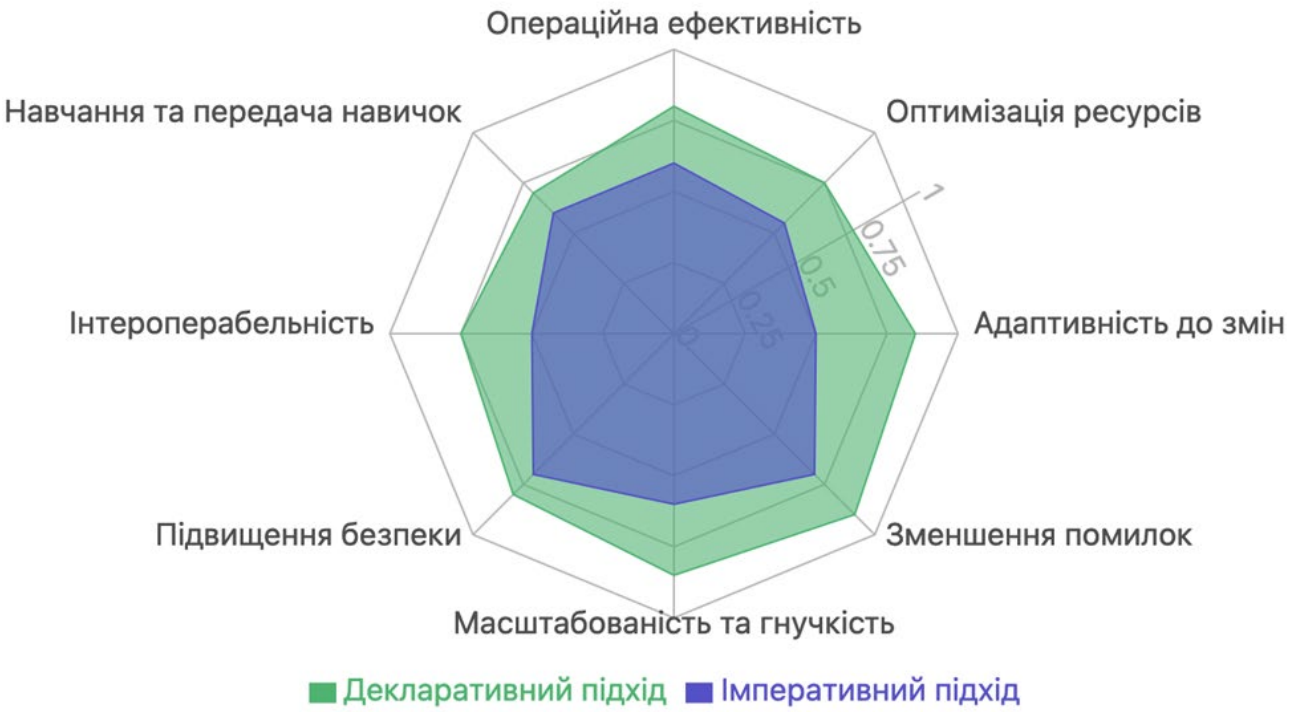


Рис. 2. Радіальна діаграма: Фактори IEDAMS

Інструменти та технології, які підтримують декларативне програмування

Декларативне програмування отримало значну популярність в різних областях програмування, існують різноманітні мови та інструменти, які підтримують цей підхід. Ось деякі з найбільш популярних з них:

SQL (*Structured Query Language*) – мова запитів, яка використовується для маніпулювання та управління базами даних. Вона дозволяє програмістам виразно описувати запити до баз даних, не вказуючи конкретних кроків для отримання результату. SQL дозволяє виражати бажаний результат, а не послідовність дій для досягнення цього стану [17];

HTML (*Hypertext Markup Language*) – мова розмітки, яка використовується для створення вебсторінок. У HTML програміст описує структуру сторінки та її вміст, не вказуючи конкретні кроки щодо розміщення елементів на сторінці. Розмітка HTML декларує структуру сторінки, а не деталі щодо відображення [18];

CSS (*Cascading Style Sheets*) – мова стилів, яка використовується для опису зовнішнього вигляду елементів веб-сторінок. Вона дозволяє програмістам декларативно визначати стилізацію елементів без прив’язки до конкретних екранів чи пристроїв. Визначення стилів CSS описує, як елементи сторінки мають виглядати, без вказівки конкретних дій;

YAML (*YAML Ain't Markup Language*) – формат серіалізації даних, який часто використовується для конфігураційних файлів та обміну даними між програмами. Синтаксис YAML декларативно описує дані та їх структуру, дозволяючи програмістам чітко виразити бажаний стан системи у текстовому вигляді;

Ansible – інструмент автоматизації, який використовує декларативний підхід до опису конфігурації систем та процесів розгортання. Він дозволяє програмістам описувати бажаний стан системи та автоматизувати процеси управління інфраструктурою без необхідності вказувати конкретні кроки для досягнення цього стану.

Приклади практичного використання декларативного підходу в різних сферах розробки програмного забезпечення

Хмарні інформаційні системи – це інформаційні системи (ІС), тобто сукупність технологій та сервісів, які базуються на концепції хмарного обчислення і використовують віртуалізацію ресурсів для надання послуг через Інтернет.

Важливою рисою хмарних ІС є їхній потужний масштабований потенціал. Це означає, що вони можуть забезпечити велику обчислювальну потужність за потреби та автоматично зменшити її, коли навантаження зменшується. Такий підхід дозволяє ефективно використовувати ресурси, забезпечуючи при цьому високу продуктивність. Підтримувальна можливість автоматичного резервного копіювання та відновлення даних забезпечує безпеку та надійність інформації.

Мультиплатформеність є важливою характеристикою хмарних ІС. Їх можна використовувати на будь-яких пристроях – комп’ютерах, смартфонах, планшетах тощо.

Також хмарні ІС забезпечують високий рівень захисту даних за допомогою шифрування, ідентифікації користувачів та інших методів безпеки [9].

Хмарні інформаційні системи відкривають нові можливості для розробки, розгортання та управління програмним забезпеченням, сприяючи зниженню витрат та підвищенню продуктивності діяльності. Використання хмарних технологій у сучасних інформаційних системах створює низку переваг та викликів.

Переваги полягають у можливості легко масштабувати ресурси залежно від потреб, що дозволяє підрозділам швидко адаптуватися до змін обсягу роботи. Крім того, використання хмарних технологій дозволяє знизити витрати на інфраструктуру та обслуговування, оскільки підписка на хмарні послуги може бути економічно вигіднішою, ніж закупівля власних серверів та програмного забезпечення. Ще однією перевагою є підвищена доступність та відмовостійкість завдяки географічно розподіленим центрам обробки даних провайдерів хмарних сервісів.

Глобальний доступ до даних та можливість працювати з ними з будь-якого місця та пристрою, що підключений до Інтернету, також є значною перевагою хмарних технологій. Автоматизація багатьох процесів та можливість автоматичного резервного копіювання даних також допомагають забезпечити ефективну роботу та безпеку.

Проте, при використанні хмарних технологій виникає ряд викликів. Одним з найбільших є забезпечення безпеки даних, що вимагає відповідних заходів, шифрування, управління доступом та дотримання нормативних вимог. Залежність від стабільного Інтернет-з’єднання також може становити проблему, хоча сучасні провайдери пропонують різні моделі підключення, включаючи приватні та гібридні хмари. Залежність від одного хмарного провайдера (*vendor lock-in*) через складність міграції даних, є ще одним викликом. Для ефективного використання хмарних технологій важливо враховувати ці виклики та знаходити шляхи їх вирішення.

Для максимального використання переваг хмарних технологій та подолання згаданих викликів потрібен ефективний та гнучкий підхід до розробки та управління інформаційними системами з використанням хмарних технологій, в чому полягає ключова роль декларативного підходу.

Поєднання декларативного підходу з хмарними технологіями дозволяє створювати і управляти інфраструктурою та ресурсами в хмарному середовищі за допомогою декларативних мов програмування або інтерфейсів. Наприклад, вже вищезгадані інструменти інфраструктурного кодування, такі як *Terraform* або *Ansible*, дозволяють описувати потрібний стан інфраструктури у декларативному стилі.

Такий підхід спрощує розгортання та управління хмарними ресурсами, забезпечуючи швидку реакцію на зміни та підтримуючи високий рівень автоматизації та стабільності системи.

Аналіз можливостей використання декларативного підходу для розробки та управління інформаційними системами з використанням хмарних технологій показав, що інтеграція декларативного підходу в розробку хмарних ІС відкриває широкі перспективи для оптимізації процесів розгортання, управління та масштабування хмарних середовищ.

Перш за все, декларативний підхід дозволяє визначити бажаний стан системи або результат, а не послідовність дій для досягнення цього стану. Це дозволяє розробникам та адміністраторам хмарних систем концентруватися на описі потрібного результату, що спрощує процес управління ресурсами та конфігурацією середовища.

Декларативні мови програмування та інструменти, такі як *Terraform* або *Ansible*, надають зручний спосіб опису бажаного стану інфраструктури хмарних середовищ. Завдяки цьому, можливе автоматизоване розгортання, конфігурація та управління інфраструктурою за допомогою скриптів або конфігураційних файлів.

Ще однією перевагою декларативного підходу є його гнучкість та масштабованість. За допомогою декларативних інструментів можна легко змінювати конфігурацію та розмір інфраструктури залежно від потреб проєкту, що робить його ідеальним для хмарних середовищ, де потрібна висока гнучкість та адаптивність.

Однак важливо враховувати виклики, пов'язані з використанням декларативного підходу до інформаційних систем з використанням хмарних технологій. Наприклад, необхідно правильно структурувати конфігураційні файли та скрипти, щоб уникнути конфліктів та непередбачуваних наслідків при автоматизованому управлінні інфраструктурою.

Використання декларативного підходу в розробці та управлінні інформаційними системами, з використанням хмарних технологій, відкриває нові можливості для оптимізації процесів, підвищення ефективності та забезпечення швидкого реагування на зміни в середовищі (рисунок 3).

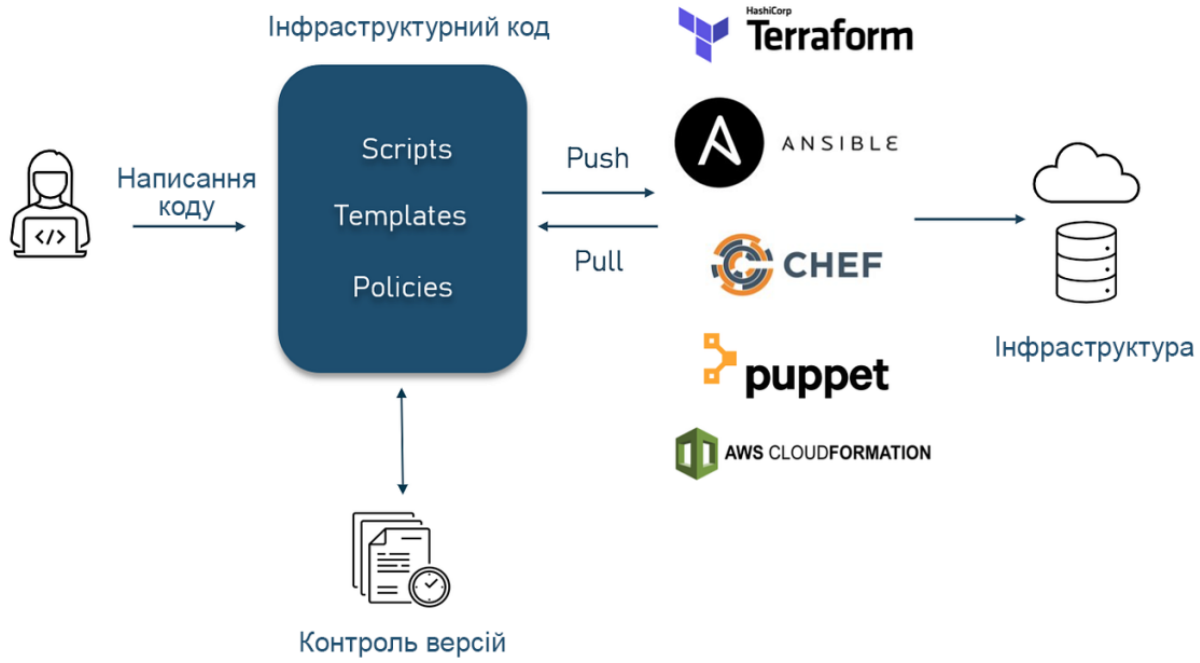


Рис. 3. Загальна схема управління хмарною інфраструктурою з використанням декларативного підходу

Впровадження декларативного підходу в хмарному середовищі відкриває нові можливості, але також має певні виклики, які варто розглянути. У деяких підрозділах Збройних сил України вже локально застосовують цей підхід у своїй інфраструктурі.

Одна з основних переваг декларативного підходу полягає у спрощенні конфігурації систем, оскільки він дозволяє описувати бажаний стан, не вдаючись у деталі процесу його досягнення. Це робить процес налаштування більш зрозумілим та інтуїтивним для розробників та адміністраторів.

Попри можливості, які пропонує декларативний підхід, існують декілька аспектів, які важливо враховувати. Наприклад, команді, що працює над проєктом, може бути складно опанувати декларативні мови програмування та відповідні інструменти. Ця складність може стати перешкодою для швидкого впровадження та ефективного використання декларативного підходу.

Незважаючи на ці виклики, декларативний підхід може забезпечити значні переваги, такі як простота конфігурації, гнучкість та автоматизація процесів у інформаційних систем з використанням хмарних технологій. Тому важливо ретельно зважити всі фактори та обрати найбільш відповідний підхід для конкретних потреб та умов проєкту (таблиця 1).

Таблиця 1

Порівняння декларативного та імперативного підходів

Критерій	**Декларативний підхід**	**Імперативний підхід**
Масштабованість	Висока. Легко адаптується до зростання системи	Обмежена. Складніше масштабувати без значних змін
Підтримка	Простіша. Код більш читабельний і легший для розуміння	Складніша. Може вимагати детального знання всіх процесів
Автоматизація	Відмінна. Легко інтегрується з CI/CD та іншими автоматизованими процесами	Обмежена. Часто вимагає додаткових інструментів для автоматизації
Узгодженість	Висока. Забезпечує єдиний підхід до конфігурації різних систем	Низька. Може призвести до розбіжностей між системами
Безпека	Покращена. Легше впроваджувати та контролювати політики безпеки	Варіативна. Залежить від ретельності реалізації кожного компонента
Гнучкість	Висока. Легко адаптується до змін вимог	Обмежена. Зміни можуть вимагати значного переписування коду
Ефективність використання ресурсів	Оптимізована. Автоматичне управління ресурсами	Залежить від навичок розробника. Може бути неефективною
Швидкість розробки	Висока. Менше коду для досягнення тієї ж функціональності	Нижча. Вимагає написання детальних інструкцій
Контроль низького рівня	Обмежений. Може бути недостатнім для специфічних оптимізацій	Високий. Повний контроль над кожною операцією.
Придатність до застосування в сучасних умовах обстановки	Висока для більшості сучасних систем. Ідеально підходить для управління складними, розподіленими системами	Обмежена. Підходить для специфічних, критично важливих систем реального часу

Приклади успішного використання декларативного підходу в хмарних проєктах

Компанії, які використовують інфраструктуру як код для автоматизації створення та управління хмарною інфраструктурою, часто використовують декларативні мови, такі як *Terraform* або *AWS CloudFormation*. Це дозволяє їм описати бажаний стан інфраструктури та автоматично реалізувати його на основі цього опису.

Проєкти, які використовують контейнери і оркестратори, такі як *Kubernetes*, часто використовують декларативні конфігураційні файли (наприклад, YAML-файли для *Kubernetes).*

Широке використання *Terraform*, *Puppet* та *Ansible* на світовому ринку робить цілком очевидним, наскільки ефективною та надійною є декларативна інфраструктура, такою ж ефективною вона може стати в перспективі з використанням у Збройних силах України [15]. Просто визначивши специфікації для інфраструктури, можна розгортати середовища за допомогою інструментів автоматизації IaC, що підвищить стабільність і продуктивність конвеєра розгортання.

Висновок. У даній статті проведено аналіз існуючих підходів, зокрема декларативного. та визначено його переваги, описано важливість використання декларативного підходу в розробці та управлінні інформаційними системами з використанням хмарних технологій. Використання декларативного програмування надає можливість опису бажаного стану системи або результату, а не послідовності дій для досягнення цього стану. Це сприяє зменшенню складності розробки, полегшує розуміння та роботу з кодом, а також сприяє автоматизації та оптимізації процесів управління інфраструктурою.

Цей підхід дозволяє програмістам описувати бажаний результат або стан системи, не вказуючи конкретних кроків для його досягнення. Натомість, програміст визначає, що потрібно зробити, а система самостійно вирішує, як це зробити.

У статті запропоновано інструмент оцінки – показник IEDAMS, який використаний для оцінки потенційних переваг застосування декларативного підходу у військових IT-структурах відносно імперативного.

Результат оцінки за аналітично-визначеними критеріями показав, що застосування декларативного підходу забезпечує підвищення ефективності розробки та управління інформаційно-комунікаційних систем до 25%.

У сфері розробки програмного забезпечення декларативний підхід застосовується у різних областях. Наприклад, мови запитів до баз даних, такі як SQL, дозволяють виразити бажані результати операцій з даними без необхідності вказувати точні кроки для їх виконання. У веброзробці розмітка HTML декларує структуру сторінки, а CSS визначає її вигляд, без вказання подробиць реалізації.

Підходи декларативного програмування знаходять широке застосування в інформаційних системах з використанням хмарних технологій. Вони дозволяють описувати потреби та вимоги до інфраструктури, конфігурації, а також процесів розгортання та управління ресурсами хмарного середовища без прив'язки до конкретних платформ чи технологій.

Подальші дослідження будуть спрямовані на розробку методів та моделей для автоматизованого аналізу, валідації та тестування декларативних описів інфраструктури ІКС ЗСУ різних ланок управління з використанням хмарних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Christian Endres, Uwe Breitenbücher, Michael Falkenthal, Oliver Kopp, Frank Leymann, Johannes Wettinger. Declarative vs. Imperative: Two Modeling Patterns for the Automated Deployment of Applications. *The 9th International Conference on Pervasive Patterns and Applications (PATTERNS).* 2017. URL: https://www.iaas.uni-stuttgart.de/publications/INPROC-2017-12-Declarative-vs-Imperative-Modeling-Patterns.pdf.

2. Twain Taylor. What does declarative mean in a cloud-native world. *Amazic*: вебсайт. URL: https://amazic.com/what-does-declarative-mean-in-a-cloud-native-world/.

3. Brown, M., & Davis, P. (2023). Declarative Approaches for Cloud Resource Management. Journal of Systems and Software, 185, 111-122. DOI: 10.1016/j.jss.2023.xxx.

4. Michael Wurster, Uwe Breitenbucher1, Antonio Brogi, Lukas Harzenetter1, Frank Leymann, and Jacopo Soldani A declarative approach for service enablement on hybrid cloud orchestration engines. *NOMS 2018 – 2018 IEEE/IFIP Network Operations and Management Symposium*. URL: https://ieeexplore.ieee.org/document/8406175.

5. Розробка технологічної стратегії SAAS рішень із використанням CLOUD-NATIVE технологій в інформаційній системі онлайн. URL: https://archive.liga.science/index.php/universum/article/view/498/504.

6. A review on declarative approaches for constrained clustering, Thi-Bich-Hanh Dao, Christel Vrain August 2024. URL: https://www.sciencedirect.com/science/article/pii/S0888613X24000227?via%3Dihub#se0320.

7. Uwe Breitenbücher, Tobias Binz, Oliver Kopp, Frank Leymann, Johannes Wettinger A Modelling Concept to Integrate Declarative and Imperative Cloud Application Provisioning Technologies. *The 5th International Conference on Cloud Computing and Services Science CLOSER*. 2015. № 1. Pp. 487–496. URL: https://www.iaas.uni-stuttgart.de/publications/INPROC-2015-55-A-Modelling-Concept-to-Integrate-Declarative-and-Imperative-Cloud-Application-Provisioning-Technologies.pdf.

8. Michael Wurster, Uwe Breitenbücher, Antonio Brogi, Lukas Harzenetter, Frank Leymann, Jacopo Soldani. Technology-Agnostic Declarative Deployment Automation of Cloud Applications. *8th IFIP WG 2.14 European Conference, ESOCC*. 2020. URL: https://link.springer.com/chapter/10.1007/978-3-030-44769-4_8.

9. Achilleos, A. P., Kritikos, K., Rossini, A. et al. The cloud application modelling and execution language. *Journal of Cloud Computing:Advances, Systems and Applications*. 2019. № 8. URL: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-019-0138-7.

10. Belmont J. M. Hands-On Continuous Integration and Delivery. 1st edn. Packt Publishing, Birmingham, 2018. URL: https://www.packtpub.com/product/hands-on-continuous-integration-and-delivery.

11. Wettinger J., Andrikopoulos V., Leymann F., Strauch S. Middleware-oriented deployment automation for cloud applications. *IEEE Transactions on Cloud Computing*. 2018. № 6 (4). Pp. 1054–1066. URL: https://www.researchgate.net/publication/296481802_Middleware-Oriented_Deployment_Automation_for_Cloud_Applications.

12. Bergmayr, A., Bruneliere, H., Cabot, J., Hinchey, M., Langer, P., Mayerhofer, T., & Wimmer, M. Benefits of declarative deployment models in DevOps for cloud applications. *Journal of Systems and Software.* 2021. № 175.

13. Rahman, A. A., Mahdavi-Hezaveh, R., & Williams, L. A systematic mapping study of infrastructure as code research. *Information and Software Technology*. 2019. № 108. Pp. 65–77.

14. Cito, J., Leitner, P., Gall, H. C.,Ꝟvšaldćuk, A., Toffetti, G., & von Lerchunderen, R. Towards declarative, multi-cloud deployment models using TOSCA. *In 2017 IEEE International Conference on Software Architecture Workshops (ICSAW)*. 2017. Pp. 1–4.

15. Morris, K. Infrastructure as code: Managing servers in the cloud. *O'Reilly Media*. 2018.

16. Guerriero, M., Garriga, M., Tamburri, D. A., & Palomba, F. Adoption, use and impact of infrastructure as code: A case study. *In 2019 IEEE/ACM 13th International Workshop on Software Engineering for Science (SE4Science)*. 2019. Pp. 1–6.

17. Sharma, S., Coyne, B., Cojocar, G. S., Smyth, B., & Enomoto, K. Understanding developers' perception of declarative infrastructure code: A focus group study. *In 2020 IEEE International Conference on Software Maintenance and Evolution (ICSME).* 2020. Pp. 672–682.

18. Smaldone, S., Brown, A. P., Laws, S., Militello, C., & Farhy, C. Taming the cloud through policy as code. *IEEE Software*. 2021. № 38 (1). Pp. 59–67.

19. Ramakrishnan, R., & Gehrke, J. Database management systems. *McGraw-Hill Higher Education.* 2003.

20. Duckett, J. HTML and CSS: design and build websites. *John Wiley & Sons*. 2011.

DOI: 10.58254/viti.6.2024.19.232

УДК 004.056.57

д-р філософії Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Кисиленко Д. Ю. ORCID: 0000-0001-5491-6231 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ВИЗНАЧЕННЯ ІНВАРІАНТНОЇ КОМПОНЕНТИ В ПОВЕДІНЦІ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ІНТЕГРАЦІЇ НЕЧІТКОЇ ЛОГІКИ ТА ГЕНЕТИЧНИХ АЛГОРИТМІВ

Виявлення поліморфного та метаморфного шкідливого програмного забезпечення є надзвичайно важливим завданням забезпечення кібербезпеки через їх здатність уникати виявлення існуючими системами кіберзахисту шляхом автоматичної модифікації власного коду та/або структури. У даному контексті запропоновано підхід до виявлення поліморфного та метаморфного шкідливого програмного забезпечення, який базується на визначенні інваріантної компоненти для кожного відомого типу шкідливого програмного забезпечення під час аналізу його поведінки. Суть даного підходу полягає у визначенні такої області поведінки, яка залишається незмінною для конкретного типу шкідливого програмного забезпечення, незалежно від проведених модифікацій. Для пошуку зазначеної інваріантної компоненти в поведінці шкідливого програмного забезпечення для кожного його типу, множина значень вихідного простору ознак описується нечіткими лінгвістичними термами з метою отримання множини нечітких продукційних правил для кожного типу шкідливого програмного забезпечення. Наступним кроком є визначення нечіткої інваріантної компоненти для кожного відомого типу шкідливого програмного забезпечення у вигляді нечіткої підмножини ознак з отриманої на попередньому кроці множини нечітких продукційних правил засобами генетичних алгоритмів. Запропонована модель дає змогу значно підвищити точність виявлення поліморфного та метаморфного програмного забезпечення на основі поведінкових характеристик, властивих вже класифікованим зразкам, що, у свою чергу, сприяє підвищенню загальної ефективності системи кібербезпеки.

Ключові слова: *поліморфне та метаморфне шкідливе програмне забезпечення, поведінковий аналіз, кібербезпека, нечітка логіка, машинне навчання, зменшення розмірності, генетичні алгоритми.*

V. Fesokha, D. Kysylenko. A model for determining the invariant component in the behavior of malware software based on the integration of fuzzy logic and genetic algorithms

The detection of polymorphic and metamorphic malware is a critical cybersecurity challenge due to its ability to evade detection by existing cyber defense systems by automatically modifying its own code and/or structure. In this context, an approach to the detection of polymorphic and metamorphic malware is proposed, which is based on the determination of an invariant component for each known type of malware during the analysis of its behavior. The essence of this approach is to define such an area of behavior that remains unchanged for a specific type of malicious software, regardless of the modifications made. To find the specified invariant component in the behavior of malware for each of its types, a set of values of the original feature space is described by fuzzy linguistic terms in order to obtain a set of fuzzy production rules for each type of malware. The next step is to determine the fuzzy invariant component for each known type of malicious software in the form of a fuzzy subset of features from the set of fuzzy production rules obtained in the previous step by means of genetic algorithms. The proposed model makes it possible to significantly increase the accuracy of detection of polymorphic and metamorphic software based on behavioral characteristics characteristic of already classified samples, which, in turn, contributes to increasing the overall effectiveness of the cyber security system.

Keywords: *polymorphic and metamorphic malware, behavioral analysis, cyber security, fuzzy logic, machine learning, dimensionality reduction, genetic algorithms.*

Актуальність та постановка завдання в загальному вигляді. Поліморфне та метаморфне шкідливе програмне забезпечення (ШПЗ) представляє собою одну з найбільш складних та еволюційних загроз для кіберстійкості існуючих інформаційних систем (ІС). Його здатність до модифікації власного коду та/або структури значно ускладнює процес виявлення та нейтралізації існуючими системами кіберзахисту, які здебільшого базуються на поєднанні сигнатурного аналізу та методів машинного навчання для виявлення ШПЗ за відомими ознаками.

За останні роки спостерігається значна еволюція методів створення ШПЗ, які використовують передові системи та технології штучного інтелекту (ШІ) [1, 2]. Існуючі підходи до створення ШПЗ стають все більш автоматизованими та доступними для зловмисників будь-якого рівня кваліфікації. Це дає змогу їм досить швидко генерувати складні

варіації коду та адаптуватися до алгоритмів і моделей існуючих систем кіберзахисту, дозволяючи ШПЗ здійснювати приховану деструктивну діяльність протягом тривалого часу.

Враховуючи зростання кількості та складності поліморфного, олігоморфного та метаморфного ШПЗ, а також недостатню ефективність існуючих систем кіберзахисту в процесі їх виявлення [1] виникає нагальна потреба у вдосконаленні існуючих підходів до виявлення спроб реалізації такого класу загроз.

Аналіз попередніх досліджень. Враховуючи високий рівень адаптації поліморфного та метаморфного ШПЗ, а також використання новітніх технологій для їх модифікації, більшість традиційних методів виявлення мають певні обмеження щодо їх ідентифікації та нейтралізації.

Аналіз нижчевикладених наукових досліджень [3–6] демонструє найбільш ефективні існуючі методи виявлення поліморфного та метаморфного ШПЗ.

У роботах [3–4] пропонується використання *декларативного підходу* до виявлення шкідливих програм, що ґрунтується на аналізі поведінки модулів об’єкта кіберзахисту. Основна ідея дослідження полягає в порівнянні поведінки потенційно шкідливих програм, зокрема на збіжність та повторювання шаблонів у трасах системних викликів, які є характерними для шкідливих програм. Основна відмінність декларативного підходу від інших полягає в тому, що він спрямований на опис бажаного результату або стану системи, а не на використання конкретних методів досягнення цього результату. Так, фахівці з кібербезпеки описують правила і політики для виявлення аномальної поведінки або підозрілих дій у системі, які адаптуються до нових типів загроз, оскільки зміни в політиках та правилах можна вносити без необхідності змінювати основний код або архітектуру системи. Поряд з цим, даний підхід має певні недоліки: декларативним правилам властива недостатня гнучкість, тому виявляти нову деструктивну діяльність, яка не відповідає заздалегідь визначеним шаблонам, їх засобами досить складно; складність у створенні декларативних правил (потребує глибокого розуміння поведінки ШПЗ та контексту, в якому воно діє); залежність від суб’єктивного експертного судження в процесі побудови декларативних правил.

У дослідженні [5] розглядається підхід до виявлення кіберзагроз на основі *еволюційних алгоритмів*. Основна ідея даного підходу полягає у визначенні підмножини найбільш інформативних ознак з вихідної множини ознак для подальшого формування чітких правил виявлення деструктивної діяльності. Визначення підмножини найбільш інформативних ознак здійснюється засобами генетичних алгоритмів (ГА), які дозволяють отримати оптимальні комбінації ознак кіберзагроз. Проте, даний підхід має певні обмеження щодо виявлення поліморфних і метаморфних кіберзагроз. Так, толерантність до неточностей певної невизначеності, забезпечується використанням як дискретних значень ознак, так і діапазонів їх значень, що значно ускладнює роботу ГА щодо визначення оптимальної підмножини ознак кіберзагроз. До того ж, підмножина правил для кожного відомого класу кіберзагроз визначається окремо, що може призвести до випадків класифікації кіберзагрози одного класу як екземпляра іншого класу.

У роботі [6] запропоновано модель виявлення кібератак нульового дня на основі визначення підмножини найбільш значущих ознак для кожного відомого класу кібератак експертним шляхом. Так, в першу чергу вихідна множина значень для всіх відомих класів кібератак описується нечіткими правилами. Далі експертом визначається підмножина ознак з подальшим перетином вихідної та результуючої підмножин, з метою отримання таких нечітких правил, які достатньо повно описують незмінну структуру в ознаках кібератак для кожного відомого їх класу. Побудована модель за рахунок використання нечіткого опису незмінної структури в ознаках кібератак для кожного відомого їх класу є адаптивною, оскільки дозволяє виявляти поліморфні та метаморфні кібератаки, побудовані на основі раніше відомих

кібератак. Основним недоліком даного підходу є його залежність від суб'єктивного експертного судження при визначенні найбільш значущих ознак кібератак.

Підводячи підсумок розглянутих підходів щодо виявлення поліморфного та метаморфного ШПЗ, можна зробити висновок, що кожен з них має певну множину обмежень, які знижують їх ефективність. Жоден з розглянутих методів не використовує весь потенціал ключової особливості поліморфних та метаморфних кіберзагроз – інваріантної компоненти в їх поведінці під час динамічного аналізу. Використання інваріантної компоненти в поведінці ШПЗ для виявлення поліморфного та метаморфного ШПЗ на основі поєднання переваг нечіткої логіки та ГА може суттєво підвищити ефективність його виявлення та забезпечити ефективний кіберзахист ІС, у тому числі від нових зразків ШПЗ.

Метою статті є розробка моделі визначення інваріантної компоненти в поведінці ШПЗ на основі інтеграції нечіткої логіки та генетичних алгоритмів.

Модель визначення інваріантної компоненти в поведінці ШПЗ. Оскільки переважна більшість зразків існуючого поліморфного та метаморфного ШПЗ є модифікаціями вже існуючих (класифікованих) шкідливих програм, то за умови збереження їх інформаційно-деструктивного вектору впливу залишається незмінною певна підмножина поведінкових ознак для кожного відомого типу ШПЗ [1, 6, 7]. Ця підмножина описує інваріанту компоненту для кожного типу ШПЗ, тоді як решта ознак відображають поліморфну та/або метаморфну компоненту ШПЗ. Виходячи з цього, поведінка кожного окремого екземпляра певного типу ШПЗ є поліморфною та/або метаморфною по відношенню до решти зразків.

Враховуючи викладене, для вирішення завдання усунення виявлених недоліків існуючих підходів до протидії поліморфному та метаморфному ШПЗ [3–6] доцільно використати підхід, запропонований в роботі [7]. Суть даного підходу полягає у визначенні підмножини таких ознак з усього вихідного простору ознак поведінки ШПЗ, значення яких є інваріантними або близькими до інваріантних для кожного окремого типу ШПЗ.

Так, визначення підмножини шуканих ознак (інваріантної компоненти) доцільно здійснювати на основі підходу зменшення розмірності простору вихідних ознак, що описують поведінку ШПЗ засобами ГА. Вибір ГА для реалізації даного завдання обумовлено їх перевагами над іншими методами зниження розмірності, зокрема властивостями стійкості до шуму в даних та потенційною здатністю визначати глобальний оптимум [7]. Оскільки значення більшості ознак, які описують поведінку ШПЗ одночасно для всіх відомих його типів є варіативними (представлені діапазонами значень), тому доцільно описати навчальну вибірку нечіткими лінгвістичними термами. Даний підхід дає змогу:

значно зменшити обчислювальну складність ГА в процесі визначення інваріантної компоненти в поведінці ШПЗ на основі підходу зменшення розмірності простору ознак;

врахувати варіативність поведінкових ознак, які характерні для поліморфного та метаморфного ШПЗ;

глибоко розуміти приховані структури в поведінці ШПЗ внаслідок їх інтерпретації нечіткими правилами;

забезпечити гнучкість та адаптивність підходу в процесі виявлення поліморфного та метаморфного ШПЗ.

Для аналітичного обґрунтування зазначеного, представимо покроковий формальний опис математичної моделі визначення інваріантної компоненти в поведінці поліморфного та метаморфного ШПЗ. На рисунку 1 зображено узагальнену схему визначення інваріантної компоненти в поведінці ШПЗ шляхом зниження розмірності простору досліджуваних ознак на основі інтеграції нечіткої логіки та ГА, де x_i – ознака [7].

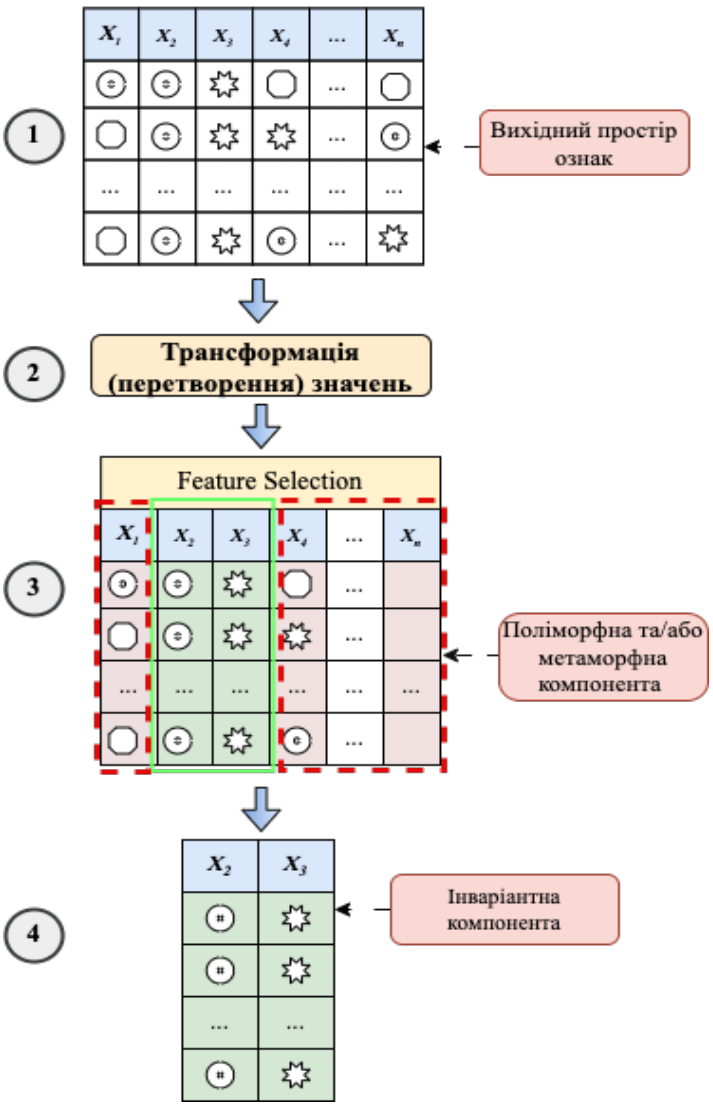


Рис. 1. Узагальнена схема визначення інваріантної компоненти в поведінці ШПЗ на основі інтеграції нечіткої логіки та ГА

1. *Ініціалізація вихідного простору ознак* $x_1 - x_n$ з навчальної вибірки опису поведінки ШПЗ, де окрема ознака x_i відповідає певному аспекту деструктивної діяльності відомих типів $T_1 - T_m$ (класів) ШПЗ, таких як [8, 13]:

worms (мережеві хробаки) – самостійно поширюються мережами створюючи власні копії;

trojans (троянське програмне забезпечення) – маскує шкідливу активність під легальне програмне забезпечення (ПЗ);

комп'ютерні віруси – прикріплюються до файлів чи програм з метою подальшої активації під час їх запуску;

rootkits (руткіти) – надають зловмисникам контроль над об'єктом атаки;

packers (пакувальники) – використовуються для стиснення або обфускації ШПЗ з метою уникнення виявлення захисними системами;

ransomware (програми вимагачі) – шифрують файли та вимагають викуп за їх розшифрування;

fileless malware (безфайлові програми) – функціонують в оперативній пам'яті, не створюючи жодних файлів на жорсткому диску;

spyware (шпигунське програмне забезпечення) – автоматично збирає конфіденційну інформацію без відома користувача;

adware (рекламне програмне забезпечення) – показує небажану рекламу;

keyloggers (логери клавіш) – відслідковують та записують кожне натискання клавіш;

bots – дистанційно керують інфікованими пристроями;

wiper malware – знищує або видаляє дані на жорсткому диску.

2. *Трансформація (перетворення) діапазонів значень ознак* навчальної вибірки засобами нечітких лінгвістичних термів з метою формування підмножин нечітких правил для кожного відомого типу ШПЗ. Для реалізації зазначеного, вхідні лінгвістичні змінні визначаються як початковий простір ознак $X_i = \left[x_i, \underline{x_i}\right]$ навчальної вибірки та вихідною лінгвістичною змінною $y \in Y = \left[y, \underline{y}\right]$ – висновком щодо належності фіксованого вектору ознак поведінки певному типу ШПЗ. Так, відповідність вектора фіксованих значень поведінки ШПЗ конкретному типу ШПЗ представлено наступним аналітичним виразом (1):

$$X = (x_1, \dots, x_n) \to y = d_j\left(a_j^1, \dots, a_i^{j_i}, \dots, w_1, w_n\right) \in D = (d_1, \dots, d_m), \quad (1)$$

де $i = \overline{1, \dots, m}$; y – лінгвістичний опис висновку $d \in D$ для вектора значень $\{x_1, \dots, x_n\}$; d – лінгвістичний терм; $a_i^{l_i}$ – номери комбінацій значень ознак; w_n – вага нечіткого правила; m – кількість можливих значень змінної y.

Відповідно до [6, 9] залежність між досліджуваним простором ознак та відповідним прийнятим рішенням може бути представлено у вигляді композиційної таблиці 1.

Таблиця 1

Композиційна таблиця множини отриманих нечітких правил

Номер вхідної комбінації	Вхідна підмножина поведінкових ознак				Ваговий коефіцієнт	Вхідна змінна y
	x_1	x_2	… x_i …	x_n		
11	a_1^{11}	a_2^{11}	… a_i^{11} …	a_n^{11}	w_{11}	d_1
12	a_1^{12}	a_2^{11}	… a_i^{12} …	a_n^{12}	w_{12}	
…	…	…	…			
$1k_1$	$a_1^{1k_1}$	$a_2^{1k_1}$	… $a_i^{1k_1}$ …	$a_n^{1k_1}$	w_{1k_1}	
…	…	…	…	…	…	…
$j1$	a_1^{j1}	a_2^{j1}	… a_i^{j1} …	a_n^{j1}	w_{j1}	d_j
$j2$	a_1^{j2}	a_2^{j2}	… a_i^{j2} …	a_n^{j2}	w_{j2}	
…	…	…	…	…	…	
jk_j	$a_1^{jk_j}$	$a_2^{jk_j}$	… $a_i^{jk_j}$ …	$a_n^{jk_j}$	w_{jk_j}	
…	…	…	…	…	…	…
$m1$	a_1^{m1}	a_2^{m1}	… a_i^{m1} …	a_n^{m1}	w_{m1}	d_m
$m2$	a_1^{m2}	a_2^{m2}	… a_i^{m2} …	a_n^{m2}	w_{m2}	
…	…	…	…	…	…	
mk_m	$a_1^{mk_m}$	$a_2^{mk_m}$	… $a_i^{mk_m}$ …	$a_n^{mk_m}$	w_{mk_m}	

де x_i – поведінкова ознака; w_n – вага нечіткого правила; $a_i^{j_k}$ – номери комбінацій значень ознак; *d* – лінгвістичний терм змінної y; *m* – кількість можливих значень змінної y.

Функція належності – гаусова. Спосіб визначення оптимальної кількості термів для кожної ознаки – показник силуету. Алгоритм нечіткого логічного виводу – Мамдані. Після трансформації значень необхідно здійснити видалення дублікатів правил.

3. *Зниження розмірності досліджуваного простору ознак* засобами ГА полягає у визначенні інваріантної компоненти в поведінці ШПЗ шляхом відбору таких ознак, які закономірно (системно) в сукупності повторюються для більшості екземплярів кожного класу ШПЗ [10, 11].

На основі викладеного виникає завдання пошуку оптимальної підмножини ознак для кожного типу ШПЗ, засобами якої точність класифікації екземплярів ШПЗ буде максимальною для коректного типу і водночас мінімальною для решти типів. Доцільність реалізації такого підходу обумовлюється виключенням можливості отримання ідентичних інваріантних компонент для різних типів ШПЗ на спільному просторі ознак та забезпечення її специфічності для кожного типу [7].

Вхідними даними на даному етапі є композиційна таблиця нечітких правил, отримана на попередньому етапі. Ген ГА – ознака $x_i \in X$. Кожне рішення (хромосома) у ГА представляє підмножину ознак X_{sub} з простору ознак *X*, яка може бути ефективною для класифікації ШПЗ за типами. Представлення підмножин у популяції здійснюється засобами двійкового кодування (вектором двійкових значень довжиною *m <= n, де m – потужність підмножини* X_{sub}*; n – потужність підмножини X*); де кожен біт відповідає певній ознаці *i*. Наявність одиниці в бітовому рядку [1, 0, 1, 0, 1] відповідає відбору *i-ї* ознаки до підмножини X_{sub}.

Цільова функція ГА (Target Function): пошук оптимальної підмножини ознак поведінки ШПЗ для подальшої класифікації за типами (2).

$$TF(X_{sub}) = \arg\max\left(Accuracy\left(X_{sub,\ target}\right) - \sum_{i \neq target} Accuracy(X_{sub,\ i}) \right), \tag{2}$$

де X_{sub} – підмножина ознак, яку генерує ГА;

$Accuracy\left(X_{sub,\ target}\right)$ – точність класифікації для коректного типу ШПЗ (цільовий тип);

$\sum_{i \neq target} Accuracy\left(X_{sub,\ i}\right)$ – сума значень точностей класифікації для всіх інших типів ШПЗ;

arg max – аргумент (підмножина ознак), при якому функція досягає максимального значення.

Функція пристосованості ГА (Fitness Function): оцінка кожної отриманої підмножини X_{sub} щодо її ефективності максимізувати точність класифікації для цільового типу ШПЗ і мінімізувати для решти типів. Математична модель даної функції пристосованості може бути представлена аналітичним виразом (3).

$$FF(X_{sub}) = Accuracy\left(X_{sub,\ target}\right) - \sum_{i \neq target} Accuracy\left(X_{sub,\ i}\right). \tag{3}$$

Система класифікації: нечіткий логічний вивід Мамдані [12].

Критерії зупинки ГА: алгоритм може бути зупинено за умов отримання максимального значення ефективності класифікації ШПЗ за показником точності.

Результат роботи ГА: отримання підмножини ознак X_{sub}, яка є інваріантною для цільового типу ШПЗ.

Виконання ГА [13]:

1. *Формування початкової популяції:* алгоритм розпочинає роботу з випадково згенерованих початкових підмножин ознак (популяції), що являє собою певне рішення задачі в першому наближенні.

2. *Обчислення значень функції пристосованості:* на кожній ітерації ГА підмножини популяції оцінюються за допомогою функції пристосованості.

3. *Перевірка умови зупинки алгоритму:* якщо результат задовольняє умову завершення алгоритму – кінець алгоритму, у противному випадку – далі.

4. *Селекція пар батьківських хромосом:* вибір батьківських підмножин для операції схрещування полягає у виборі (на основі розрахованих на 2-му етапі значень функції пристосованості) тих підмножин X_{sub}, які будуть брати участь в створенні нащадків для наступного покоління. Дана операція здійснюється відповідно до принципу природного відбору, за яким найбільші шанси на участь в створенні нових нащадків мають підмножини з найбільшими значеннями функції пристосованості. Найбільш популярним вважається метод рулетки, який отримав свою назву за аналогією з відомою азартною грою. Кожній підмножині виділено сектор колеса рулетки, величина якого пропорційна значенню її функції пристосованості. Чим більше значення функції, тим більший сектор на колесі рулетки.

5. *Застосування генетичних операторів (схрещування, мутація)*: оператор схрещування (P_c), сприяє обміну генетичною інформацією між батьківськими підмножинами з метою створення нових нащадків. Цей процес полягає у випадковому об'єднанні підмножин батьківської популяції у пари, де в точках схрещування (L_k) відбувається обмін генетичною інформацією. Це сприяє розширенню простору пошуку та збереженню важливих ознак в нащадках. Результатом схрещування пари батьківських підмножин є створення пари нащадків. Оператор мутації P_m зазвичай використовується на батьківській популяції перед схрещуванням, або на новій популяції, що утворена в результаті схрещування. Мутація полягає у випадковій заміні ознак у підмножині з метою уникнення локальних мінімумів. Далі формується нова популяція, яка стає поточною для наступної ітерації. Процес виконується до виконання умов зупинки.

6. *Отримання результату:* якщо аналітичний опис поведінки деякого екземпляра конкретного типу ШПЗ можна представити у вигляді (4) [6]:

$$X = \{x_1, x_2, \dots, x_i, \dots, x_n\}, \text{де } i = \overline{1,n}, \tag{4}$$

то поведінку поліморфного (метаморфного) йому екземпляра того ж типу ШПЗ представимо як (5):

$$X_{plmf} = \{f_1(x_1), f_2(x_2) \ \dots, x_i, \dots, f_m(x_m)\}, i \in I_{inv}, f_i(x_i) \in F_{plmf}, \tag{5}$$

де x_i – поведінкова ознака; $f_i(x_i)$ – функція модифікації ознак; I_{inv} – підмножина індексів інваріантних ознак; F_{plmf} – підмножина функцій $f_i(x_i)$, які змінюють ознаки x_i.

Звідси, інваріантна компонента описується наступним чином (6):

$$X_{inv} = \{x_i \in X \mid x_i = static\}, i \in \tag{6}$$

Так, для типів ШПЗ [14] Ransomware, Fileless Malware, Spyware, Adware, Trojans, Worms, Rootkits, Keyloggers, Bots, Wiper Malware (7):

$$X_{ransom} = \{x_1^1, x_2^1, \dots, x_n^1\} \rightarrow X_{ransom}^{inv}\{x_1^1, x_2^1, \dots, x_m^1\}, \tag{7}$$

$$X_{fileless} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{fileless}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{spy} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{spy}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{ad} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{ad}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{trojans} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{trojans}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{worms} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{worms}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{rootkits} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{rootkits}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{keyloggers} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{keyloggers}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{bots} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{bots}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$
$$X_{wiper} = \{x_1^1, x_2^1, \dots, x_n^1\} \to X_{wiper}^{inv} = \{x_1^1, x_2^1, \dots, x_m^1\},$$

де m – кількість поведінкових ознак інваріантної компоненти ШПЗ.

Після виконання певної кількості ітерацій алгоритм сходиться до найкращої підмножини X_{sub}, яка буде являти собою оптимальне або субоптимальне рішення. Таким чином, на основі отриманих нечітких підмножин поведінкових ознак для кожного відомого типу ШПЗ, які описують їх інваріантну активність у процесі реалізації кібервпливу, здійснюємо виявлення поліморфного або метаморфного ШПЗ засобами нечіткого логічного виводу (8).

$$\mu^{d_j}(x_1, x_2, \dots, x_{n(mp)}) = \max_{p=\overline{1,k_j}}\{w_{jp}\min_{i=\overline{1,n}}[\mu^{jp}(x_i)]\}, \mathrm{j} = \overline{1,m}. \quad (8)$$

В якості прийнятого рішення про наявність/відсутність деструктивної активності ШПЗ визначається результат з максимальним значенням, отриманим в результаті згортки функцій належності термів нечітких правил опису їх інваріантних компонент для кожного типу ШПЗ $T_1 - T_m$.

Оцінка ефективності. Для визначення точності виявлення ШПЗ на основі запропонованої моделі було використано офіційний набір даних про кіберзагроз ML-Based NIDS Datasets, зокрема NF-UQ-NIDS-v2 [15], який містить опис різноманітних типів ШПЗ. Обрані зразки ШПЗ у NF-UQ-NIDS-v2 [15]:

analysis – різноманітні загрози, націлені на вебдодатки через порти, електронну пошту та скрипти (2190 зразків);

generic – ШПЗ, здатне до несанкціонованого саморозмноження локальними ресурсами комп'ютера (12098 зразків);

ransomware – ШПЗ для шифрування файлів з метою вимагання компенсації в обмін на метод/ключ розшифрування (3420 зразків);

shellcode – ШПЗ для віддаленого контролю об'єкта впливу (1426 зразків);

theft – ШПЗ для отримання конфіденційної інформації, наприклад, крадіжка даних або клавіатурне шпигунство (2410 зразків);

worms – ШПЗ для самокопіювання та поширення на інші вузли мережі (163 зразки).

В таблиці 2 наведено результати визначення нечітких інваріантних компонент ШПЗ, описаних зазначеними підмножинами ознак для кожного типу ШПЗ з усього представленого простору ознак, а також ефективність виявлення ШПЗ за показником точності на їх основі.

Таблиця 2

Визначені інваріантні компоненти поведінки
ШПЗ і точність виявлення ШПЗ

ШПЗ / **Ознака**	Analysis	Generic	Ransomware	Shellcode	Theft	Worms
L4_SRC_PORT						
L4_DST_PORT	■					
PROTOCOL			■	■	■	■
L7_PROTO						
IN_BYTES				■		
IN_PKTS	■	■		■		■
OUT_BYTES	■	■	■	■		■
OUT_PKTS	■	■		■		
TCP_FLAGS						
CLIENT_TCP_FLAGS						
SERVER_TCP_FLAGS						
FLOW_DURATION_MILLISECONDS						
DURATION_IN	■	■	■	■		■
DURATION_OUT		■				
MIN_TTL				■		
MAX_TTL						
LONGEST_FLOW_PKT	■	■	■	■		■
SHORTEST_FLOW_PKT			■		■	
MIN_IP_PKT_LEN						
MAX_IP_PKT_LEN	■	■	■	■		■
SRC_TO_DST_SECOND_BYTES	■	■	■	■		■
DST_TO_SRC_SECOND_BYTES	■	■		■	■	■
RETRANSMITTED_IN_BYTES	■	■	■	■	■	
RETRANSMITTED_IN_PKTS		■				
RETRANSMITTED_OUT_BYTES	■	■		■	■	
RETRANSMITTED_OUT_PKTS	■	■		■	■	
SRC_TO_DST_AVG_THROUGHPUT	■	■		■		
DST_TO_SRC_AVG_THROUGHPUT	■	■		■		
NUM_PKTS_UP_TO_128_BYTES	■	■	■	■		■
NUM_PKTS_128_TO_256_BYTES	■	■		■		■
NUM_PKTS_256_TO_512_BYTES				■	■	■
NUM_PKTS_512_TO_1024_BYTES						
NUM_PKTS_1024_TO_1514_BYTES	■	■		■		
TCP_WIN_MAX_IN						
TCP_WIN_MAX_OUT						
ICMP_TYPE						
ICMP_IPV4_TYPE						
DNS_QUERY_ID	■		■	■	■	■
DNS_QUERY_TYPE	■		■	■	■	■
FTP_COMMAND_RET_CODE	■		■		■	■
Точність (%)	100	99,6	98,6	100	98	98,8

Висновки. У статті вирішується актуальне наукове завдання визначення інваріантної компоненти в поведінці ШПЗ. Запропоновано модель визначення інваріантної компоненти в поведінці ШПЗ на основі поєднання переваг нечіткої логіки та ГА. Суть даної моделі, що відрізняє її від існуючих, полягає в автоматизованому визначенні засобами ГА підмножини таких поведінкових ознак ШПЗ, описаних нечіткими лінгвістичними термами, які представляють унікальну інваріантну компоненту для кожного відомого типу ШПЗ. Оцінка ефективності розробленої моделі демонструє високу точність виявлення ШПЗ на основі попередньо визначених нечітких інваріантних компонент ШПЗ. Застосування даної моделі дає змогу описувати поведінку ШПЗ за умов певної нечіткості значень досліджуваних ознак без залучення експертів, а також підвищити ефективність виявлення поліморфного та метаморфного ШПЗ.

Перспективним напрямком подальших наукових досліджень є розробка методу самонавчання підсистеми кіберзахисту на основі використання запропонованої моделі в процесі протидії ШПЗ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Фесьоха В. В., Кисиленко Д. Ю., Нестеров О. М. Аналіз спроможності існуючих систем антивірусного захисту та покладених у їхню основу методів до виявлення нового шкідливого програмного забезпечення у військових інформаційних системах. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2023. Т. 3. С. 143–151.

2. Фесьоха В. Особливості протистояння оборонного та наступального штучного інтелектів у кіберпросторі. *International Science Journal of Engineering & Agriculture*. 2024. Т. 3, № 4. С. 105–114. URL: https://doi.org/10.46299/j.isjea.20240304.11.

3. Bernardi M. L., Cimitile M., Mercaldo F. Process mining meets malware evolution: a study of the behavior of malicious code. *International symposium on computing and networking – across practical development and theoretical research*. 2016. URL: https://www.semanticscholar.org/paper/Process-Mining-Meets-Malware-Evolution:-A-Study-of-Bernardi-Cimitile/7838664913ba2ab34d78f6120188293bd77a7fb3.

4. Ardimento P., Bernardi M. L., Cimitile M. Malware phylogeny analysis using data-aware declarative process mining. *IEEE conference on evolving and adaptive intelligent systems (EAIS)*. 2020. URL: https://www.semanticscholar.org/paper/Malware-Phylogeny-Analysis-using-Data-Aware-Process-Ardimento-Bernardi/859dd8a091b4af71426a189225ee09a3a2e78a69.

5. Метод виявлення кіберзагроз на основі еволюційних алгоритмів / С. М. Лисенко, Д. І. Стопчак, В. В. Самотес // Вісник Хмельницького національного університету. Технічні науки. 2017. № 6. С. 81–88. URL: http://nbuv.gov.ua/UJRN/Vchnu_tekh_2017_6_15.

6. Zero-day polymorphic cyberattacks detection using fuzzy inference system / V. V. Fesokha et al. *Austrian Journal of Technical and Natural Sciences*. 2020. P. 8–13. URL: https://doi.org/10.29013/ajt-20-5.6-8-13.

7. Фесьоха В. В., Кисиленко Д. Ю., Фесьоха Н. О. Обґрунтування вибору підходу до визначення інваріантної компоненти у поведінці поліморфного (метаморфного) шкідливого програмного забезпечення на основі зниження розмірності простору ознак. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2024. Т. 5. С. 181–192.

8. Енциклопедія Інтернет-загроз – ESET. *ESET*. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/.

9. Subach I., Fesokha V. Model of detecting cybernetic attacks on information-telecommunication systems based on description of anomalies in their work by weighed fuzzy rules. *Collection "Information technology and security"*. 2017. Vol.5, no. 2. P. 145–152. URL: https://doi.org/10.20535/2411-1031.2017.5.2.136984.

10. Feature dimensionality reduction: a review – Complex & Intelligent Systems. *SpringerLink*. URL: https://link.springer.com/article/10.1007/s40747-021-00637-x#:~:text=The%20basic%20principle%20of%20feature,5,6,7].

11. Sanjyal A. Dimensionality reduction VS feature selection. *Medium*. URL: https://medium.com/@asanjyal81/dimensionality-reduction-vs-feature-selection-e68f91aa8724.

12. Зінов‘єва О. Г., Лубко Д. В. Алгоритм Мамдані в системах нечіткого виведення. *ElarTSATU: Home*. URL: http://elar.tsatu.edu.ua/handle/123456789/16952.

13. Kanade V. Genetic algorithms – meaning, working, and applications – spiceworks. *Spiceworks*. URL: https://www.spiceworks.com/tech/artificial-intelligence/articles/what-are-genetic-algorithms/.

14. 12 Types of Malware + Examples That You Should Know | CrowdStrike. *CrowdStrike: We Stop Breaches with AI-native Cybersecurity*. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/.

15. ML-Based NIDS Datasets. *School of Information Technology and Electrical Engineering*. URL: https://staff.itee.uq.edu.au/marius/NIDS_datasets/#RA6.

DOI: 10.58254/viti.6.2024.20.243

УДК 681.396.6

д-р техн. наук, професор Хорошко В. О. ORCID:0000-0001-6213-7086 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Клімович С. О. ORCID: 0000-0001-7209-2176 (ВІТІ ім. Героїв Крут)
Ланко А. В. ORCID: 0009-0001-1124-1526 (ВІТІ ім. Героїв Крут)

МАТЕМАТИЧНА МОДЕЛЬ КОНТРОЛЮ ЯКОСТІ ОЦІНКИ ТЕХНІЧНОГО СТАНУ РАДІОЕЛЕКТРОННОГО ОБЛАДНАННЯ

У статті розглядається питання контролю технічного стану радіоелектронного обладнання спеціального призначення в умовах впливу зовнішніх факторів. Основна увага приділяється формалізації процесу контролю через побудову математичної моделі, яка описує залежність вихідних параметрів системи контролю від внутрішніх та зовнішніх впливів.

Проаналізовано існуючі методи контролю, які відображають складнощі вибору точок контролю в сучасних інтегральних схемах. Показано необхідність впровадження нових, більш гнучких та адаптивних рішень при розв'язанні задач технічного діагностування. У роботі пропонується вдосконалена математична модель контролю технічного стану радіоелектронного обладнання, яка дозволяє більш точно оцінювати функціональний стан об'єкта контролю в реальному часі. Процес контролю описується в моделі через імовірності зміни стану узагальненого показника який забезпечує точність системи контролю. Такий підхід до контролю якості функціонального стану об'єкта на основі побудови стохастичних графів дозволяє оцінити імовірність помилки і точність під час контролю технічного стану.

Результати дослідження можуть бути застосовані для ефективного обслуговування радіоелектронного обладнання, а також покращення показників діагностування технічного стану та передбачення можливих відмов об'єкта контролю.

Ключові слова: *радіоелектронне обладнання, система контролю (діагностування), методика, узагальнений показник, елементарні операції, імовірність станів.*

V. Khoroshko, S. Klimovych, A. Lanko. Mathematical model of quality control assessment of the technical condition radio electronic equipment

The article examines the issue of monitoring the technical condition of special-purpose radio-electronic equipment under the influence of external factors. The main attention is paid to the formalization of the control process through the construction of a mathematical model that describes the dependence of the initial parameters of the control system on internal and external influences.

The existing control methods are analyzed, which reflect the difficulties of selecting control points in modern integrated circuits. The necessity of introducing new, more flexible and adaptive solutions in solving the problems of technical diagnostics is shown. The work proposes an improved mathematical model for monitoring the technical condition of radio-electronic equipment, which allows more accurate assessment of the functional state of the control object in real time. The control process is described in the model through probabilities of changing the state of a generalized indicator that ensures the accuracy of the control system. This approach to quality control of the functional state of the object based on the construction of stochastic graphs allows to estimate the probability of error and accuracy during the control of the technical condition.

The results of the research can be applied to the effective maintenance of radio-electronic equipment, as well as improving indicators of diagnosing the technical condition and predicting possible failures of the control object.

Keywords: *radio-electronic equipment, control system (diagnosis), method, generalized indicator, elementary operations, probability of states.*

Постановка завдання. При проєктуванні засобів і систем контролю (діагностування) радіоелектронного обладнання (РЕО) спеціального призначення, а також у процесі їх експлуатації виникають задачі передбачення негативних (аварійних, заперечних) ситуацій процесу контролю. Зазвичай, цей процес відбувається в умовах, які потребують врахування елементів випадковості впливу зовнішніх факторів. Вирішення цих задач передбачає в собі формалізацію дослідження процесів формування рішень при контролі, а для застосування аналітичних методів у цих дослідженнях необхідна побудова математичної моделі контролю (системи рівнянь, операторів), яка описує залежність вихідних характеристик системи контролю (СК) від внутрішніх та зовнішніх впливів при функціонуванні РЕО [1, 2].

Якість контролю РЕО (обладнання, технічних процесів) визначається наступними поняттями (ознаками): фізична величина, сукупність фізичних величин, технічна характеристика, узагальнений показник тощо.

Аналіз основних досліджень і публікацій. Проведений аналіз показав, що у роботах [1–12] наведені методи, способи та принципи контролю і діагностування різних радіоелектронних систем. В окремих роботах [1] стверджується, що важливою і достатньою умовою перевірки електричних зв'язків у мікросхемі є:

– доступність функціональних елементів крізь первинні входи;

– можливість транспортування несправностей до первинних виходів.

При цьому, об'єкт контролю (мікросхема), як правило, лише частково відповідає умовам, що згадані у роботі [1].

Враховуючи складність вибору контрольних точок і неможливість забезпечити доступ до них (неможливість створення додаткових контрольних виходів), доцільно розробити варіант аналізу схеми з врахуванням існуючих обмежень. Це особливо важливо при контролі та діагностуванні схем з високим ступенем інтеграції елементів і наявності великої кількості зворотних зв'язків, що характерно для великих інтегральних схем (ВІС).

Слід зауважити, що в роботах [2–3] наведені моделі контролю технічного стану РЕО, але ці моделі відносяться до статичного стану систем. Тобто, коли система функціонує нормально або коли система вже знаходиться у аварійному стані.

Слід враховувати, що методи та способи, які описані в літературі [4–5] не дають можливості швидко отримати якісні результати контролю функціонального стану об'єкта, а отримані результати ще слід додатково аналізувати та опрацьовувати.

На відміну від згаданих варіантів розв'язання визначеної технічної задачі, застосування математичної моделі дозволяє якісно оцінити функціональний стан об'єкта контролю у реальному часі та отримати інформацію щодо контролю якості цієї оцінки. Крім того, застосовування додаткових обчислень на обробку отриманої інформації не потрібне.

Метою статті є опис математичної моделі контролю якості оцінки технічного стану радіоелектронного обладнання, що дозволить здійснювати швидке обслуговування радіоелектронного обладнання.

Виклад основного матеріалу. Ознака якості контролю РЕО може знаходитись в одному з m можливих станів. При цьому події F_z, які визначають умови знаходження узагальненого показника (УП) в z-му стані записуються в наступному вигляді:

$$F_z: \{\theta \in [d_{z-1};\ d_z]\}, \tag{1}$$

де d_{z-1} – нижня границя z-го стану УП;

d_z – верхня границя z-го стану УП.

З точки зору дослідження операцій контролю, як будь-який інший захід (система дій), об'єднаний одним задумом і направлений задля досягнення визначеної цілі, являється операцією контролю.

Операція контролю [3] вміщує елементарні операції (ЕО), які виконуються у визначеній послідовності, а ступінь деталізації визначається метою дослідження. Процес контролю (операція контролю) полягає в тому, що УП піддається послідовному перетворенню.

Висновок за приналежністю УП за розрізненням, з точки зору контрольного експерименту, стану виконується шляхом розбраковки, порівняння результатів виміру перетвореного УП з встановленими межами станів.

При цьому стани G_i, визначають умови прийняття рішення визначеності УП i-му стану, записується у вигляді:

$$G_i: \{Y \in [D_{i-1};\ D_i]\}, \tag{2}$$

де Y – результат виміру перетвореного УП;

D_{i-1} – нижня границя i-го стану перетвореного УП;

D_i – верхня границя i-го стану перетвореного УП.

Оскільки події F_z і G_i внаслідок помилок контролю можуть не співпадати, за результатами контролю УП, знаходяться в z-му стані, можуть бути розрізнені m взаємно виключних подій $F_z\ G_i, i = \overline{1,m}$.

Графічно операція контролю z-го стану УП може бути представлена у вигляді стохастичного графу (рисунок 1) у якому імовірності відсутності дуг відповідають вірогідним імовірностям переходів, а імовірності реалізації вузлів – безумовним імовірностям подій.

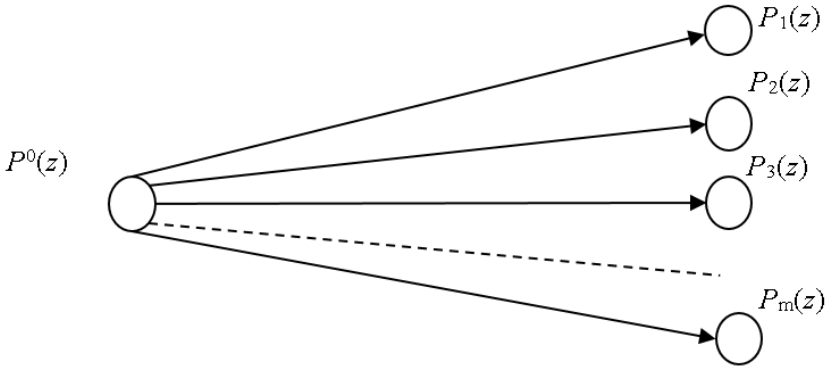


Рис. 1. Стохастичний граф операції контролю z-го стану УП

З рисунку видно, що $P^0(z) = P(\theta \in F_z)$ – імовірність знаходження УП у стані z; $P_{iz} = P(\gamma \in G_i/\theta \in F_z)$ умовна імовірність визнати УП за результатами контролю в i-му стані за умови, що він знаходиться в z-му стані; $P_i(z) = P\begin{pmatrix}\theta \in F_z \\ \gamma \in G_i\end{pmatrix}$ – безумовна імовірність відношення УП, яке знаходиться в z-му стані відповідно до i-го.

На рисунку 1 прийняті наступні значення:

$$P_i(z) = P^0(z)P_{zi}. \tag{3}$$

Таким чином, якість контролю z-го стану УП описується імовірністю його находження в даному стані перед контролем і матрицею перехідних імовірностей [6]:

$$\|P_{z1}, P_{z2}, \dots, P_{zi}, \dots, P_{zm}\|. \tag{4}$$

Оскільки все сказане відноситься до контролю будь-якого з можливих станів УП, отримані результати можуть бути застосовані для опису процесу контроля його наступних m–1 станів. В зв'язку з цим, що УП, віднесений за результатами контролю до i-го стану, перед контролем міг знаходитись в будь якому з m можливих станів, то імовірність отримання рішення (УП знаходиться в i-му стані) визначається за формулою:

$$P(G_i) = \sum_{z=1}^{m} P^0(z)\, P_{zi}. \tag{5}$$

Таким чином, процес контролю УП може бути описаний матрицею імовірностей його різнісних станів перед початком контролю і матрицею перехідних імовірностей:

$$\left\| \begin{matrix} P_{11},\ P_{12}, \dots, P_{1j}, \dots, P_{1m} \\ P_{i1},\ P_{i2}, \dots, P_{ij}, \dots, P_{im} \\ P_{m1},\ P_{m2}, \dots, P_{mj}, \dots, P_{mm} \end{matrix} \right\|. \tag{6}$$

Однією з основних характеристик СК є точність. В подальшому під точністю СК будемо розуміти її якість, яка відображає наближення до нуля її помилок, а під помилками СК – відношення результатів контролю від деяких ідеальних показників. Поняття точності

і помилок СК можливо узагальнити, включивши у будь-які відхилення від бажаного результату, у тому числі і вагомі, пов'язані з частковою або повною її відмовою. Мета контролю УП – визначення стану, в якому він знаходиться. Помилка СК в цілому – це подія, котра полягає у відношенні до деякого *i*-го стану УП у дійсності, що знаходиться в *j*-му стані. Очевидно, що матриця перехідних імовірностей ідеального (абсолютно точного) контролю повинна бути одиничною матрицею порядку *m* тобто $P_{zj}(r \neq j) = 0,\ P_{zj}(z = j) = 1$. Оскільки матиця перехідних імовірностей вміщує імовірності усіх можливих при контролі УП переходів, як бажаних та і не бажаних, тоді вона може слугувати показником його точності, при чому елементи матриці $P_{z=j}$ характеризують правильність (точність), а елементи $P_{z\neq j}$ – помилки.

Для побудови математичної моделі формування рішення при контролі якості функціонування РЕО, яка описує залежності вихідних характеристик СК від вхідних і внутрішніх впливів, розглянемо формування рішення при якому, як результат послідовного виконання ряду ЕО, котрі виконують послідовно перетворення УП, і в результаті дій деяких ЕО, наступна операція використовує результат перетворення УП усіма попередніми ЕО.

Позначимо через $\theta^1, \theta^2, \dots, \theta^i, \dots, \theta^N, N$ – результати перетворення УП однією, двома, … *i*, ..., *N* ЕО, виконаних послідовно.

Розглянемо перетворення УП, який знаходиться в стані F_z, рядом послідовно виконаних ЕО контролю. Після виконання $(k-1)$ ЕО перетворень УП θ^{k-1} може знаходитись в будь-якому з *m* можливих станів. Позначимо безумовно імовірність знаходження перетвореного УП в *i*-му стані після завершення $(k-1)$ ЕО через $P_i^{(k-1)}(z)$, при цьому

$$P_i^{(k-1)}(z) = P\begin{pmatrix}\theta^{k-1} \in F_i^{k-1}\\ \theta \in F_z\end{pmatrix}, \tag{7}$$

де F_i^{k-1} – *i*-те з *m* можливих станів перетворення УП після завершення $(k-1)$ ЕО.

Аналогічно для k-ї ЕО маємо:

$$P_i^k(z) = P\begin{pmatrix}\theta^k \in F_i^k\\ \theta \in F_z\end{pmatrix}. \tag{8}$$

Перетворення УП, знаходиться після виконання k-ї ЕО в стані P_j^k на її початку тобто після завершення $(k-1)$ ЕО, може знаходитись в будь-якому з можливих станів. Тоді $P_i^k(z)$ визначається:

$$P_i^k(z) = \sum_{i=1}^{m} P_j^{k-1}(z)\, P_{ij}^k(z), \tag{9}$$

де $P_{ij}^k(z)$ – умовна імовірність переходу перетвореного УП з стану F_j^{k-1} в стан F_j^k при виконанні $(k-1)$ ЕО, тобто

$$P_{ij}^k(z) = P\begin{pmatrix}\theta^k \in F_j^k / F_j^{k-1}\\ \theta \in F_z\end{pmatrix}, \tag{10}$$

k-та ЕО *z*-го стану УП може бути описана рядком безумовних імовірностей станів перед початком їх дій і матрицею перехідних імовірностей:

$$\left\|\begin{matrix}P_{11}^k(z), \dots, P_{1j}^k(z), \dots, P_{1m}^k(z)\\ P_{i1}^k(z), \dots, P_{ij}^k(z), \dots, P_{im}^k(z)\\ P_{m1}^k(z), \dots, P_{mj}^k(z), \dots, P_{mm}^k(z)\end{matrix}\right\|. \tag{11}$$

Матриця перехідних імовірностей (11) – квадратна матриця порядку *m* з невід'ємними елементами, при чому доданок елементів матриці дорівнює одиниці:

$$\sum_{i=1}^{m} P_{ij}^{k}(z) = 1 \qquad . \tag{12}$$

Відповідно до виразу (9), матриця-рядок безумовних імовірностей на виході k-ї ЕО – добуток матриці-рядка безумовних імовірностей на її вході на квадратну матрицю перехідних імовірностей.

Перша ЕО при контролі z-го стану УП повністю описується безумовною імовірністю z-го стану УП $P^0(z)$ та матрицею рядком перехідних імовірностей:

$$\left\| P_{z1}^{1}(z), \dots, P_{zj}^{1}(z), \dots, P_{zm}^{1}(z), \right\|. \tag{13}$$

Безумовні імовірності станів на виході першої ЕО визначаються за формулою:

$$P_j^k(z) = P^0(z) P_{zj}^1(z), j = \overline{1, m}. \tag{14}$$

Послідовне виконання n ЕО можливо замінити однією еквівалентною операцією для котрої матриця перехідних імовірностей є добутком матриць перехідних імовірностей всіх ЕО:

$$P_{ij}^{(k,k+n)}(z) = \sum_{\gamma_1=1}^{m} \sum_{\gamma_2=1}^{m} \dots \sum_{\gamma_n=1}^{m} P_{\gamma}^{k}(z) P_{\gamma_1\gamma_2}^{k+1}(z) \dots P_{\gamma_{n-1}\gamma_2}^{k+n}(z). \tag{15}$$

Таким чином, якщо відома матриця-рядок безумовних імовірностей на початку деякої ЕО і матриця перехідних імовірностей наступних операцій, безумовні імовірності станів УП на виході останньої ЕО визначається за формулою, відповідною (8):

$$P_j^{(k,k+n)}(z) = \sum_{i=1}^{m} P_j^k(z) P_{ij}^{(k,k+n)}(z). \tag{16}$$

Перехідні імовірності $P_j^{k,k+n}(z)$ визначаються за формулою (16).

Безумовні імовірності станів на виході операції контролю визначаються з виразу:

$$P_j(z) = P_j^n(z) = P^0(z) P_{zj}^{(1,\,n)}(z), \tag{17}$$

$$P_{zj}^{(1,\,n)}(z) = \sum_{i=1}^{m} P_{zi}^{1}(z) P_{ij}^{(2,\,n)}(z), \tag{18}$$

де $P_{zi}^{1}(z)$– перехідні імовірності першої ЕО;

$P_{ij}^{(2,\,n)}(z)$ – перехідні імовірності наступних ЕО, які визначають за формулою (15).

Оскільки все сказане відноситься до контролю будь-якого z-го стану УП, отримані результати розповсюджуються на контроль решти $m - 1$ станів УП.

Таким чином, для опису операцій контролю (визначення імовірності станів перетвореного УП на її виході) необхідно знати імовірність станів УП на її виході і перехідні імовірності кожної з ЕО, які складають операцію контролю, для обрахунків котрих необхідно знати характеристики похибок виконання цих операцій.

Для визначення перехідних імовірностей ЕО розглянемо деяку k-ту ЕО при контролі z-го стану УП. Дана операція після перетворення інформації, отриманої після перетворення її попередніми ЕО, при чому дійсне перетворення не відповідає необхідному перетворенню через недосконаліть вибраних методів і засобів контролю, її реалізації, що призводить до виникнення помилок перетворення. Якщо б помилки перетворення були відсутні, дана ЕО призводила до перетворення УП в той стан, в якому вона його сприймала. Тоді матриця перехідних імовірностей представляла собою одиничну матрицю де $P_{ij}^{k} = 1$ при $i = j$ і $P_{ij}^{k} = 0$ при $i \neq j$.

Для реальної ЕО матриця перехідних імовірностей відрізняється тим більше від одиничної, чим більше помилок перетворення (вона характеризує точність ЕО). При дослідженні похибки ЕО, необхідно мати на увазі дві сторони цього питання [7]:

перше, здатність ЕО виконувати необхідне перетворення УП при її ідеальній реалізації засобами контролю;

друге, втрати або викривлення інформації пов'язане з похибкою засобів, реалізованих ЕО.

Першій відповідає методична помилка, друга характеризує інструментальну помилку ЕО.

Для визначення впливу методичної та інструментальної складових помилок перетворення ЕО на її перехідні імовірності розглянемо k-ту ЕО при контролі z-го стану УП відповідно до формули (8):

$$P_{ij12}^{(k,\,k+1)}(z) = \sum_{\gamma=1}^{m} P_{i\gamma1}^{k}(z) P_{\gamma j2}^{(k+1)}(z), \qquad (19)$$

де $P_{ij12}^{(k,\,k+1)}$ – умовна імовірність переходу перетворення УП з i-го стану в j-те при послідовній дії двох помилок перетворення;

$P_{i\gamma1}^{k}(z)$, $P_{i\gamma2}^{(k+1)}(z)$ – умовна імовірність переходу перетвореного УП з i-го стану в j-те при дії першої (другої) в даній послідовності дії з двох помилок перетворення.

При підстановці у формулу (19) замість індексів 1 та 2 відповідно індекси M (методична складова похибки перетворення) або І (інструментальна складова) похибки перетворення залежно від послідовності їх дії, визначаються умови імовірності переходу перетвореного УП з i-го стану в j-те при сумісній дії методичних та інструментальних складових похибки перетворення ЕО. Оскільки все сказане відноситься до контролю z-го стану УП, отримані результати розповсюджуються на контроль решти $m - 1$ станів УП.

Висновки

Розглянута математична модель формування рішення при контролі РЕО дозволяє при відомих характеристиках УП об'єкта і засобів, реалізованих ЕО контролю, визначити імовірність станів перетвореного УП на виході останньої ЕО при контролі будь-якого з можливих станів об'єкта контролю і тим самим оцінити ступінь пристосованості операції контролю до виконання поставленої задачі або її ефективність. Модель дозволяє також оцінити вплив окремо взятої ЕО на результат контролю і раціональним чином вибрати її характеристики.

Подальші дослідження слід проводити у напрямку створення ефективних математичних та імітаційних моделей, які нададуть змогу достатньо швидко та точно визначати функціональний стан об'єкта контролю та якості його контролю з функціональними модулями різного типу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кузавков В. Технічна діагностика складних технічних об'єктів / В. Кузавков, В. Хорошко, О. Янковський // Захист інформації, Т. 24, № 3, 2022. С. 115–120.

2. Креденцер Б.П. Оценка эксплуатационно-технических характеристик объектов телекоммуникаций при априорной неопределенности / Б. П. Креденцер, А. И. Миночкин, Д. И. Могилевич. К.: Феникс, 2012. 335 с.

3. Креденцер Б.П. Оцінка надійності резервованих систем при обмеженій вихідній інформації / Б.П. Креденцер, В.В. Вишнівський, М.К. Жердєв та інші. К.: Фенікс, 2013. 334 с.

4. Geff I. Disz M. Unified approach to the study of self-checking systems – Digital Proc., 2007, v5, #6, p. 289–307.

5. Ashjaee M., Reddy S. On totally self-checking checkers for separable codes. – IEEE Trans. Comput., 2009, v.C-27, #7, p. 736–745.

6. Барковський В. В. Теорія імовірностей та математична статистика. 5-те вид. / В. В. Барковський, Н. В. Барковська, О. К. Лопатін. Київ: Центр учбової літератури, 2010. 424 с.

7. Белоконь Р. Н. Исследование влияния методических и инструментальных составляющих ошибки контроля определяющих параметров изделия на показатели достоверности контроля качества изделия / Р. Н. Белоконь // Современные методы оценки качества продукции. К.: Знания, 1994. С. 22–24.

8. Міночкін А. І. Перспективи створення та розвитку систем діагностування радіоелектронних засобів із вбудованим програмним забезпеченням / А. І. Міночкін, В. В. Кузавков, С. О. Клімович // Системи і технології зв’язку, інформатизації та кібербезпеки. Київ: ВІТІ. 2024. № 5. С. 78–86.

9. Кузавков В. В. Обґрунтування вибору показників оцінки ефективності функціонування автоматизованої системи контролю / В. В. Кузавков, О. Г. Янковський, Ю. В. Болотюк // Сучасні інформаційні технології у сфері безпеки та оборони. Київ. 2022. Том 2 (44). С. 21–27.

10. Вишнівський В. В. Особливості використання фізичного діагностування при побудові інтелектуальної системи діагностики радіоелектронної техніки / В. В. Вишнівський, С. І. Глухов, К. П. Сторчак // Зв’язок. 2019. № 1. С. 8–13.

11. Жердєв М. К. Методика обробки діагностичної інформації для автоматизованої системи технічного діагностування радіоелектронної техніки / М. К. Жердєв, С. І. Глухов, М. М. Нікіфоров // Розвиток радіотехнічного забезпечення, АСУ та зв’язку Повітряних Сил 2019. С. 70–78.

12. Рижов Є. В. Оцінка впливу діагностичного забезпечення на надійність радіоелектронних систем / Є. В. Рижов, Л. М. Сакович, С. І. Глухов, Ю. А. Настишин // Військово-технічний збірник, 2021 (24), С. 3–8.

DOI: 10.58254/viti.6.2024.21.250

УДК 004.056.5

д-р техн. наук, ст. наук. співр. Чевардін В. Є. ORCID:0000-0002-1070-4568 (ВІТІ ім. Героїв Крут)

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ РІШЕННЯ ЩОДО ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

В роботі розглянуті основні підходи до побудови архітектури відкритих ключів PKI з розділенням на базову, дворівневу та багаторівневу ієрархії. Розглянуті сучасні способи атак на існуючі інфраструктури відкритих ключів, протоколи побудови захищених з'єднань як провідних так і безпровідних систем.

Визначені основні класи атак на інфраструктури PKI, з яких основна увага приділена найбільш небезпечному класу атак – людина посередині (MITM-атакам). В роботі наведено моделі різних класів MITM-атак, їх деталі та існуючі способи зменшення ризиків їх реалізації.

Також наведені існуючі приклади успішних атак на компанії та різні організації, які реалізовували моделі MITM-атак на прикладному, мережевому та фізичному рівні моделі міжмережної взаємодії. Для інфраструктури PKI одним з варіантів наводиться її сегментування, що дозволяє зменшувати масштаби впливу атаки на центр сертифікації ключів.

Також у роботі наведено альтернативний спосіб захисту від MITM-атак з використанням технології розподіленого мікрореєстра (DLT) для створення децентралізованих систем розповсюдження криптографічних ключів (DKMS). Рішення базується на використанні мікрореєстрів (distributed micro ledger technology – DMLT). Застосування DMLT для створення DKMS дозволяє забезпечити захист від більшості класів MITM-атак.

Ключові слова: *інфраструктура відкритих ключів, протоколи захисту інформації, уразливості протоколів, атаки MITM.*

V. Chevardin Organizational and technical solutions for the construction of protected information and communication systems.

The paper presents the main approaches to the construction of the PKI public key architecture divided into basic, two-level, and multi-level hierarchies. Modern methods of attacks on existing public key infrastructures, protocols for building secure connections of both wired and wireless systems are considered.

The basics of the class of attacks on PKI infrastructures are defined, of which the main attention is paid to the most dangerous class of attacks – man-in-the-middle (MITM-attacks). The paper provides models of various classes of MITM attacks, their details and existing methods of reducing the risks of their implementation. Existing examples of successful attacks on enterprises and various organizations that implemented MITM attack models at the application, network, and physical levels of the network interaction model are also given.

For the PKI infrastructure, one of the options is its segmentation, which allows to reduce the scope of attacks on the key certification center. The paper also provides an alternative way to protect against MITM attacks using distributed micro ledger technology (DLT) to create a decentralized cryptographic key distribution system (DKMS). The solution is based on the use of micro ledgers (distributed ledger technology – DMLT). Using DMLT to create a DKMS allows protection against additional classes of MITM attacks.

Keywords: *public key infrastructure, information protection protocols, protocol vulnerabilities, MITM attacks.*

Актуальність досліджень. Аналіз існуючого стану застосування систем кібербезпеки та захисту інформації, що використовуються в інформаційних системах спеціального призначення, показав гостру потребу в підвищенні ефективності процесів аналізу уразливостей існуючих систем захисту інформації та прийняття відповідних рішень щодо їх усунення урядовими та регіональними командами реагування на кіберзагрози. Брак фінансування, матеріального та інформаційного забезпечення військ, сил, викликало потребу в розробці нових наукових засад та підходів щодо підвищення кіберготовності та кіберзахищеності інформаційно-комунікаційних систем держави. В зв'язку з цим, створення стійких до кібервпливів інфраструктурних рішень щодо побудови інформаційно-комунікаційних систем є єдиним способом забезпечення кібербезпеки та структурної надійності інформаційно-комунікаційних систем об'єктів критичної інфраструктури держави. Це можливо зробити шляхом побудови інформаційного середовища для отримання розвідувальної інформації, передачі інформації для управління системами озброєння та військової техніки, а також для проведення інформаційно-психологічних та кібероперацій.

Основою таких систем є єдина платформа формування захищених комунікаційних зв’язків з надійною інфраструктурою відкритих криптографічних ключів, генерації ключових послідовностей, шифрування та розшифрування даних, забезпечення функцій автентифікації суб’єктів та об’єктів доступу, моніторингу процесів у системі з обов'язковим резервуванням критичних елементів та даних.

Результати аналізу хибних підключень громадян України до мережі Інтернет та порушення доступності ресурсів Інтернет дозволили визначити найбільш розповсюджену загрозу, відому як атака "men in the middle". MITM-атака реалізується різними способами, а саме створенням хибних базових станцій мобільного зв’язку, хибних центрів розподілу криптографічних ключів, хибних dns-серверів, arp-серверів та іншими способами [1–4]. Для існуючих підходів з централізованим розподілом криптографічних ключів, таких як інфраструктура відкритих ключів PKI, цей клас атак створює загрозу перехоплення відкритих ключів та їх підміни або блокування між головним сервером та будь-яким клієнтом, що робить уразливим практично всі організаційно-технічні структури, що використовують PKI. В зв’язку з чим, виникла потреба в пошуку альтернативних підходів до побудови схем генерації та розповсюдження криптографічних ключів з підвищеною захищеністю до MITM-атак.

Метою даної роботи є розробка нового підходу до побудови інфраструктури відкритих криптографічних ключів зі зменшенням ризику втрати конфіденційності, цілісності та доступності ресурсів інформаційно-комунікаційної системи в умовах диверсифікації MITM-атак.

1. Викладення матеріалу

Розглянемо основні елементи інфраструктури PKI, які забезпечують функції електронного цифрового підпису та автентифікації для інформаційно-комунікаційних мереж та систем.

Цифрові сертифікати – це цифрові файли, які забезпечують можливість ідентифікації (організації, особи, служби або програмного коду) та автентичності відкритих ключів шифрування та цифрового підпису. Цифрові сертифікати поділяються на типи:

сертифікати SSL/TLS для перевірки домену (DV), перевірки організації (OV), розширеної перевірки (EV);

сертифікати підпису коду;

сертифікати підпису документів;

сертифікати підпису електронної пошти (S/MIME);

сертифікати автентифікації клієнтів.

Ключові пари – це криптографічні елементи шифрування/розшифрування даних, підпису/верифікації даних, які складаються з публічного (відкритого) та особистого (секретного) ключів.

Органи сертифікації – це, як правило, центр сертифікації (ЦС), яких може бути для однієї організації один або декілька. Залежно від розміру організації та ієрархічної структури ЦС можуть поділятися на: кореневий ЦС, проміжний ЦС та ЦС видачі (може також бути одночасно і проміжним).

За архітектурною особливістю PKI може поділятися на загальнодоступну PKI (Public CA) та приватну (Private CA).

Загальнодоступна PKI використовується для забезпечення захисту браузерів, месенджерів, програмного коду, електронної пошти та інших інформаційних систем загального призначення, як правило, з використанням протоколу SSL/TLS.

Приватна PKI використовується для забезпечення захисту для внутрішніх мереж, доступу користувачів до ресурсів інформаційних систем, використання приватних та внутрішніх Wi-Fi мереж організації, мобільних пристроїв користувачів. Для цього, як правило, використовують приватні PKI, кореневі сертифікати яких встановлюються на кожному

пристрої. Однією з загроз для такого варіанта розгортання PKI є компрометація секретних ключів кореневого сертифікату, що створює загрозу всій інфраструктурі організації і потребує відкликання всіх сертифікатів, підписаних з використанням цифрового підпису кореневого центру сертифікації. Для зниження ризиків втрати конфіденційності інформації, що циркулює в організації, здійснюють розділення PKI інфраструктури на сегменти. Розглянемо варіанти.

Базова однорівнева архітектура PKI наведена на рисунку 1, яка побудована на використанні Кореневого Центру Сертифікації (КЦС), який забезпечує функції захисту для всіх користувачів організації.

Рис. 1. Базова однорівнева архітектура PKI

Базова дворівнева архітектура PKI наведена на рисунку 2.

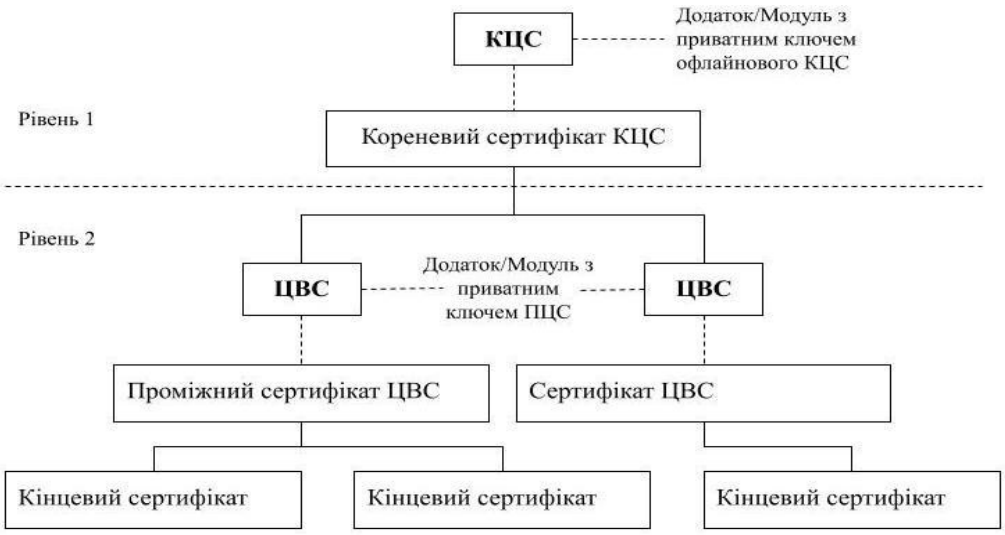


Рис. 2. Базова дворівнева архітектура PKI

Базова дворівнева архітектура PKI побудована на використанні офлайнового (недоступного всім користувачам через мережу Інтернет) Кореневого Центру Сертифікації (КЦС), який підписує сертифікати відкритих ключів центрів видачі сертифікатів (ЦВС). Генерацію цифрового підпису на рівні 2 здійснюють ЦВС, які забезпечують функції захисту для всіх користувачів організації. Між собою ЦВС зв'язуються через мережу Інтернет.

Базова трирівнева архітектура PKI побудована на використанні офлайнового КЦС, який підписує сертифікати проміжних центрів сертифікації (ПЦС) на рівні 2 (без використання мережі Інтернет). Генерацію цифрового підпису та підпис сертифікатів для всіх ЦВС на рівні 3 здійснюють ПЦС. Між собою ПЦС зв'язуються через мережу Інтернет. Для всіх ЦВС (3-й рівень) сертифікати підписують з секретними ключами ПЦС. ЦВС видають сертифікати кінцевим користувачам. Використання трирівневої архітектури дозволяє зробити окремі

сегменти сертифікації користувачів в організації. Це знижує ризик блокування або компрометації конфіденційної інформації користувачів у випадку компрометації секретного ключа одного з ПЦС або ЦВС. У разі компрометації секретного ключа ЦВС під загрозу компрометації ключів користувачів підпадає лише один сегмент мережі організації (рис. 3), що є перевагою над базовою однорівневою архітектурою, з одного боку. З іншого боку, трирівнева або багаторівнева архітектура вимагає збільшення витрат на підтримку та забезпечення роботи ПЦС, ЦВС та захист каналів обміну сертифікатами між ними.

Базова трирівнева архітектура PKI наведена на рисунку 3.

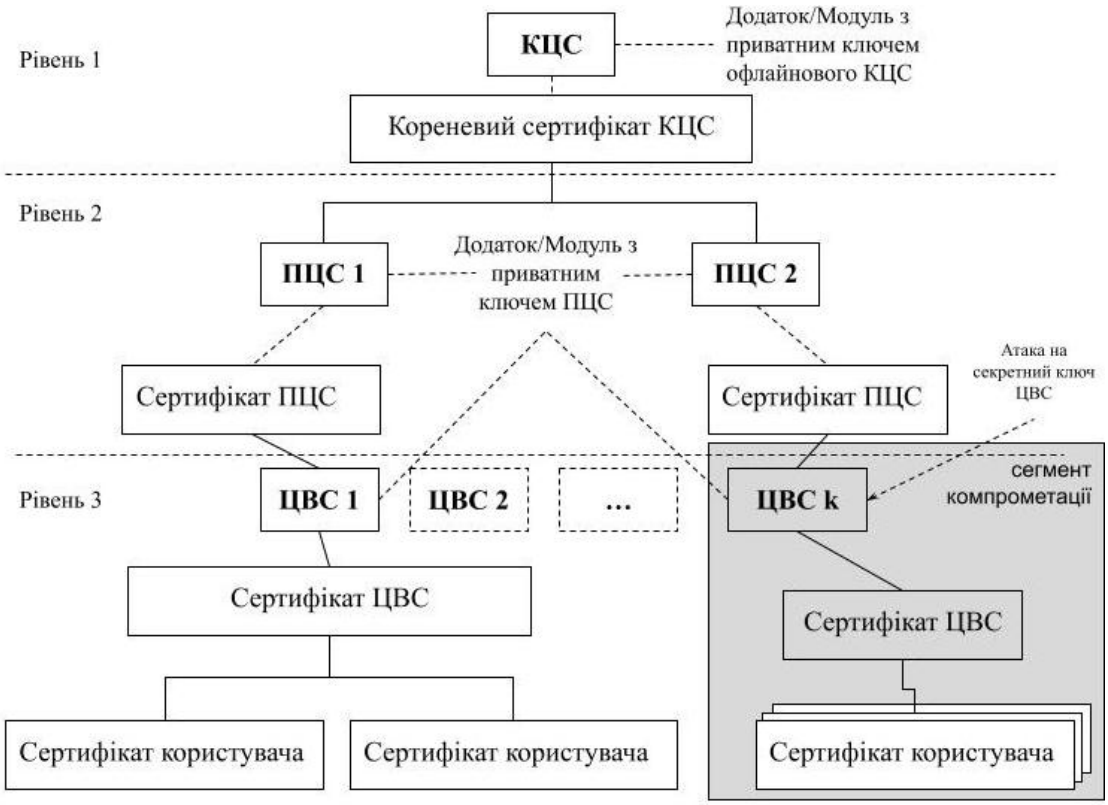


Рис. 3. Базова трирівнева архітектура PKI

Основним етапом атак на інфраструктури PKI сьогодні є захоплення контролю кореневих сертифікатів організацій та окремих користувачів, що надає зловмиснику можливість відкликання, блокування, створення нових сертифікатів користувачів. Розглянемо більш детально етапи сучасних атак на елементи та протоколи захисту інформації та інфраструктури PKI.

Класи атак на PKI

Клас атак на відмову в обслуговуванні (Dos атаки) (порушення доступності):

атаки на центр сертифікації (CA DoS) спрямовані на перевантаження ЦС запитами або запуск DDoS атак, що порушує видачу та перевірку сертифікатів;

атаки на відповідача протоколу статусу онлайн-сертифіката (OCSP DoS), спрямовані на перевантаження ЦС запитами протоколу OCSP, що блокує можливість перевірки користувачами дійсність сертифікатів.

Клас атак на основі фішингу та соціальної інженерії.

Атаки на основі використання методів та технік соціальної інженерії та фішингових розсилань пошти з шкідливим вкладенням, прикладом такої атаки є атака на домен live.com, яка була здійснена шляхом надсилання електронного листа на легальну адресу, включену до

дозволених адрес відповідно вимог CA/Browser Forum Baseline Requirements. Зловмисник зміг зареєструвати ту ж саму адресу, що дозволило йому схвалити використання домену.

Клас атак на секретний ключ користувача (порушення конфіденційності):

атаки на основі викрадення секретних ключів (Private Key Theft). Цей клас атак оснований на різних техніках, спрямованих на викрадення секретних ключів власників сертифікатів, що надає змогу зловмиснику видавати себе за легального користувача захищеної системи та здійснювати подальші шкідливі дії від його імені;

атаки на основі використання зловмисного програмного засобу (Keylogging) для захоплення інформаційних потоків від засобів введення інформації на ПЕОМ користувачів. Ці атаки дають можливість реалізувати сценарій MITM-атаки зі створенням хибного ключа легального користувача або викраденням ключа легального користувача.

Клас атак з використання компрометації центру сертифікації (порушення конфіденційності), які реалізують модель MITM-атаки:

атаки на основі створення фальшивих сертифікатів центру сертифікації, який був зламаний або мав критичну уразливість, яка дає можливість його експлуатації. Прикладом реалізації цієї атаки є використання утиліти Certipy, розробленої Олівером Ляком, для експлуатації уразливості сертифікатів Active Directory (AD CS), яка знаходить уразливі шаблони сертифікатів та надає зібрані дані у форматі BloodHound та json, а саме: CA Name, DNS Name, Certificate Subject, Certificate Validity Start & End, Access Rights & Permissions, Vulnerable Certificate Name, Vulnerabilities. У разі успішної атаки отримують геш NTLM адміністраторів, який можна використовувати для автентифікації та компрометації контролера домену;

атаки на основі створення фальшивого ЦВС для видачі підроблених сертифікатів. Прикладом цієї атаки вважається випадок з компанією Lenovo. До переліку довірених центрів сертифікації Lenovo було включено центр сертифікації Superfish CA. Виявлена уразливість програмно-апаратних засобів мала місце у користувачів, які користуються застарілими програмно-апаратними засобами та браузерами Firefox. Для захисту від такої уразливості в програмі Windows Defender є оновлення, яке видаляє додаток Superfish. Слід зазначити, що сертифікат для Superfish CA, підписаний компанією Komodia, не виключає наявність уразливостей в інших додатках з сертифікатами, підписаними компанією Komodia, таких як My Family Secure, Kurupira Webfilter.

Клас атак з відкликанням сертифікатів (порушення цілісності), які реалізують модель MITM-атаки:

атаки на основі маніпуляцій зі списками відкликаних сертифікатів (CRL) здійснюються з метою запобігання виявлення користувачами відкликаних сертифікатів. Це призводить до використання клієнтами скомпрометованих або тих, що втратили чинність сертифікатів відкритих ключів. В разі чого зловмисник може скористатися уразливими або скомпрометованими ключами клієнтів та отримати доступ до інформації або послуг цифрового підпису клієнта жертви;

атаки на основі маніпуляції відповідача протоколу статусу онлайн-сертифіката (OCSP) з метою надання хибної інформації щодо статусу сертифіката. В разі чого зловмисник може маніпулювати статусом сертифікатів та примушувати клієнтів використовувати свої сертифікати, внаслідок чого також отримати доступ до інформації або послуг цифрового підпису клієнта жертви.

Nicolas Serrano, Hilda Hadan, L. Jean Camp [7] провели аналіз інцидентів, пов'язаних з роботою центрів сертифікації відкритих ключів з великою кількістю сертифікатів, а саме Let's Encrypt – 92,300,644, Sectigo – 27,859,495 DigiCert – 12,577,372, GoDaddy – 2,476,593, GlobalSign – 680,249 Amazon – 644,901 та інших. Найбільша кількість інцидентів, пов'язаних з ЦВС, прийшлася на DigiCert, Comodo, Symantec, WoSign, Camerfirma. Однією з основних

причин інцидентів стали невідповідність полів сертифікатів вимогам базового рівня безпеки, що склали 38.52 %, невідповідність базовому рівню безпеки відповідачів проколу статусу сертифікатів OCSP та списку відкликаних сертифікатів (CRL), які склали 10.29 %, атаки на основі видачі фальшивих сертифікатів склали 4.75 %, атаки на основі зниження рівня безпеки, а саме використання 512/1024 біт ключа протоколу RSA (4.75 %), використання алгоритму SHA-1/MD5 (3.96 %).

Клас атак на основі вразливостей криптографічних протоколів, які реалізують модель MITM-атаки:

атаки на основі використання слабких криптографічних ключів. Цей клас атак використовує нестійкі параметри криптографічних систем. Прикладом експлуатації уразливостей протоколів асиметричної криптографії є факторизація експортованих RSA-ключів (FREAK), шляхом деградації стійких RSA-ключів до нестійких (export grade RSA) з послідовним зламом. Прикладом експлуатації вразливостей геш-функцій є пошук колізій та атак на алгоритм SHA-1. Прикладом експлуатації уразливостей алгоритмів потокового шифрування є атаки на симетричні криптоалгоритми RC4 та схеми генерації спільного секрету DHE. Сьогодні можна знайти багато сайтів, які працюють на сертифікатах, отриманих до 2015 року, або дозволяють використовувати сертифікати, що створені з використанням SHA-1, або 512 бітових RSA-ключів;

атаки на основі використання застарілих протоколів криптографічного захисту інформації. Прикладом такої атаки став випадок коли зловмисник зміг узгодити в протоколі використання застарілої версії TLS протоколу (уразливість CVE-2014-3511). Цей тип атак розповсюджений за причиною частого використання організаціями застарілого обладнання.

Клас атак з використанням нового ключа користувача, які реалізують модель MITM-атаки. Одним з прикладів таких атак є порушення цілісності протоколу handshake, під час якої зловмисник імітує нового користувача інформаційної системи та намагається діяти від його імені для отримання конфіденційної інформації від справжніх користувачів мережі. Як правило, виділяють три типи атак цього класу:

атаки на основі викрадення сесій. Цей клас атак дають можливість зловмисникам перехоплювати та маніпулювати зв'язками між двома користувачами, надаючи фальшивий сертифікат з метою подальшого прослуховування або зміни даних;

атаки на основі підробки сертифікатів. Цей клас атак оснований на використанні нових шахрайських сертифікатів з метою представлення зловмисника легальним сервером чи службою, що надають послуги ЕЦП, використання яких жертвою призводить до втрати конфіденційності інформації, що передається захищеними каналами. Прикладом такої атаки став випадок Gogo Found Spoofing Google SSL Certificates, який був виявлений у компанії Gogo, яка надавала послуги служби захисту Інтернет з'єднань Gogo Inflight Internet. Ця служба використовувала сертифікати SSL MITM для контролю під'єднання користувачів для відвідування сайтів Google та ресурсів YouTube. В результаті цих дій компанія Gogo мала потенційні можливості для отримання даних клієнтів Інтернет послугами. Використання попереджень від служби безпеки браузерів, які викликають підозру відповідно до політики безпеки Gogo Inflight Internet, можуть блокувати та знищувати законні SSL сертифікати та послаблювати моделі довіри браузерів користувачів.

Таким чином, кожен з розглянутих типів атак на інфраструктуру PKI може представляти більшу чи меншу загрозу для організації, що залежить від типу архітектури PKI, реалізованої в організації. Але найбільшу загрозу складають класи MITM-атак та атак на основі ураливостей криптографічних протоколів. Результати проведеного огляду показали найбільшу кількість атак, пов'язану з наступними причинами: закладні програмні засоби (Software bugs) – 24 %, невідповідність вимогам або неправильна інтерпретація (Believed to be compliant, Misinterpretation, Unaware) – 18 %, бізнес процеси, уразливості конфігурації центрів

видачі сертифікатів та тестування (Business model, CA decision, Testing) – 13 %, людські помилки (Human error) – 9 %, решта причин склали менше 8 %.

В зв'язку з цим, для визначення шляхів підвищення захищеності та надійності PKI, треба дослідити варіанти реалізації MITM-атак та існуючі уразливості криптографічних протоколів.

Способи реалізації атак класу MITM

Спосіб реалізації MITM-атаки 1

Розглянемо варіант 1 проведення MITM-атаки на користувачів Інтернет, які працюють за стандартними протоколами міжмережної взаємодії. Під час встановлення з'єднання між користувачами та сервером зловмисник виступає посередником для обох сторін. Як правило, метою зловмисника є підміна кореневого сертифікату відкритого ключа серверу на хибний відкритий ключ з метою подальшого прослуховування трафіку або нав'язування хибної інформації. Варіант цієї атаки наведено на рис. 4. шляхом порівняння етапів роботи протоколу Handshake та варіанта етапів роботи протоколу Handshake з втручанням зловмисника на етапі створення сесійних ключів користувача.

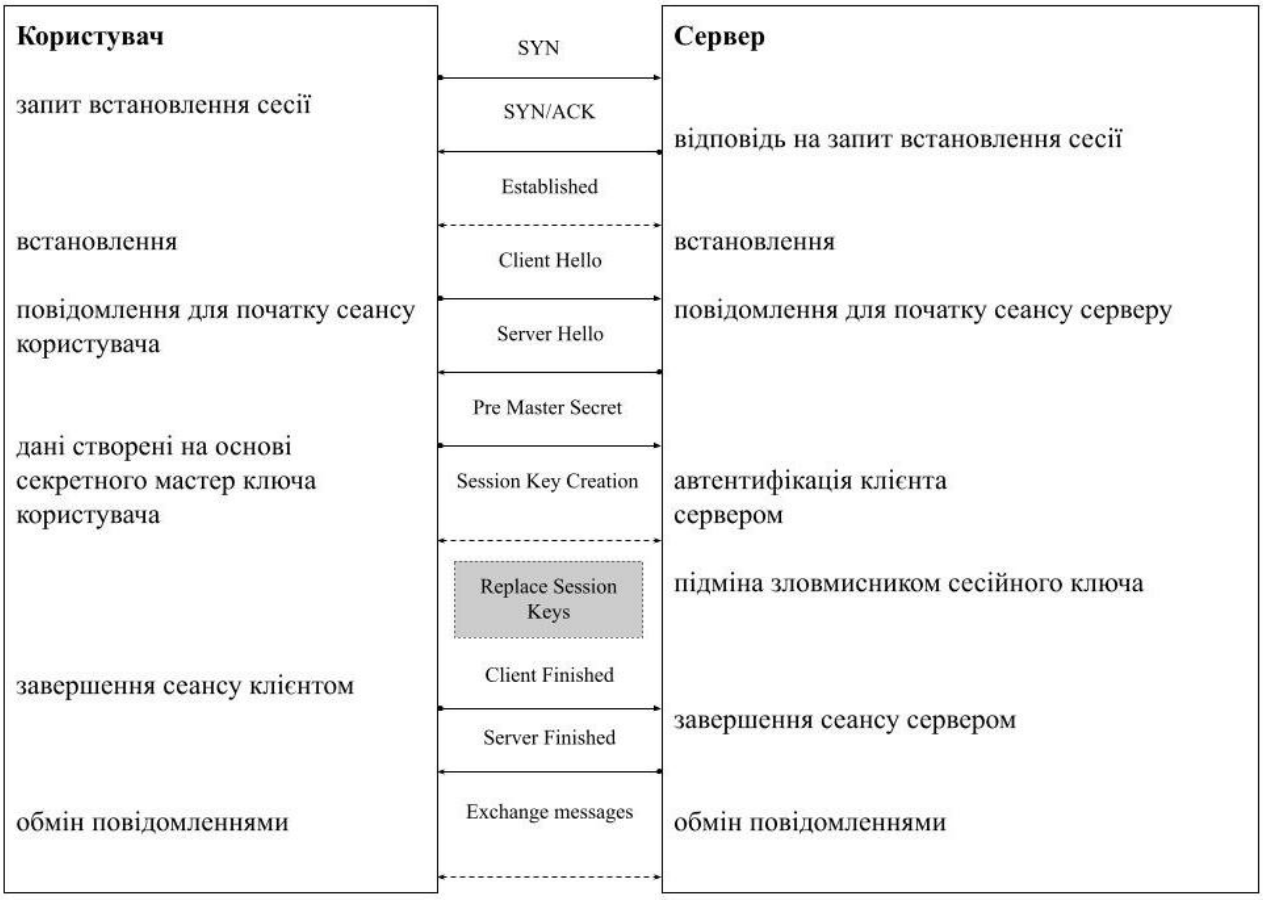


Рис. 4. Модель MITM-атаки на протокол SSL Handshake
порівняно з кроками класичного протоколу SSL Handshake

З рисунка 4 можна побачити місце, з якого зловмисник впливає на процедуру Handshake. На етапі створення сесійного ключа, під час автентифікації клієнта сервером, зловмисник надає свою інформацію для отримання сесійного ключа від серверу. Для справжнього клієнта зловмисник надає інший ключ згенерований власноруч. Після підміни сесійних ключів зловмисник становиться ретранслятором всього трафіку від серверу і до серверу для клієнта жертви.

Спосіб реалізації MITM-атаки 2

Атака на основі вразливості протоколів WPA2 або WPA3 (Wifi-Eavesdropping), яка реалізується прослуховуванням сесій (встановлення з’єднань) в Wi-Fi мережі. Для реалізації цього варіанта MITM-атаки використовують користувачів, що підключаються, як правило, до публічних мереж та мають обладнання бездротового доступу з дозволом переспрямування ICMP трафіку (рис. 5). За таким сценарієм зловмисник може визначати IP-адресу, відкриті UDP-порти користувача (жертви) та серверу, з яким він намагається зв’язатися. Зловмисник може надсилати підроблені пакети, використовуючи вихідну IP-адресу точки доступу.

Прикладом такої атаки є використання вразливості CVE-2022-25667, яка використовує іншу вразливість, пов’язану з уразливостями схем та протоколів автентифікації CWE-287. Приклад класу уразливостей CWE-287: CVE-2021-35033 – уразливість програмного забезпечення маршрутизатора Wi-Fi, яке використовує жорстко закодований пароль для оболонки BusyBox, що дозволяє обходити автентифікацію через порт UART; CVE-2021-35395 – уразливість програмного забезпечення в модулях SFK, реалізоване за рахунок переповнення буфера на основі стека мікросхеми Wi-Fi модуля, що використовується для IoT пристроїв та інші.

Рис. 5. Атака на основі прослуховування бездротової Wi-Fi мережі (Wifi-Eavesdropping)

За узагальненими даними від www.cve.details, www.mitre.org, www.cve.org уразливість CVE-2022-25667, знайдена в 89 % найбільш розповсюджених Wi-Fi маршрутизаторах. Ця уразливість дозволяла здійснити MITM-атаку на протоколи бездротового доступу з використанням Wi-Fi модулів.

Спосіб реалізації MITM-атаки 3

Атака на основі вразливості протоколів WPA2 або WPA3, яка реалізується шляхом викрадення сесії (встановлення з'єднань) в Wi-Fi мережі (Session Hijacking). Для реалізації цього варіанта MITM-атаки зловмисник перехоплює сесію легального користувача, використовуючи два сценарії викрадення сесій: захоплення сесії (Session Side Jacking) та Cross-Site Scripting (XSS).

Спосіб реалізації MITM-атаки 4

Атака на основі вразливості протоколу HTTPS (HTTPS Spoofing), яка також називається омографічна атака. Цей тип атаки будується на підміні справжньої адреси сайту на хибну, шляхом використання певних символів коду, наприклад, ASCII. Як правило, звичайний користувач не відрізняє хибну адресу від справжньої.

Спосіб реалізації MITM-атаки 5

Цей клас атак основний на уразливості програмного забезпечення OpenSSL, яке є базовою програмною платформою побудови протоколів захисту інформації для багатьох протоколів та сервісів: OpenVpn, SSL, TLS та операційних систем: Windows, Linux, IoS. Прикладом, цього варіанта MITM атаки є експлуатація уразливості CVE-2015-1793, а саме знаходження для бібліотеки програмних функцій OpenSSL версій 1.0.2b, 1.0.2c, 1.0.1n і 1.0.1o можливості використання альтернативного ланцюжка сертифікатів, який містить сертифікати зі слабкими ключами, які мають прапорець CA flag з позначкою "issue", що призводить до появи уразливості в усіх програмах, що використовують сертифікати SSL, TLS і DTLS. В такому випадку зловмисник стає довіреною стороною, як звичайний центр сертифікації ЦВС, що видав недійсні загальнодоступні сертифікати SSL/TLS для будь-якого домену в мережі Інтернет.

Спосіб реалізації MITM-атаки 6

Цей клас атак основний на примусовому пониженні версії протоколу MITM TLS та маніпулювання ARP-таблицями. Це досягається в декілька кроків:

крок 1 – визначення MAC адреси машини жертви, де Користувач А запитує кожен пристрій у мережі, запитуючи: «Хто використовує цю адресу IP_B?» Користувач В генерує відповідь користувачу А, "IP_B використовує MAC-адресу MAC_B". Користувач А отримує відповідь і оновлює свій ARP-кеш для створення пари IP_B та MAC_B. Користувач А тепер використовує MAC_B для надсилання даних користувачу В.

Враховуючи, що кешовані ARP-таблиці оновлюються за відповіддю навіть без запиту, без автентифікації повідомлень або перевірки цілісності, це дає можливість зловмиснику підробити інформацію в даній відповіді для перехоплення сеансу та маніпулювання ARP-таблицями.

Крок 2 – маніпулювання таблицями кешу ARP-пристрою, де Користувач С (зловмисник) надсилає відповідь користувачу А, наступного змісту: "IP_B використовується MAC-адресою MAC_C". Щоразу, коли Користувач А бажає зв'язатися з користувачем В, він надсилає дані через користувача С. Користувач С надсилає відповідь користувачу В, з наступним змістом: "IP_A використовується MAC-адресою MAC_C". Щоразу, коли користувач В бажає зв'язатися з користувачем А, він надсилатиме дані через користувача С.

Тепер користувач С отримує всі пакети, надіслані між користувачами А і В (наприклад, між АРМ клієнта і маршрутизатором). Користувач С може увімкнути переадресацію IP для перенаправлення всього отриманого трафіку на відповідний пристрій для перехоплення, зміни або скидання отриманих пакетів. Це використовується для зловживання функцією браузерів для узгодження попередніх версії SSL/TLS. Атака MITM завершена.

Спосіб реалізації MITM-атаки 7

Цей тип MITM-атак заснований на зниженні версії протоколу TLS під час встановлення з'єднання за протоколом рукостискання, який вже розглядався раніше. Для цієї атаки

використовується сценарій з примусовим зниженням версії протоколу TLS, що призводить до появи уразливості в самому протоколі старої версії.

Протокол рукостискання, це відомий, що починається з “ClientHello”, де користувач А (клієнт) надсилає користувачу В (серверу) версію SSL або TLS. У застарілих версіях SSL (версія 2) цей пакет рукостискання можна було перехопити та змінити, але для версії SSLv3 це вже неможливо сьогодні. Сучасні браузери підтримують SSLv3 до TLSv1.2, але використовуватимуть найвищу версію, яку підтримує сервер. Користувач С (зловмисник) не може безпосередньо змінювати будь-які пакети, надіслані під час рукостискання, але може перехоплювати та скидати певні пакети, змусивши браузер вважати, що користувачу В (сервер) не підтримує певну версію SSL/TLS, внаслідок чого знизити узгоджену версію.

Приклад.

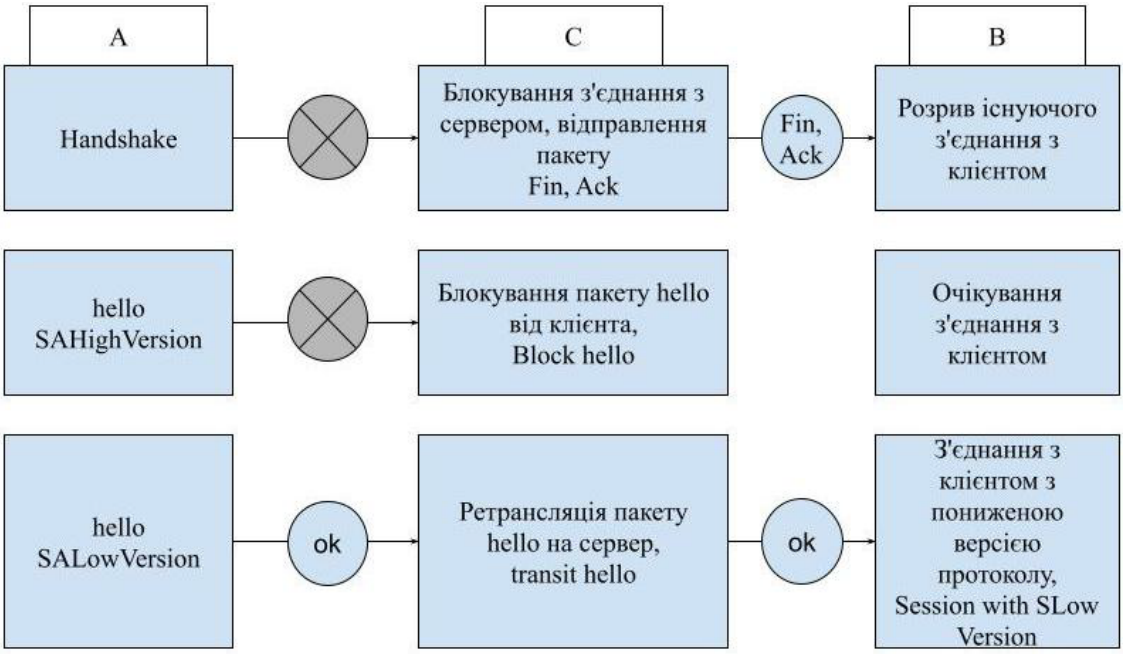


Рис. 6. Схема MITM-атаки заснована на зниженні версії протоколу TLS під час встановлення з’єднання за протоколом рукостискання

Користувач А надсилає «ClientHello» на сервер.

Користувач С перехоплює та скидає пакет (у разі встановлення нової сесії).

Користувач С відкидає поточний пакет рукостискання.

Користувач С надсилає TCP-пакет «FIN, ACK» користувачу В, що припиняє діюче підключення.

В результаті Користувач А повторно намагається підключитися, надсилаючи ”ClientHello” з однією з попередніх версій SSL/TLS. Атака MITM завершена.

Атаки з пониженням версії протоколу базуються на припущенні, що помилка або припинення з’єднання означає збій з’єднання через збій протоколу SSL/TLS. Крім того, для забезпечення сумісності з попередніми версіями SSL/TLS Користувач А може спробувати створити кілька з’єднань, доки не буде встановлено успішне з’єднання.

Таким чином, Користувач С, повторюючи зниження версії протоколу, може переконати Користувача А узгодити SSLv3 із Користувачем В. Ця атака на пониження версії протоколу була перевірена під час підключення до Facebook за допомогою останніх версій Firefox, Chrome і Opera.

Іншим прикладом MITM-атаки є експлуатація уразливості Oracle з операційною системою Ubuntu 14.04 (CVE-2016-2107), для усунення якої було запропоновано Fix OpenSSL Padding Oracle vulnerability (CVE-2016-2107) – Ubuntu 14.04. Деталі цієї атаки та рекомендації щодо захисту описані в [8, 9].

Сценарії захисту від MITM-атак

Способами зменшення шкоди від реалізації MITM-атаки є розділення мережі на зони зберігання та використання відповідних пар ключів, що зменшує кількість клієнтів, які можуть стати жертвами атак нав'язування або порушення конфіденційності даних. Це удосконалення описаної системи за рахунок створення альтернативної інфраструктури відкритих ключів зі зменшенням ефекту розповсюдження зони дії атаки за рахунок сегментації інфраструктури. Розглянемо варіант побудови інфраструктури PKI з урахуванням особливостей розглянутих класів MITM-атак.

Сценарій 1

Одним із перших рішень було використання HTTP Public. Закріплення ключа (HTTP Public Key Pinning-HPKP) або закріплення сертифіката. За допомогою цього механізму вебхост буде надсилати один або більше криптографічних ідентифікаторів (відкритий ключ або сертифікат) для агента користувача (веббраузер) у HTTP-заголовку. Наприклад, це може бути відкритим ключем сертифіката домену або відкритим ключем у його ланцюжку довіри). Агент користувача зберігає ідентифікатор на деякий час, перевіряючи його ідентичність, яку пропонує хост кожного разу, коли користувач відвідує його із закріпленим ідентифікатором. Ця схема уможливила виявлення фальшивих сертифікатів. Так, один із найпомітніших випадків був в організації “DigiNotar-2011”.

Одним з захисних механізмів, який замінив закріплення сертифікату, став новий атрибут – прозорість сертифіката (Certificate Transparency). Цей механізм дозволяє перевіряти сертифікати клієнтів на предмет виявлення фальшивих, але не захищає від появи нових шахрайських сертифікатів. Цей недолік можна позбавитися шляхом використання центрів сертифікації для кожного домену, які перевіряють фальшиві сертифікати. В такому випадку веббраузери не є центральним органом контролю, але мають повноваження застосовувати політику журналювання.

Враховуючи, що ЦС не є обов’язковим для реєстрації нещодавно виданих сертифікатів у журналах Certificate Transparency (CT), деякі кореневі програми вимагають цього, щоб довіряти цифровому сертифікату. Наприклад, коренева програма Google, для якої часова позначка підписаного сертифіката SCT (Signed Certificate Timestamps) видається кожного разу, коли центр сертифікації надсилає новий сертифікат до журналу CT, а згодом кожна позначка SCT додається до відповідного сертифіката для перевірки помилкових полів. Недоліком цього підходу є відсутність можливості запобігти іншим загрозам порушення цілісності журналів CT та справжності часових міток SCT, у випадку відсутності системи реєстрації подій.

Сценарій 2

Окремим підходом до підвищення стійкості та надійності інфраструктури відкритих ключів є використання спеціальних програм “нотаріусів” для автентифікації цифрових сертифікатів, наданих серверами. Призначенням «нотаріусів» є збирання інформації щодо сертифікатів різних користувачів, які мають доступ до певного домену, та наступним використанням цієї інформації для захисту від використання хибних сертифікатів. Це ускладнює задачу зловмисника нав’язати хибну інформацію та зменшує вірогідність атаки MITM. Такий підхід був використаний в MECAI (Mutually Endorsing CA infrastructure), де «нотаріуси» також були центрами видачі сертифікатів, з обмеженням, що центр сертифікації не може бути власним «нотаріусом» для своїх сертифікатів. Ця вимога реалізує заборону використання самопідписаних сертифікатів та зменшує ризики MITM-атак.

Іншими підходами є використання суверенних ключів, додаткового контролю сертифікатів, спеціального середовища EFF SLL, MonkeySphere, AKI, Crossbear, DoubleCheck, S-Links, DNSChain, PoliCert, DetecTor та ICSI-нотаріус, опис яких можна знайти в [53].

Підсумовуючи огляд сценаріїв 1 та 2 можна зазначити, що вони є реактивними, що потребує постійного моніторингу та виявлення відхилень або аномалій у центрах видачі сертифікатів та у виданих цифрових сертифікатах.

В такому сенсі, альтернативними рішеннями є превентивні і активні підходи. Одним з таких рішень є використання технології децентралізованого розповсюдження та управління ключами (технології блокчейн) для забезпечення цілісності та автентичності процедур ідентифікації та автентифікації як центрів видачі сертифікатів, так і самих сертифікатів відкритих ключів.

Сценарій 3

Цей підхід оснований на використанні децентралізованих ідентифікаторів DID (Decentralized Identifiers), які визначені специфікацією W3C (World Wide Web Consortium), та використовуються децентралізованою системою управління ключами (Decentralized Key Management Systems-DKMS). Створення DKMS стала альтернативою існуючим системам, яка забезпечує захист від атак на мобільні платформи, які постійно змінюють позицію та з'єднуються з різними базовими станціями, що створює загрози процедурам генерації та розповсюдження криптографічних ключів. Відомим прикладом застосування DKMS стала концепція Vehicular Decentralized Key Management System (VDKMS) для мереж Cellular Vehicular-to-Everything (V2X). В основі концепції VDKMS лежить принцип суверенної ідентичності Self-Sovereign Identity (SSI). Принцип SSI заключається в використанні набору відомостей про особу, якими вона може керувати, ділитися з будь-якими приватними особами або публічними сервісами, відкликати до них доступ у будь-який час за своїм бажанням. Для ідентифікації даних застосовують формат Decentralized Identifier (DID). Принцип суверенної ідентичності SSI використовують для ефективної системи керування ключами, що дозволяє подолати обмеження на впровадження DKMS для мобільних платформ, прикладом яких є мережі VANET (Vehicular Ad hoc NETworks) та системи зв'язку з динамічною топологією MANET.

Для реалізації цього завдання використовують архітектуру, яка включає рівень додатку, рівень децентралізованої системи керування ключами, рівень SSI та рівень контролю транзакцій. Ця архітектура також називається технологією розподіленого реєстру (distributed ledger technology – DLT). З метою зменшення ризиків з незначними витратами на обчислення запропоноване рішення базується на використанні мікрореєстрів (distributed micro ledger technology – DMLT). Застосування DMLT для створення DKMS дозволяє забезпечити захист від більшості класів MITM-атак.

Структура DKMS на основі технології DMLT

Реалізація концепції DKMS включає наступні складові:

мобільна платформа;

реєстратор;

сервіс-провайдер;

блокчейн-складова (мікрореєстр).

Для взаємодії компонентів VDKMS здійснюються етапи:

забезпечення (Provision);

реєстрація (Registration);

перевірка облікових даних (Credentials Verification);

авторизація (Authorization).

Варіант побудови інфраструктури PKI з урахуванням особливостей розглянутих класів MITM-атак та сценаріїв захисту

Розглянемо варіант альтернативної інфраструктури PKI, яка має змішану інфраструктуру, що складається з елементів класичної PKI інфраструктури та елементів розподіленого реєстру. На рис. 7 наведена запропонована модель побудови гібридної системи розповсюдження криптографічних ключів.

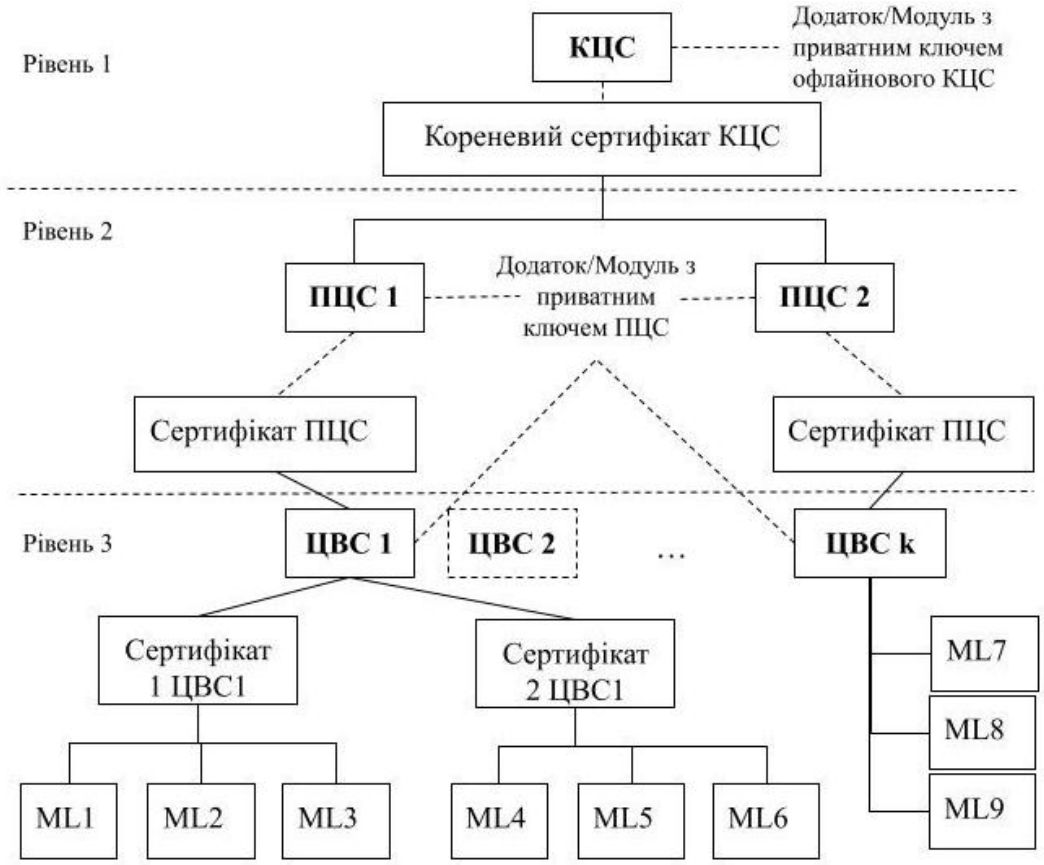


Рис. 7. Варіант альтернативної інфраструктури PKI з використанням концепції DKMS та технології DMLT

В запропонованій структурі розповсюдження криптографічних ключів на рис. 7 базовою структурою є існуюча модель побудови інфраструктури відкритих ключів, в якої на нижньому рівні, тобто на рівні, який найбільш схильний до впливів зловмисників, застосовується технологія розподілених мікрореєстрів (ML1-ML9), яка відрізняється від існуючої технології розподілених реєстрів використанням більш скороченого формату реєстру та підвищеною швидкістю транзакцій для обміну змінами реєстрів. Для побудови окремих ланцюгів (мікрореєстрів) використовуються сертифікати центрів видачі сертифікатів нижнього (третього рівня) (сертифікат 1 ЦВС 1, ЦВС 2, ЦВС k). В запропонованій схемі кожен реєстр є окремою мережею транзакцій, які можна розділяти як на окремі функціональні рівні, так і за рівнем критичності інформації, що планується оброблятися або передаватися в системі. Під час проведення експериментів були використані існуючі програмні бібліотеки для побудови блокчейну та створення мікрореєстрів [10, 11].

Висновки

В ході проведення дослідження було отримані результати аналізу існуючих способів організації атак "людина посередині" та способів реалізації кожного типу MITM-атак.

Визначено, що MITM-атаки є однією з найбільш небезпечних загроз практично усіх сучасних протоколів захисту інформації, що працюють через неконтрольовані канали передачі даних, а саме через безпровідні канали, через мережі стандарту 802.11 та через відкриті канали Інтернет. В якості об'єкта дослідження в роботі були визначені три варіанти побудови інфраструктури відкритих ключів, базова (однорівнева), дворівнева та багаторівнева. Визначені три класи центру розподілу криптографічних ключів, а саме: кореневий центр сертифікації ключів, центр видачі сертифікатів (ЦВС), проміжний центр сертифікації ключів. Визначено, вразливість (недолік) кожного підходу щодо побудови структурних схем взаємодії центрів сертифікації ключів, та обґрунтована перевага сегментування інфраструктури відкритих ключів з метою зниження шкоди під час компрометації або інших атак на інфраструктуру відкритих ключів.

Основним результатом, отриманим в роботі, є запропонована гібридна схема використання централізованого та децентралізованого підходу щодо розповсюдження криптографічних ключів, а саме використання класичної багаторівневої інфраструктури відкритих ключів, на нижньому рівні якої застосовується технологія децентралізованого розповсюдження ключів DKMS, яка використовує мікрореєстри, що зберігаються на кожному програмно-апаратному пристрої в клієнтському програмному забезпеченні. Запропоноване рішення дозволяє знизити ймовірність реалізації MITM-атаки на рівні доступу користувачів до центрів видачі сертифікатів пропорційно кількості користувачів для конкретного сегмента (окремого мікрореєстру). Також застосування технології DLT дозволить розділяти мережі на рівні сервісів, що надає можливість зменшити масштаби атак на інфраструктури та системи розповсюдження криптографічних ключів.

Наступним кроком досліджень заплановано дослідження показників швидкодії роботи розробленої гібридної інфраструктури з використанням технології DLT з використанням розробленого програмного забезпечення на основі відкритих джерел.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Twigg, N. Dimmock. Attack-Resistance of Computational Trust Models. In Proceedings of the 12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'03). 2003.

2. E. Bruneton, T. Coupaye, M. Leclerc, V. Quéma, and J.-B. Stéfani. The Fractal Component Model and its Support in Java. Software - Practice and Experience (SP&E), special issue on Experiences with Auto-adaptive and Reconfigurable Systems, 36 (11-12): 1257–1284, 2006.

3. A. Joseph Ed. "Security and Privacy in Pervasive Computing", IEEE Pervasive Computing, 6 (4): 73–75. 2007.

4. R. Oppliger, G. Pernul and C. Strauss, Using Attribute Certificates to Implement Role Based Authorization and Access Control Models, in the Proc. of 4. Fachtagung Sicherheit in Informationsystemen (SIS 2000), Zurich, Switzerland, 2000, 169–184.

5. G. Myles, A. Friday and N. Davies. Preserving Privacy in Environments with Location-Based Applications. Pervasive Computing, 2 (1): 56–64. 2003.

6. T. Dierks and C. Allen, The TLS Protocol Version 1.0, IETF RFC 2246, Jan. 1999.

7. Nicolas Serrano, Hilda Hadan, L. Jean Camp. A Complete Study of P.K.I. (PKI's Known Incidents) A. SSRN Electronic Journal · January 2019. Web: https://www.researchgate.net/publication/334789185.

8. URL: https://gist.github.com/ArturT/bc8836d3bedff801dc324ac959050d12.

9. URL: https://stackoverflow.com/questions/31621118/disable-sslv3-on-nginx.

10. URL: https://github.com/tko22/simple-blockchain.

11. URL: https://github.com/codingtmd/mini-blockchain/tree/master.

DOI: 10.58254/viti.6.2024.22.264

УДК 681.35

Черниш Ю. О. ORCID: 0000-0002-6626-5656 (ВІТІ ім. Героїв Крут)
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)

ПРИЙНЯТТЯ РІШЕНЬ В ПРОЦЕСІ ПОШУКУ ВРАЗЛИВОСТІ SERVER-SIDE WEB APPLICATION

Процес пошуку вразливості складається з трьох етапів. На першому етапі здійснюється ідентифікація дефекту програмних та програмно-апаратних компонентів з оцінкою їх придатності для експлуатації. Другий етап присвячений вибору існуючого або розробці нового експлойту для ідентифікованого дефекту. На третьому етапі відбувається налагодження зручності використання та надійності експлойту. Вразливість (vulnerability) системи об'єкта кіберзахисту до здійснення негативного технічного ефекту (negative technical impact) завжди базується на експлуатації її дефектів. Ідентифікація дефекту з оцінкою придатності до застосування є багатоетапним процесом вибору рішення в умовах невизначеності. Ефективність процесу пошуку дефекту можна підвищити на основі застосування теорії прийняття рішень.

Ідея полягає у зменшенні невизначеності, використовуючи інформаційну модель для пошуку вразливості із можливістю її кількісного аналізу. Для кількісного аналізу застосовуються класичні критерії вибору рішень в умовах невизначеності. Інформаційна модель є ієрархічною, має чотири рівні та включає чотири типи елементів. Перший рівень складається з методів Initial Access, другий – з категорій вразливості Web Application. Третій та четвертий рівень оцінки, відповідно, дефектів та вразливості компонентів.

Доцільність, раціональність та обґрунтованість рішень з пошуку дефектів базується на застосуванні апробованих джерел експертного досвіду світового рівня. Так, Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) визначає, системи класу Server-side Web Application привабливим для хакерів об'єктом атак з найбільшою середньою кількістю потенційних дефектів у складі принаймні трьох компонентів: Web Server, Web Application Server, DBMS Server. Для з'ясування розподілу дефектів Server-side Web Application за характерними класами необхідно скористатися Open Worldwide Application Security Project (OWASP), для детального ознайомлення з ними – Common Weakness Enumeration (CWE). Застосування National Vulnerability Database (NVD) та Common Vulnerabilities and Exposures (CVE) доповнює оцінку знайденого дефекту.

Ключові слова: *прийняття рішень, пошук вразливостей, об'єкт кіберзахисту*

Y. Chernysh, P. Khusainov, T. Tereshchenko. Decision Making in the Searching Weakness Process of Server-Side Web Application.

The vulnerability search process consists of three stages. At the first stage, the weakness of software and firmware components is identified and their suitability for exploitation. The second stage is devoted to choosing an existing or developing a new exploit for the identified weakness. The third stage configures the usability and reliability of the exploit for the identified vulnerability. The vulnerability of the system of the cyber protection object to negative technical impact is always based on the exploitation of its defects. Weakness identification with applicability assessment is a multi-stage process of choosing solutions under conditions of uncertainty. The efficiency of the weakness search process can be improved by using decision making theory.

The idea is to reduce uncertainty by using an information model to search for weakness and to make it possible to process it quantitative analysis. For quantitative analysis, classical criteria for choosing solutions under uncertainty conditions were used. The information model is a hierarchy, has four levels and includes four types of elements. First level consists a techniques of Initial Access. First level consists a techniques of Initial Access, second – of category wekness Web Application. The third and fourth levels of assessment, respectively, of weaknesses and vulnerabilities.

The expediency, rationality and reasonableness of solutions for finding defects is based on the application of proven sources of world-class expert experience. Thus, Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) defines Server-side Web Application class systems as an attractive attack target for hackers with the highest average number of potential defects in at least three components: Web Server, Web Application Server, DBMS Server. To find out the distribution of Server-side Web Application defects by characteristic classes, it is necessary to use the Open Worldwide Application Security Project (OWASP), for a detailed study of them - Common Weakness Enumeration (CWE). The application of the National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE) complements the evaluation of the found defect.

Keywords: *decision making, searching vulnerabilities, cyber protection object.*

Постановка завдання. Пошук вразливості системи (об'єкта кіберзахисту) є послідовним та багатоетапним процесом прийняття рішень, який розглядається у контексті можливостей застосування тактик, технік, процедур *Adversarial Tactics*, *Techniques & Common Knowledge (ATT&CK)*. Організація пошуку та виявлення потенційної вразливості здійснюється власником системи (далі – Власник) шляхом оголошення публічної пропозиції. У публічній пропозиції, зокрема, визначається інформація про систему, часові строки, початкові умови, обмеження та порядок звітування про виконання робіт (послуги) дослідником потенційної вразливості (далі – Дослідник). Вразливість системи – властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режим функціонування системи, здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів [1, 2].

Розглянемо діяльність Дослідника за умови його неприналежності до множини користувачів системи, розташування поза адміністративними межами інфраструктури об'єкта кіберзахисту, а також без полягання на дію фактора "соціальної інженерії" стосовно легітимних користувачів. Процес пошуку потенційної вразливості складається з трьох послідовних етапів. На першому етапі здійснюється ідентифікація дефекту (проєктування, реалізації та/або налаштування) програмних (програмно-апаратних) компонентів з оцінкою її придатності для експлуатації вразливості системи (об'єкта кіберзахисту). Другий етап присвячений вибору існуючого або розробці нового експлойта для ідентифікованого дефекту. На третьому етапі відбувається налагодження працездатності та надійності (у системному оточенні) програмної реалізації експлойта для ідентифікованого (і найбільш перспективного, з точки зору Дослідника) дефекту системи (об'єкта кіберзахисту).

На кожному з етапів вирішення задачі пошуку потенційної вразливості Дослідник знаходиться під впливом невизначеності. Причинами невизначеності (неповноти, недостатності, обмеженості, неточності) інформації для вибору рішення можуть бути:

неможливість точного передбачення наслідків рішень;

неможливість повторення або експериментальної перевірки рішення;

особа, яка приймає рішення (ОПР) немає можливості контролю всіх факторів;

наявність множини альтернативних рішень та необхідність вибору одного з них;

низька якість початкової інформації формулювання задачі та вибору рішення.

На підставі викладеного, пропонується розглянути підхід до інформаційного забезпечення вибору рішення в умовах невизначеності Дослідником потенційної вразливості компонентів *Server-Side Web Application* системи (об'єкта кіберзахисту) у контексті науково-методичного апарату прийняття рішень.

Аналіз публікацій. Тактики (тактичні цілі) *ATT&CK for Enterprise* уособлюють експертні знання про відношення понять "ціль – спосіб – результат" для кожного з кроків можливих сценаріїв кібератаки. Доведення Дослідником вразливості системи (об'єкта кіберзахисту) на предмет можливості її компрометації цілком відповідає досягненню тактичної цілі (тактики) *Initial Access* з використанням, принаймні, однієї з десяти незалежних технік (методів, способів). Вибір Дослідником техніки (методу, способу дії) досягнення тактичної цілі (тактики) *Initial Access* обумовлено початковим умовам задачі [3].

Вразливість (*vulnerability*) системи (об'єкта кіберзахисту) призводить до нав'язування йому непередбаченого негативного технічного впливу (*negative technical impact*). Іншими словами, нав'язування негативного технічного впливу базується на можливості непередбаченого використання (експлуатації) певного дефекту (*weakness*) програмних, апаратних, програмно-апаратних чи системних компонентів, які при певних умовах призводять до вразливого стану (вразливості) системи (об'єкта кіберзахисту). Атака (*attack*) –

спроба експлуатації дефекту системи з метою нав'язування їй вразливого стану для прояву негативного технічного ефекту шляхом застосування програмного експлойта (*exploit*) [4].

Дефекти програмних (програмно-апаратних) компонентів, які при певних умовах можуть призвести до вразливості *Server-side Web Application* за версією *Top 10 Web Application Security Risks*, розподілені на десять категорій [5].

Формулювання мети статті. Найбільш широкий спектр практичних задач діяльності Дослідника потенційної вразливості системи (об'єкта кіберзахисту) обмежений необхідністю дотримання таких умов:

відсутність або найменший рівень повноважень при спробі експлуатації дефекту будь-якого програмного (програмно-апаратного) компонента системи (об'єкта кіберзахисту);

відсутність фізичного доступу до апаратних засобів системи (об'єкта кіберзахисту);

відсутність можливостей або недоцільність впливу на ланцюги постачання програмних (програмно-апаратних) компонентів, апаратних засобів для інфраструктури;

відсутність можливостей або недоцільність використання способів соціальної інженерії стосовно легітимних користувачів системи (об'єкта кіберзахисту);

підключення інфраструктури системи (об'єкта кіберзахисту) до Інтернет або інших глобальних систем передачі даних.

За таких умов діяльність Дослідника, щодо компрометації системи (об'єкта кіберзахисту), повинна бути спрямована на досягнення тактичної цілі (тактики) *Initial Access* і є застосуванням техніки (методу, способу дії) *Exploit Public-Facing Application.* При цьому найбільш популярним видом організації інфраструктури *Public-Facing Application* є *Server-Side Web Application* [6].

Ідентифікація Дослідником дефекту (проєктування, реалізації та/або налаштування) програмних (програмно-апаратних) компонентів з оцінкою його придатності для експлуатації вразливості *Server-Side Web Application* багатокроковий процес з багатьма актами вибору рішень в умовах невизначеності. Зменшення впливу невизначеності і, відповідно, підвищення ефективності процесу пошуку Дослідником потенційної вразливості системи (об'єкта кіберзахисту), зокрема, у компонетах *Server-Side Web Application* може бути зроблено на основі науково-методичного апарату прийняття рішень. Ключовими елементами запропонованого результату дослідження: структура інформаційної моделі предметної області та забезпечення її придатності для обробки із застуванням відомих критеріїв (мінімаксний, Лапласа, Севіджа, Гурвіца, Ходжа-Лемана, Гермейера).

Основна частина. Прийняття рішень (ПР) людиною завжди є результатом складних психологічних процесів. Розрізняють функціонально-динамічний та логіко-психологічний підхід до дослідження процесів ПР [7].

Функціонально-динамічний підхід спрямований на дослідження комплексу психологічних механізмів ПР. 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 ПР.

Логіко-психологічний підхід базується на представленні процесів ПР у формі послідовності етапів: постановки задачі; здобуття та обробка інформації для ПР; аналіз та ідентифікації проблемної ситуації; вироблення множини альтернативних рішень; вибір рішення; реалізація рішення. Сукупність дій, щодо забезпечення етапів ПР, розглядається

як композиція множин операцій інформаційної підготовки ПР, вибору та реалізації рішення (як результату процесів ПР).

Вибір рішення є прерогативою людини і принципово не може мати формального подання. Особа, яка приймає рішення (ОПР) керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб’єктивними уявленнями, судженнями, емоціями. Прямий чи опосередкований вплив на вибір рішення ОПР можуть мати психологічні властивості, які не є вродженими і з розвитком особистості змінюються (формуються) залежно від конкретних суспільно-історичних умов:

світогляд (система поглядів на суспільство та природу явищ);

інтереси (спрямованість на певні предмети та явища);

здібності (індивідуальні особливості – умови успішного виконання якої-небудь однієї або кількох видів діяльності);

темперамент;

характер;

увага (спрямованість свідомості на певний предмет або діяльність: стійкість, перемикання, розподіл та об’єм).

Традиційними показниками оцінки ефективності широкого спектра процесів людської діяльності є величина середньої тривалості, матеріальні або фінансові витрати. Аналіз особливостей (з урахуванням визначених вище умов) процесу пошуку потенційної вразливості системи (об’єкта кіберзахисту) показав значну залежність від рівня кваліфікації Дослідника щодо реалізації складних форм експлуатації можливих дефектів.

Розрізняють два широких класи задач вибору рішень при неповній інформації про задачу та проблемну ситуацію ПР. Перший клас задач відомий як “прийняття рішень в умовах ризику”, другий – “прийняття рішень в умовах невизначеності”. Неповнота інформації ПР в умовах ризику передбачає існування функцій розподілу ймовірностей для всіх досліджуваних величин, в умовах невизначеності – функції розподілу невідомі або не можуть бути визначені. На практиці невизначеність не означає повної відсутності інформації про задачу. Можуть бути відомими деяка кінцева кількість значень кожної величини, але без відповідних функцій розподілу ймовірностей. Розгляд проблематики вирішення задач прийняття рішень в умовах ризику можливо при наявності експериментальних даних необхідного об’єму для визначення функцій розподілу кожної з досліджуваних величин. Для предметної області пошуку потенційної вразливості системи (об’єкта кіберзахисту) такі властивості непритаманні, що робить недоцільним розгляд умов ризику.

Розглянемо задачу вибору рішення в умовах невизначеності у контексті пошуку потенційної вразливості системи (об’єкта кіберзахисту) на етапі *Initial Access* шляхом *Exploit Public-Facing Application* у формі інфраструктури *Server-Side Web Application* (рис. 1). Успішний результат діяльності Дослідника полягає у доведенні вразливості системи (об’єкта кіберзахисту) шляхом демонстрації нав’язування їй певного негативного технічного впливу.

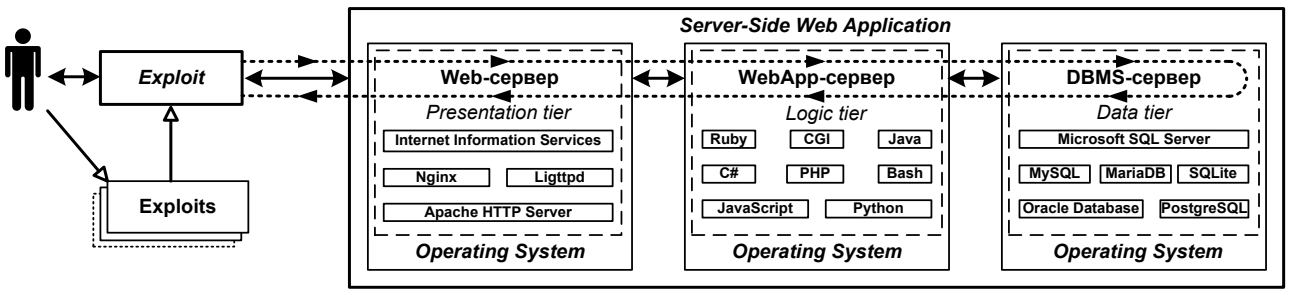


Рис. 1. Інтерпретація задачі пошуку потенційної вразливості *Server-Side Web Application*

Вибір рішень в умовах невизначеності здійснюється із застосуванням критеріїв ПР. Нагадаємо, що критерієм називається необхідна і достатня ознака оцінки або вибору рішення. Розрізняють прості (із застосуванням одного показника) та складні (комбінування кількох показників) критерії. Показник – кількісна характеристика досліджуваного об'єкта, яка має назву та діапазон можливих значень. Критерії ПР відображають більш або менш оптимістичну (песимістичну) суб'єктивну стратегію ОПР при виборі рішення.

Так, традиційними (відображають найбільш широко вживані стратегії) критеріями ПР в умовах невизначеності являються мінімаксний (максиміний), Лапласа (Байеса-Лапласа), Севіджа. Розширення спектра можливих стратегій здійснюється шляхом введення похідних критеріїв ПР Гурвіца, Ходжа-Лемана, Гермейера. Матриця рішень формується на підставі значень оціночної функції. Формалізоване подання оціночної функції відображає залежність між початковими умовами, факторами та результатом, яка визначається у термінах залежних та незалежних змінних. Можливі варіанти значень залежних та незалежних змінних утворюють відповідний набір значень оціночної функції для всієї множини альтернативних рішень. Вибір змінних (залежні, незалежні) та відношень між ними для створення оціночної функції уособлює сутність якості урахування особливостей предметної області ПР.

Обов'язковою умовою доведення вразливості є наявність (існування) працездатної програмної реалізації експлойта. Іншими словами, демонстрація нав'язування негативного технічного впливу шляхом експлуатації дефектів компонентів *Server-Side Web Application* без застосування відповідного експлойта не є дійсною і не може бути здійснена. Множина альтернативних рішень визначається кількістю окремих засобів у колекції вже відомих і/або розроблених експлойтів (exploits), вибір одного з альтернативних рішень – уособлюється з вибором експлойта, що найбільш придатний для практичного нав'язування негативного технічного впливу в інфраструктурі компонентів *Server-Side Web Application.*

Розглянемо проблемні питання вразливості *Server-side Web Application* за версією *The Open Worldwide Application Security Project (OWASP)*. Вразливості *Server-side Web Application* розподілені за категоріями *Top 10 Web Application Security Risks*, а їх формулювання здійснено на основі асоційованих записів *Common Weakness Enumeration (CWE)* та *Common Vulnerabilities and Exposures (CVE)*. Опис категорій *Top 10 Web Application Security Risks* доповнюються оцінками загальної кількості асоційованих записів *CWEs Mapped* та *Total CVEs* зі складу відповідного вектора кількісних характеристик.

1. Контроль доступу (*A01:2021 Broken Access Control*). Стислий опис дефектів: недотримання принципу найменших привілеїв; відсутність (недостатність, некоректність, неправильна реалізація) контролю (перевірки) розширення (зміни) повноважень та використання маркерів доступу (функцій інтерфейсу прикладного програмування, посилань на об'єкти). *CWEs Mapped* = 34. *Total CVEs* = 19013.

2. Криптографічні перетворення (*A02:2021 Cryptographic Failures)*. Стислий опис дефектів: використання менш стійких криптографічних елементів (ключів, векторів ініціалізації, гамм шифру) при неможливості утворення захищеного каналу; відсутність (недостатність, некоректність, неправильна реалізація) контролю (перевірки) автентичності та дійсності (ключів, цифрових підписів, програмних компонентів, ідентифікаційних сертифікатів); надлишкова інформативність реакції компонентів при обробці некоректних (неправильних) комбінацій криптографічних даних. *CWEs Mapped* = 29. *Total CVEs* =3075.

3. Коректність вхідних даних (*A03:2021 Injection*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю та усунення небезпечних (некоректних) вхідних даних (співставлень, інтерпретацій об'єктів); надлишкова інформативність реакції компонентів при обробці некоректних (неправильних) запитів до системи керування базою даних. *CWEs Mapped* = 33. *Total CVEs* = 32078.

4. Безпечний дизайн (*A04:2021 Insecure Design*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур *OWASP Software Assurance Maturity Model (SAMM)* на всіх етапах розробки компонентів *Server-side Web Application* із застосуванням апробованих програмних елементів. *CWEs Mapped* = 40. *Total CVEs* = 2691.

5. Неправильні налаштування безпеки (*A05:2021 Security Misconfiguration*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур безпеки використання хмарних сервісів; використання компонентів (облікових записів) з налаштуваннями за замовчанням; надлишкова інформативність відповідей на некоректні (недоречні) запити до компонентів *Server-side Web Application*; відсутність (недостатність, некоректність, неправильна реалізація) контролю (перевірки) використання актуальних версій оновлень безпеки та аналізу ризиків. *CWEs Mapped* = 20. *Total CVEs* =789.

6. Контроль вразливих та застарілих версій компонентів (*A06:2021 Vulnerable and Outdated Components*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю та оновлення застарілих (неактуальних) версій компонентів *Server-side Web Application*. *CWEs Mapped = 3. Total CVEs* = 0.

7. Ідентифікація та автентифікація (*A07:2021 Identification and Authentication Failures*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю за проявом нестійкості до угадування (прогнозування) можливих значень одноразових паролів (маркерів, ідентифікаторів) та їх повторного використання; критичне порушення логіки процесу двофакторної автентифікації та відновлення паролів; можливість витоку незашифрованих (зашифрованих з використанням нестійких криптографічних алгоритмів) значень паролів через діагностичні повідомлення або у відповідях на некоректні (недоречні) запити до компонентів *Server-side Web Application*. *CWEs Mapped = 22. Total CVEs =3897.*

8. Цілісність компонентів і даних (*A08:2021 Software and Data Integrity Failures*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю автентичності (цілісності, безпечності) даних у складі серіалізованих об’єктів (конвеєрів обробки даних за замовчуванням) та програмних компонентів *Server-side Web Application*, що інсталюються (оновлюються) з репозиторіїв (зовнішніх носіїв). *CWEs Mapped* = 10. *Total CVEs* =1152.

9. Реєстрація подій та моніторинг (*A09:2021 Security Logging and Monitoring Failures*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур реєстрації, обліку, архівування (резервування) та систематичного (ретроспективного) аналізу повідомлень про події функціонування компонентів *Server-side Web Application*; низька інформативність (прагматична цінність) повідомлень про події; неузгодженість форматів повідомлень від різних джерел; потрапляння критичної технологічної інформації (ідентифікаторів, параметрів автентифікації) до вмісту повідомлень про події з можливістю її витоку. *CWEs Mapped* = 4. *Total CVEs* = 242.

10. Коректність запитів *Web*-сервера (*A10:2021 Server-Side Request Forgery*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю (перевірки) та запобігання (усунення) запитів *Web*-сервера до інших компонентів *Server-side Web Application* від запитів *Web*-клієнта. *CWEs Mapped* = 1. *Total CVEs* = 387.

Сукупність асоційованих з категоріями *Top 10 Web Application Security Risks* записів *CWE* та *CVE* утворюють інформаційну модель вибору рішення в умовах невизначеності в процесі пошуку вразливості *Server-Side Web Application* (рис. 2). Під поняттям “інформаційна модель” зазвичай розуміють організовану за певними правилами сукупність інформації про властивості об’єкта (системи, процесу), який підлягає спостереженню (керуванню). Інформаційна модель повинна відображати залежні та незалежні змінні оціночної функції предметної області, мати раціональну інформативність, форму та композицію.

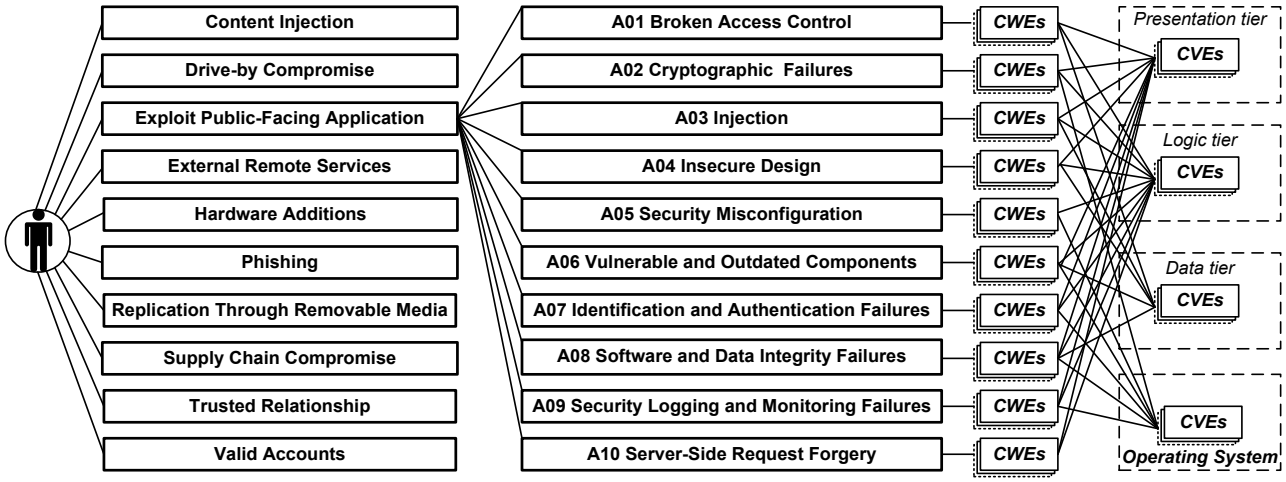


Рис. 2. Порядок утворення інформаційної моделі вибору рішення в задачах пошуку потенційної вразливості *Server-Side Web Application* для тактичної цілі *Initial Access*

Інформаційна модель вибору рішення в процесі пошуку вразливості *Server-Side Web Application* є ієрархією, яка складається з чотирьох рівнів та містить чотири типи інформаційних елементів. На практиці не існує встановленої процедури генерування ієрархій. Зазвичай ця процедура починається з вивчення літератури для збагачення думками. Знайомлячись із чужими працями, ми нібито проходимо через стадію мозкового штурму для складання переліку всіх концепцій, істотних для завдання, незалежно від їхнього співвідношення чи порядку. Далі, здійснюється спроба створення деякої ієрархічної системи понять та відношень між ними на основі застосування таких аксіом:

зв’язані з поняттям інформаційні елементи утворюють незалежні множини;

елементи однієї множини визначають групу елементів рівня ієрархії;

елементи груп різних зв’язаних рівнів ієрархії функціонально впливають один на одного через інтерпретацію відношень між поняттями відповідних незалежних множин;

кожен елемент ієрархії може бути функціонально-зв’язаним з кількома поняттями;

роль елемента відносно іншого, може бути головною, підлеглою або нейтральною.

Розглянемо ієрархію запропонованої інформаційної моделі (відлік рівнів ієрархії здійснюється зліва направо).

Перший рівень ієрархії відображує можливі тактики (способи дії) Дослідника для досягнення тактичної цілі *Initial Access* (за версію *MITRE ATT&CK for Enterprise*). Досягнення тактичної цілі *Initial Access* полягає у нав’язуванні Дослідником виконання власного алгоритму негативного технічного впливу з повноваженнями вразливого програмного компоненту об’єкта кіберзахисту. Досвід історії дослідження фахівцями корпорації *MITRE* відомих кіберінцидентів (кібератак) дозволив визначити десять незалежних методів нав’язування. Вибір способу дії з множини альтернативних варіантів першого рівня ієрархії обумовлені інтерпретацією сформульованих раніше початкових умов процесу пошуку Дослідником потенційної вразливості *Exploit Public-Facing Application*:

відсутність або найменший рівень повноважень суб’єкта доступу до інфраструктури, який керується Дослідником;

відсутність фізичного доступу Дослідника до апаратних засобів інфраструктури;

відсутність можливостей або недоцільність (велика вартість, висока невизначеність досягнення успіху) впливу Дослідника на ланцюги постачання програмних (програмно-апаратних) компонентів та апаратних засобів для інфраструктури;

відсутність у Дослідника можливостей використання способів соціальної інженерії стосовно легітимних користувачів інфраструктури;

суб'єкт доступу, який керується Дослідником, може взаємодіяти з компонентами *Server-Side Web Application* через вхідний маршрутизатор його інфраструктури, політика фільтрації маршрутизатора немає жодних обмежень.

Другий рівень ієрархії відображає множину альтернативних варіантів спрямування зусиль Дослідника в процесі пошуку потенційної вразливості *Server-Side Web Application* за десятьма категоріями *Top 10 Web Application Security Risks*. Числовий ідентифікатор категорії вразливості є порядковою ранговою оцінкою її значущості для компрометації системи компонентів *Server-Side Web Application.* Рангова оцінка визначається на підставі оціночної функції ваги категорії вразливості. Вхідними даними для обчислення значення оціночної функції є сукупність кількісних значень таких часткових показників:

CWEs Mapped (кількість типових дефектів, що мали місце для прояву вразливості);

Max Incidence Rate, Avg Incidence Rate (максимальний та середній процент існуючих *Web Application*-продуктів, які мають дефекти з переліку *CWE* для цієї категорії вразливості);

Max Coverage, Avg Coverage (максимальний та середній процент *Web Application*-продуктів, які мають хоча б один дефект з переліку *CWE* для цієї категорії вразливості відносно всіх *Web Application*-продуктів всіх організацій);

Total Occurrences (загальна кількість ідентифікованих *Web Application*-продуктів, які мають хоча б один дефект з переліку *CWE* для цієї категорії вразливості);

Total CVEs (загальна кількість *CVE* для яких є характерним згадування хоча б одного з переліку *CWE* для цієї категорії вразливості).

Третій рівень ієрархії містить ідентифікатори підмножин записів класифікатора *CWE*, які асоційовані з відповідними категоріями вразливості *Top 10 Web Application Security Risks*. Система оцінки *Common Weakness Scoring System (CWSS)* забезпечує механізм для визначення пріоритетності у дефектів (проєктування, реалізації та/або налаштування) програмних (програмно-апаратних) та апаратних компонентів цільового об'єкта [8, 9]. Значення результуючої оцінки *CWSS* базується на застосуванні трьох груп показників.

Перша, за порядком згадування, група показників *Base Finding metric group* (основні пошукові характеристики дефекту) уособлюють величину ризику визначеного дефекту, впевненість у точності його ідентифікації та достовірність засобів контролю. Значення метрик *Base Finding metric group* визначають:

результат успішної ідентифікації та експлуатації дефекту (*Technical Impact, TI*);

необхідний рівень повноважень для експлуатації дефекту (*Acquired Privilege, AP*);

набутий рівень повноважень після експлуатації дефекту (*Acquired Privilege Layer, AL*);

можливість запобігання експлуатації дефекту на основі використання існуючих захисних механізмів (*Internal Control Effectiveness, IC*);

впевненість у можливості успішної експлуатації дефекту (*Finding Confidence, FC*).

Друга група показників *Attack Surface metric group* (характеристики умов "поверхні" реалізації атаки для експлуатації дефекту) відображає якість бар'єрів (захисних механізмів). Значення метрик *Attack Surface metric group* визначають:

необхідний рівень повноважень суб'єкта атаки для доступу до програмної реалізації функціональних можливостей компонента, що містить дефект (*Required Privilege, RP*);

необхідний рівень повноважень суб'єкта атаки в системному операційному середовищі для успішної експлуатації дефекту (*Required Privilege Layer, RL*);

канал комунікації, який надає суб'єкту атаки доступ до функціональних можливостей результату успішної експлуатації дефекту (*Access Vector, AV*);

надійність процедури захисту доступу до функціональних можливостей результату успішної експлуатації дефекту (*Authentication Strength, AS*);

участь легітимного користувача при експлуатації дефекту (*Level of Interaction, IN*);

поширеність успішної експлуатації дефекту (*Deployment Scope, SC*).

Третя група показників *Environmental metric group* описує характеристики системного операційного оточення компонентів цільового об'єкта, в якому ідентифіковано дефект:

ступінь негативного впливу результату успішної експлуатації дефекту на процеси використання цільового об'єкта за призначенням (*Business Impact, BI*);

ймовірність ідентифікації дефекту суб'єктом атаки (*Likelihood of Discovery, DI*);

ймовірність успішної експлуатації дефекту суб'єктом атаки (*Likelihood of Exploit, EX*);

можливість запобігання експлуатації дефекту з використанням засобів системного операційного оточення компонента, який містить дефект (*External Control Effectiveness, EC*);

частота ідентифікації дефекту даного типу у інших компонентах (*Prevalence, P*).

Розрізняють цільовий, узагальнений, контекстний та агрегований метод застосування *CWSS.* Цільовий метод спрямований на оцінювання окремої вразливості, що була виявлена при розробці конкретного програмного пакета компонентів. Предметом узагальненого методу є клас вразливості незалежно від конкретного програмного пакета. Величина узагальненої оцінки визначається на підставі аналізу прояву класу вразливості у конкретному програмному пакеті компонентів. Узагальнені та цільові оцінки можуть суттєво відрізнятися. Контекстний метод базується на врахуванні особливостей процесів діяльності, системного оточення, ризиків тощо. Цей метод може застосовуватися в комбінації з методами цільового та узагальненого оцінювання або доповнюючи їх. Агрегований метод спрямований на одержання загальної оцінки кількох вразливостей. Хоча агрегування може бути найбільш застосовним для цільового методу, його також можна використовувати для узагальненого оцінювання, цільової та контекстної оцінки.

Четвертий рівень ієрархії відображає розподіл записів *CVE* за компонентами *Server-Side Web Application,* які забезпечують функції *Presentation tier, Logic tier, Data tier* та *Operating System*.

Система оцінки вразливостей *Common Vulnerability Scoring System (CVSS)* базується на застосуванні сукупності чотирьох груп показників. Група показників *Base* (базові) призначена для опису незмінних властивостей у часі та у різних системних середовищах. Група *Threat* (загрози) відображає зміни характеристики з плином часу, а група *Environmental* (оточення) – змінні характеристики з урахуванням особливостей системного операційного середовища. Четверта група показників *Supplemental* (додаткова) застосовується для уточнення характеристик [10-11].

Величина результуючого кількісного значення оцінки *CVSS* визначає серйозність вразливості, яка розраховується на основі стандартизованої формули *CVSS* на основі метрик, утворених відповідно до груп показників *Bas*e, *Threat* та *Environmental*. Базова метрична оцінка (*Base Metrics*) уособлює величину серйозності вразливості як розумний найгірший вплив у будь-якому операційному системному середовищі, незалежно від плину часу. Тимчасові метрики (*Temporal Metrics*) коригують базовий рівень вразливості на основі факторів, які змінюються з часом, наприклад, доступність коду для експлойта. Метрики середовища (*Environmental Metrics*) уточнюють базовий та тимчасовий ступені серйозності до конкретного системного операційного середовища, наприклад, наявність засобів захисту.

Група факторів оцінювання величини *Base Metrics* (*Base metric group*) має внутрішній поділ на метрики можливостей експлуатації вразливості (*Exploitability metrics*) та метрики наслідків впливи (*Impact metrics*). Склад підгрупи *Exploitability metrics*:

вектор атаки (*Attack Vector, AV*);

повторюваність атаки (*Attack Complexity, AC*);

необхідний рівень привілеїв суб'єкта атаки (*Privileges Required, PR*);

необхідність взаємодії з користувачем, який працює в системі (*User Interaction, UI*);

умови масштабування атаки (*Scope, S*).

Показники факторів підгрупи *Impact metrics* відображають прямий наслідок успішної експлуатації вразливості у формі негативного впливу, відповідно, на конфіденційність (*Confidentiality, C*), цілісність (*Integrity, I*) та доступність (*Availability, A*) інформації, яка циркулює в інфраструктурі цільового об'єкта.

Група факторів оцінювання величини *Temporal Metrics* (*Temporal metric group*) призначені для оцінювання поточного стану придатності способів експлуатації вразливості, доступності тексту програмної реалізації цільового компонента для дослідження, здійснення виправлень та існування деяких можливостей обходу захисних механізмів. Склад підгрупи *Temporal metric group*:

показник ймовірності експлуатації вразливості із застосуванням існуючого практичного експлойта (*Exploit Code Maturity, E*);

рівень усунення вразливості (*Remediation Level, RL*);

ступінь впевненості у вразливості та її технічних деталях (*Report Confidence, RC*).

Група факторів оцінювання величини *Environmental Metrics* (*Environmental metric group*) відображає унікальні вимоги щодо впливу вразливості системного операційного середовища на конфіденційність (*Confidentiality Requirement, CR*), цілісність (*Integrity Requirement, IR*) та доступність (*Availability Requirement, AR*) інформації, що циркулює у інфраструктурі цільового об'єкта. Сукупність показників *Environmental metric group* є модифікованим еквівалентом *Base metric group* з урахуванням особливостей цільового об'єкта. Ідентифікатори модифікованих показники мають на початку назви слово *Modified*.

Векторний рядок *CWSS* та *CVSS* є текстовим представленням значень показників у стислій формі. Оцінки *CWSS* і *CVSS* не обов'язково порівнюються. Не всі фактори *CWSS* можна описати символічно за допомогою дискретних значень. Використання *CWSS* та *CVSS,* в умовах невизначеності, обумовлено проявом неповної інформація у звітах про вразливості (не містять усіх відповідних деталей, необхідних для оцінки). Якщо інформація відсутня, застосовується консервативний підхід, який полягає у виборі найбільшої величини оцінок.

Концептуально *CVSS* і *CWSS* дуже схожі. Однак у *CVSS* є деякі важливі переваги та обмеження. Однією з сильних сторін *CVSS* є її простота. Відмінності між *CVSS* та *CWSS*:

CVSS для оцінювання вразливості в інстальованих програмних компонентів;

CVSS розглядає вразливості, які вже виявлені та перевірені;

CWSS можна застосувати до того, як будуть доведені будь-які вразливості;

CVSS не можна масштабувати для оцінки програмного пакета компонентів;

CWSS придатний для оцінювання в умовах невизначеності;

CVSS непридатна до використання за умов неповної інформації;

CWSS надає оцінку дефекту до того як він сприяв вразливості;

CVSS має ухил врахування впливу на фізичну систему;

CWSS має невелике упередження на користь програми, яка містить дефекти;

CVSS може використовуватися як вхідні дані для управління ризиками організації;

CVSS не залежить від постачальника та платформи;

CWSS можуть бути розраховані автоматично.

На практиці оцінки *CVSS* не мають регулярного розподілу, як правило, з перекосом у бік високих оцінок; цілком можливо, що *CWSS* може мати кращий розподіл. Однак, оскільки оцінки *CWSS* можна розрахувати в ранніх сценаріях з низьким рівнем інформації, багато факторів є "тимчасовими" за своєю природою, незалежно від того, до якої групи вони належать. Спрощена модель конфіденційності/цілісності/доступності не забезпечує глибини та гнучкості *CVSS* забезпечує узгодженість, корисну для системних і мережевих адміністраторів, які не є фахівцями, для встановлення пріоритетів вразливості.

Висновки. Запропонований підхід до ПР, в умовах невизначеності, який супроводжує діяльність Дослідника потенційної вразливості, базується на використанні інформаційної

моделі для ПР, яка придатна для обробки із застосуванням критеріїв ПР. Ухил ОПР на більш чи менш оптимістичну (песимістичну) суб’єктивну стратегію досягається застосуванням відповідного критерію ПР. В якості прикладу вирішення задачі розглядається пошук вразливості компонентів інфраструктури *Server-Side Web Application* при виборі Дослідником техніки (способу дії) *Exploit Public-Facing Application* на етапі *Initial Access.*

Подальші дослідження щодо перевтілення науково-методичного апарату теорії ПР в діяльність фахівців з кібербезпеки спрямовані на врахування особливостей відношень між інформаційними елементами *CWSS* та *CVSS.*

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України “Про основні засади забезпечення кібербезпеки України”.
2. Постанова Кабінету Міністрів України від 16 травня 2023 року № 497 “Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж”.
3. Adversarial Tactics, Techniques & Common Knowledge. URL: https://attack.mitre.org.
4. Common Attack Pattern Enumerations and Classifications. URL: https://capec.mitre.org.
5. Open Worldwide Application Security Project. URL: https://owasp.org.
6. Терещенко Т. П., Остапчук В. М., Хусаінов П. В., Черниш Ю. О. Оцінка та запобігання прояву вразливості Server-Side Web Application / за заг. ред. Г. Д. Радзівілова // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць. Київ: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2024. № 5. 240 с. DOI: 10.58254/viti.5.2024. С. 204–214.
7. Герасимов Б. М., Локазюк В. М., Оксіюк О. Г., Поморова О. В. Інтелектуальні системи підтримки прийняття рішень: навч. посібник. К.: Вид-во Європ. ун-ту, 2007. 335 с.
8. Common Weakness Enumeration. URL: https://cwe.mitre.org.
9. Common Weakness Scoring System. URL: https://cwe.mitre.org/cwss/cwss_v1.0.1.html.
10. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org.
11. Common Vulnerability Scoring System. URL: https://www.first.org/cvss/.

АВТОРИ НОМЕРА

1. ***Артюх Сергій Григорович*** – ад'юнкт Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

2. ***Бербер Ілона Олегівна*** – курсант кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут ім. Ігоря Сікорського", м. Київ, Україна.

3. ***Бернацький Андрій Петрович*** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

4. ***Бєляков Роберт Олегович*** – кандидат технічних наук, доцент, заступник начальника кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

5. ***Борисов Ігор Володимирович*** – кандидат технічних наук, заступник начальника Науково-дослідного інституту воєнної розвідки.

6. ***Бригадир Сергій Петрович*** – старший науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

7. ***Войтко Тетяна Миколаївна*** – науковий співробітник науково-дослідного відділу впровадження стандартів доброчесності наукового центру проблем виховання доброчесності та запобігання корупції у секторі безпеки та оборони Національного університету оборони України, м. Київ, Україна.

8. ***Волков Олександр Віталійович*** – кандидат технічних наук, старший науковий співробітник, старший викладач Воєнної академії ім. Євгенія Березняка.

9. ***Волошин Василь Вікторович*** – молодший науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

10. ***Гримуд Андрій Геннадійович*** – доктор філософії, слухач Національного університету оборони України, м. Київ, Україна.

11. ***Гріньков Володимир Олександрович*** – кандидат технічних наук, доцент кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

12. ***Гріньков Станіслав Володимирович*** – співробітник Державної установи «Відкриті публічні фінанси», м. Київ, Україна.

13. ***Грінькова Галина Василівна*** – співробітник Науково-дослідного інституту воєнної розвідки.

14. ***Данилюк Ігор Андрійович*** – кандидат технічних наук, доцент, головний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

15. ***Думітраш Вячеслав Олексійович*** – провідний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

16. ***Жук Олександр Володимирович*** – доктор технічних наук, професор, начальник кафедри комунікаційних технологій та кіберзахисту Інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України, м. Київ, Україна.

17. ***Зінченко Михайло Олександрович*** – начальник науково-дослідного управління Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

18. ***Карпенко Андрій Олександрович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

19. ***Кисиленко Дар’я Юріївна*** – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

20. ***Клімович Сергій Олегович*** – кандидат технічних наук, доцент, начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

21. ***Ковальчук Богдан Петрович*** – молодший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

22. ***Комаров Володимир Олександрович*** – кандидат технічних наук, провідний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

23. ***Кузавков Василій Вікторович*** – доктор технічних наук, професор, начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

24. ***Куцаєв Павло Володимирович*** – молодший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

25. ***Ланко Антон Вікторович*** – заступник начальника факультету телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут з навчальної роботи, м. Київ, Україна.

26. ***Лобода Вероніка Вікторівна*** – старший науковий співробітник відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту ім. С. П. Корольова, м. Житомир, Україна.

27. ***Лобода Роман Іванович*** – старший науковий співробітник науково-дослідного відділу роботизованих систем наукового центру Житомирського військового інституту ім. С. П. Корольова, м. Житомир, Україна.

28. ***Мальцева Ірина Робертівна*** – старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

29. ***Марченко Віталій Вікторович*** – доктор філософії, доцент Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна.

30. ***Марченко Павло Андрійович*** – аспірант Інституту аерокосмічних технологій Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського», м. Київ, Україна.

31. ***Масесов Микола Олександрович*** – кандидат технічних наук, старший науковий співробітник, докторант Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

32. ***Матвєєв Євген Валерійович*** – викладач кафедри комплексів авіаційного озброєння Харківського національного університету Повітряних Сил ім. Івана Кожедуба, м. Харків, Україна.

33. ***Мацаєнко Андрій Миколайович*** – кандидат технічних наук, старший викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

34. ***Міночкін Анатолій Іванович*** – Заслужений працівник освіти України, доктор технічних наук, професор, провідний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

35. ***Мірошніченко Сергій Іванович*** – викладач кафедри комп’ютерно-інтегрованих технологій та кібербезпеки Житомирського військового інституту ім. С. П. Корольова, м. Житомир, Україна.

36. ***Міхєєв Юрій Іванович*** – кандидат технічних наук, старший дослідник, доцент кафедри інформаційної боротьби Інституту стратегічних комунікацій Національного університету оборони України, м. Київ, Україна.

37. ***Остапчук Віктор Миколайович*** – кандидат технічних наук, начальник Головного управління зв’язку та кібербезпеки Генерального штабу Збройних Сил України, м. Київ, Україна.

38. ***Остапчук Тетяна Василівна*** – старший науковий співробітник науково-дослідної лабораторії проблем фінансового забезпечення військ (сил) науково-дослідного управління військово-гуманітарних досліджень науково-дослідного центру Військового інституту Київського національного університету ім. Тараса Шевченка, м. Київ, Україна.

39. ***Павленко Михайло Михайлович*** – старший науковий співробітник відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту ім. С. П. Корольова, м. Житомир, Україна.

40. ***Паламарчук Світлана Анатоліївна*** – головний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

41. ***Панченко Ігор В’ячеславович*** – кандидат технічних наук, начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

42. ***Пількевич Ігор Анатолійович*** – доктор технічних наук, професор, професор кафедри комп’ютерно-інтегрованих технологій та кібербезпеки Житомирського військового інституту ім. С. П. Корольова, м. Житомир, Україна.

43. ***Погребняк Сергій Васильович*** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

44. ***Прийма Олексій Олегович*** – викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

45. ***Процюк Юрій Олександрович*** – провідний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

46. ***Радзівілов Григорій Данилович*** – кандидат технічних наук, професор, заступник начальника Військового інституту телекомунікацій та інформатизації ім. Героїв Крут з наукової роботи, м. Київ, Україна.

47. ***Романов Дмитро Олександрович*** – начальник Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

48. ***Романюк Валерій Антонович*** – доктор технічних наук, професор, професор кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

49. ***Сайко Володимир Григорович*** – доктор технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

50. ***Сердюк Павло Євгенійович*** – науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

51. ***Симоненко Олександр Анатолійович*** – кандидат технічних наук, доцент, начальник відділу забезпечення якості освітньої діяльності та вищої освіти Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

52. ***Сорочкін Олександр Миколайович*** – старший викладач кафедри комплексів авіаційного озброєння Харківського національного університету Повітряних Сил ім. Івана Кожедуба, м. Харків, Україна.

53. ***Сосулін Михайло Володимирович*** – викладач кафедри комплексів авіаційного озброєння Харківського національного університету Повітряних Сил ім. Івана Кожедуба, м. Харків, Україна.

54. ***Терещенко Тетяна Павлівна*** – старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

55. ***Троцько Олександр Олександрович –*** кандидат технічних наук, доцент, начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

56. ***Усик Анна Андріївна*** – начальник групи автоматизованих систем управління кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

57. ***Фесьоха Віталій Вікторович*** – доктор філософії, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

58. ***Фомін Микола Миколайович*** – доктор філософії, начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

59. ***Хорошко Володимир Олексійович*** – доктор технічних наук, професор, науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

60. ***Хусаінов Павло Володимирович*** – кандидат технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

61. ***Чайківський Віталій Володимирович*** – студент Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна.

62. ***Чевардін Владислав Євгенійович*** – доктор технічних наук, старший науковий співробітник, начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

63. ***Чередниченко Олексій Юрійович*** – старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

64. ***Черниш Юлія Олександрівна*** – старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

ПАМ'ЯТКА АВТОРУ

Наукові статті у фахових виданнях повинні мати такі необхідні елементи:

анотація як стисла стаття;

постановка проблеми у загальному вигляді та її зв'язок із важливими науково-практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано розв'язання зазначеної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується стаття;

формулювання мети статті (**постановка наукового завдання**);

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів;

висновки з цього дослідження і **перспективи** подальших досліджень у зазначеному напрямку;

список використаних джерел: 10–15 посилань терміном **не більше 10 років.**

Редакція не рекомендує використання джерел інформації держав-агресорів.

До друку приймаються оригінальні наукові праці, які не було відправлено до інших редакцій та не опубліковано раніше в інших виданнях.

Рукопис статті потрібно подавати разом з наступними документами:

довідка про результати перевірки на академічний плагіат;

акт експертної оцінки про можливість відкритого опублікування (1 примірник);

згода на публікацію статті та оприлюднення персональних даних;

відомості про автора (авторів) за формою: прізвище, ім'я та по батькові; науковий ступінь, вчене звання, посада; назва установи, де працює автор, її місце розташування (місто, країна); обліковий запис автора ORCID, електронна адреса та номер телефону.

Відомості про автора (авторів) подаються окремим супровідним файлом. Наприклад:

№ з/п	Українська мова	Англійська мова
1	**Шевченко Олександр Іванович** Кандидат технічних наук Доцент Старший викладач Військовий інститут телекомунікацій та інформатизації імені Героїв Крут; м. Київ, Україна https://orcid.org/0000-0000-0000-0000 e-mail _____, телефон _____	**Shevchenko Oleksandr** Candidate of Technical Sciences Associate Professor Senior Lecturer Military Institute of Telecommunications and Informatization Technologies named after Heroes of Kruty; Kyiv, Ukraine https://orcid.org/0000-0000-0000-0000

Рукопис подається в друкованому та електронному вигляді у текстовому редакторі Microsoft Word, а також може бути надісланий за електронною адресою: naukaviti@viti.edu.ua, naukaviti@gmail.com.

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, naukaviti@gmail.com.