Міністерство освіти і науки України
Чорноморський національний університет імені Петра Могили

Кваліфікаційна наукова
праця на правах рукопису

Ухань Єгор Олександрович

УДК 004.725.5:004.056

ДИСЕРТАЦІЯ

МЕТОДИ ТА ЗАСОБИ ФОРМУВАННЯ КОНТРОЛЬОВАНИХ ЗОН В БЕЗДРОТОВИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

Спеціальність 123 Комп'ютерна інженерія
Галузь знань 12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____Є. О. Ухань

Науковий керівник Журавська Ірина Миколаївна, д-р техн. наук, професор

Миколаїв – 2026

АНОТАЦІЯ

Ухань Є. О. Методи та засоби формування контрольованих зон в бездротових комп'ютерних мережах**.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія. – Чорноморський національний університет імені Петра Могили, Миколаїв, 2026.

Дисертаційне робота присвячена розв'язанню науково-прикладної задачі підвищення ефективності захисту бездротових комп'ютерних мереж (БКМ) та управління радіопокриттям шляхом розроблення засобів й методів формування та аналізу безпеки контрольованих зон (КЗ). Обґрунтування актуальності роботи пов'язане з вразливістю БКМ до несанкціонованого доступу через поширення сигналу за межі зони фізичного контролю та необхідністю інтеграції фізичних заходів обмеження сигналу з логічними механізмами захисту.

Актуальність дослідження зумовлена необхідністю створення комплексних механізмів формування контрольованих зон (КЗ), які б поєднували фізичні методи обмеження сигналу з логічними та програмними засобами контролю периметра. Використання інтелектуального моніторингу та апаратних засобів корекції покриття, таких як джаммери, дозволяє локалізувати мережевий простір та мінімізувати ризики витоку інформації в умовах динамічного мережевого середовища.

Метою дослідження є підвищення ефективності захисту бездротових комп'ютерних мереж та керованості радіопокриттям шляхом розроблення, удосконалення та розвитку методів формування контрольованих зон та аналізу безпеки, що інтегрують радіотехнічні, логічні та організаційні засоби протидії несанкціонованому доступу.

Об'єкт дослідження – процес формування та функціонування контрольованих зон у локальних бездротових комп'ютерних мережах.

Предмет дослідження: методи (фізичні, логічні, програмні) та засоби (джаммери, WIDS, протоколи безпеки) створення керованого та захищеного бездротового периметра.

Методи дослідження: метод теоретичного аналізу стандартів IEEE 802.11, метод математичного моделювання затухання сигналу (ITU Indoor Model), методи мережевої сегментації (VLAN), методи автентифікації (SAE) та експериментальні методи вимірювання RSSI для оцінки точності меж КЗ.

Наукова новизна отриманих результатів:

– **вперше розроблено** метод позиціонування WiFi-джаммерів, який, на відміну від існуючих, реалізує нормалізацію покриття радіосигналу для формування контрольованої зони, що дозволяє локалізувати сигнал у приміщеннях зі складною геометрією без використання екранування;

– **удосконалено** комбінований метод створення контрольованої зони, який, на відміну від існуючих, поєднує фізичне регулювання потужності передавача та логічну ідентифікацію пристроїв (цифровий відбиток пристрою), що дозволяє підвищити рівень виявлення несанкціонованих точок доступу під час атак типу «злий двійник» до 91,5 %, зберігаючи працездатність системи на рівні 88,5 % у складних завадових середовищах;

– **удосконалено** модель формування контрольованої зони, яка, на відміну від існуючих, реалізує шестиетапний цикл від RF-моделювання до адаптивного управління трафіком, що забезпечує цілісність внутрішнього та зовнішнього периметрів мережі;

– **набув подальшого розвитку** метод аналізу безпеки бездротового зв’язку за стандартами 3-го та 4-го поколінь, який, на відміну від існуючих, використовує штучний інтелект, що дозволяє динамічно змінювати рівні шифрування залежно від виявленого типу загрози.

Практичне значення отриманих результатів полягає у розробленні методики формування та моніторингу КЗ на базі програмно-апаратних засобів, які дозволяють створювати захищені сегменти мережі у корпоративних, промислових та критичних інфраструктурах. Результати реалізовані у вигляді

алгоритмів налаштування маршрутизаторів для стабілізації покриття в межах приміщення; системи WIDS-моніторингу несанкціонованих пристроїв на основі фільтрації MAC-адрес за «білими списками»; методики налаштування спрямованих антен та пересувних джаммерів для адаптивного керування периметром.

Основні результати дисертаційної роботи впроваджено у НДР ЧНУ ім. Петра Могили «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» (№ держ. реєстрації 0121U109898) та у навчальний процес за першим (бакалаврським) рівнем вищої освіти на кафедрі комп'ютерної інженерії Чорноморського національного університету імені Петра Могили при проведенні лекційних занять та лабораторних робіт з дисциплін «Комп'ютерні системи» українською мовою та «Microcontrollers» англійською мовою (Акт впровадження від 04 червня 2025 р.)

Апробація результатів дисертації. Матеріали дисертаційної роботи доповідалися, обговорювалися та отримали схвалення на трьох міжнародних та трьох всеукраїнських науково-практичних конференціях.

Публікації. За темою дисертації опубліковано 11 наукових праць, з них 1 публікація у періодичному науковому виданні, проіндексованому у Scopus, 3 статті у фахових виданнях України категорії Б, 6 тез доповідей на міжнародних та всеукраїнських наукових конференціях, 1 свідоцтво про реєстрацію авторського права на твір.

У вступі обґрунтовано актуальність теми дослідження методів і засобів формування контрольованих зон у бездротових комп'ютерних мережах, показано взаємозв'язок дисертації з науково-дослідною роботою, визначено мету й завдання роботи, описано об'єкт, предмет і застосовані методи дослідження, а також наведено відомості про наукову новизну та практичне значення отриманих результатів. Додатково подано інформацію про особистий внесок здобувача та список опублікованих праць, що відповідають темі дисертаційного дослідження.

Перший розділ присвячено аналізу наявних методів захисту БКМ: встановлено обмеження логічних протоколів щодо атак фізичного рівня та обґрунтовано необхідність переходу до комплексного формування КЗ. Окреслено невирешені проблеми: ідентифікація прихованих вузлів; динамічна адаптація потужності; затримка в Zabbix. Поставлено задачі дослідження.

У другому розділі розроблено методи та засоби формування та керування контрольованими зонами: вперше розроблено математичну модель затухання сигналу (ITU-R P.1238), методи нормалізації покриття, логічну сегментацію мережі через VLAN та особливості автентифікації WPA3 SAE.

У третьому розділі розроблено програмно-апаратні засоби та наведено застосування маршрутизаторів MikroTik CCR2116 як мережевого ядра, інтеграцію моніторингу Zabbix з системою керування базами даних (СКБД) PostgreSQL та створення активного модуля протидії (джаммера) на базі ESP32.

Четвертий розділ присвячений експериментальним дослідженням: проведено калібрування RF-моделі (уточнення коефіцієнтів N = 31,2 та L_f = 11,5 дБ), стабілізації периметра при потужності 8 дБм та оцінку ефективності джаммінгу (час реакції системи – 2,15 с). Узагальнено отримані результати дослідження, що підтвердили ефективність поєднання програмного обмеження потужності та адаптивного пригнічення сигналів для створення захищеного бездротового середовища.

У висновках узагальнено основні результати дослідження та встановлено перспективні напрями використання розроблених та вдосконалених методів, моделей та засобів захисту локальних бездротових мереж.

Ключові слова: *контрольована зона, бездротова комп'ютерна мережа, захист інформації, WiFi-сигнал, джаммер, моніторинг, бази даних, критична інфраструктура, віддалений доступ, мережеве сховище, кібербезпека, шифрування, інструменти тестування безпеки, протоколи автентифікації, аналіз трафіку.*

ABSTRACT

Ukhan Y. O. Methods and means of controlled zones' forming in wireless computer networks. – Qualification scientific work on manuscript rights.

Dissertation for obtaining the Doctor of Philosophy scientific degree in the specialty 123 Computer Engineering (branch of knowledge 12 Information Technologies). – Petro Mohyla Black Sea National University, Mykolaiv, 2026.

The PhD thesis is devoted to solving the scientific and applied problem of increasing the efficiency of wireless computer network (WCN) protection and radio coverage management by developing a conceptual model and methods for forming controlled zones (CZ). The relevance of the work is related to the vulnerability of WCNs to unauthorized access due to signal propagation beyond physical control and the need to integrate physical signal limitation measures with logical security mechanisms developing.

The relevance of the study is determined by the need to create complex mechanisms for forming controlled zones that combine physical signal limitation methods with logical and software perimeter control tools. The use of intelligent monitoring and hardware coverage correction tools, such as jammers, allows for localizing network space and minimizing data leakage risks in a dynamic network environment.

Object of research is the process of forming and functioning of controlled zones in local wireless computer networks.

Subject of research are the methods (physical, logical, software) and means (jammers, WIDS, security protocols) for creating a managed and protected wireless perimeter.

Research methods method of theoretical analysis of IEEE 802.11 standards, method of mathematical modeling of signal attenuation (ITU indoor model), network segmentation methods (VLAN), authentication methods (SAE) and experimental RSSI measurement methods to assess the accuracy of short circuit limits.

Scientific novelty of the obtained results

For the first time:

The method for positioning WiFi jammers, which, unlike existing ones, implements normalization of radio signal coverage to form a controlled zone, which allows localizing the signal in rooms with complex geometry without using shielding.

Improved:

The combined method for creating a controlled zone, which, unlike existing ones, combines physical control of transmitter power and logical identification of devices (digital fingerprint of the device), which allows increasing the detection rate of unauthorized access points during "evil double" attacks to 91.5%, while maintaining system performance at 88.5% in complex interference environments.

Improved:

The model for forming a controlled area, which, unlike existing ones, implements a six-stage cycle from RF modeling to adaptive traffic management, ensuring the integrity of the internal and external perimeters of the network.

Have been developed further:

The method for analyzing wireless security according to 3rd and 4th generation standards, which, unlike existing ones, uses artificial intelligence, which allows you to dynamically change encryption levels depending on the type of threat detected.

Practical value of the results:

The developed CZ formation method allows for the creation of protected network segments in corporate, industrial, and critical infrastructures. The results are implemented as algorithms for configuring routers to stabilize coverage within premises; a WIDS monitoring system for unauthorized devices based on MAC address filtering using "white lists"; methodologies for using directional antennas and mobile jammers for adaptive perimeter management.

The main scientific results of the dissertation work have been implemented in the R&D project of Petro Mohyla BSNU "Development of automation modules for wireless recovery devices for post-infarction, post-stroke patients in individual conditions of remote rehabilitation" (State Reg. No. 0121U109898).

Approbation of dissertation results: Materials of the dissertation work were reported, discussed, and approved at 3 international and 3 all-Ukrainian scientific and technical conferences.

Publications: 11 scientific works have been published on the topic of the dissertation, including 1 publication in a periodic scientific edition indexed in Scopus, 3 articles in specialized editions of Ukraine (Cat. B), 6 abstracts of reports at the scientific conferences, and 1 certificate of copyright registration for a work.

The introduction substantiates the relevance of the research topic, shows the connection of the dissertation with research projects, defines the purpose and tasks of the work, describes the object, subject, and applied research methods, and provides information about the scientific novelty and practical significance of the results. Additionally, information on the author's personal contribution and a list of published works corresponding to the topic of the dissertation research are provided.

The first chapter is devoted to the analysis of existing methods of BKM protection: limitations of logical protocols regarding physical layer attacks are established and the need for a transition to complex formation of the CC is justified. Unsolved problems are outlined: identification of hidden nodes; dynamic power adaptation; delay in Zabbix. Research tasks are set.

The second chapter develops methods and tools for the formation and management of controlled zones: a mathematical model of signal attenuation (ITU-R P.1238) has been developed for the first time, along with methods for coverage normalization, logical network segmentation via VLAN, and the specific features of WPA3 SAE authentication.

The third chapter software and hardware means were developed and the use of MikroTik CCR2116 routers as a network core, integration of Zabbix monitoring with the PostgreSQL database management system (DBMS), and creation of an active countermeasure module (jammer) based on ESP32 were presented.

The fourth chapter devoted to experimental research: calibration of the RF model was performed (refining coefficients $N = 31.2$ and $L_f = 11.5$ dBm), the perimeter was stabilized at a power of 8 dBm, and the effectiveness of jamming was evaluated

(system reaction time – 2.15 s). The obtained results are summarized, confirming the effectiveness of the combination of software power limitation and adaptive signal suppression for creating a secure wireless environment.

The conclusions summarize the results, which confirmed the effectiveness of combining software power limitation and adaptive signal suppression to create a protected wireless environment. The conclusions summarize the main results of the research and identify promising directions for the the developed and improved methods, models, and means.

Keywords: controlled zone, wireless computer network, information protection, WiFi signal, jammer, monitoring, databases, critical infrastructure, remote access, network storage, cybersecurity, encryption, security testing tools, authentication protocols, traffic analysis.

СПИСОК ОПУБЛІКОВАНИХ НАУКОВИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

1. Burlachenko I. S., Zhuravska I. M., Ukhan Y. O., Tohoiev O. R., Tiutiunyk Y. I. Multi-agent monitoring system for heat loss mapping of multi-story buildings. *CEUR Workshop Proceedings*. 2019. Vol. 2516. P. 218–225. ISSN 1613-0073. URL: http://ceur-ws.org/Vol-2516/ (Last accessed: 14.12.2019).

2. Ухань Є. О., Журавська І. М. Концептуальна модель формування контрольованої зони в бездротових комп'ютерних мережах. *Наука і техніка сьогодн*і. 2026. Вип. 2 (56). С. 2336–2347. DOI: 10.52058/2786-6025-2026-2(56)-2336-2347. ISSN 2786-6025.

3. Ухань Є. О. Методи та засоби моделювання зон покриття Wi-Fi та впливу інтерференції на якість сигналу. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво :* наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 60. С. 312–317. DOI: 10.36910/6775-2524-0560-2025-60-33. ISSN 2524-0552.

4. Ухань Є. О., Журавська І. М. Формування контрольованих зон

у локальних бездротових комп’ютерних мережах. *Комп’ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 59. С. 241–246. DOI: 10.36910/6775-2524-0560-2025-59-30. ISSN 2524-0552.

Праці, які засвідчують апробацію матеріалів дисертації

5. Ухань Є. О., Журавська І. М. Аналіз можливостей використання штучного інтелекту для захисту бездротових комп'ютерних мереж. *Сучасні Інформаційні Технології –2025* : матеріали XV Міжнар. наук. конф., Одеса, 15–16 травня 2025 р. Нац. ун-т “Одеська політехніка” / Одеса : Наука і техніка, 2025. С. 212–214. URL: https://ics_conf.tilda.ws/ukr#rec41121601, https://drive.google.com/drive/folders/1uXN7b84231YhSfT_tY6I9eMhPjDrIBKJ (дата звернення: 10.05.2025).

6. Ухань Є. О. Модель WiFi-мережі на базі технології 802.11ad. *Могилянські читання – 2024* : тези доп. XXVII Всеукр. наук.-практ. конф., Миколаїв, 6–10 листоп. 2024 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2024. С. 140–143. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/2507 (дата звернення: 27.04.2025).

7. Ухань Є. О. Математична модель позиціонування WiFi-джаммерів для формування контрольованої зони у сегменті локальної мережі. *Ольвійський форум – 2024: стратегії країн Причорноморського регіону в геополітичному просторі :* тези доп. XXI Міжнар. наук. конф., Миколаїв, 20–23 черв. 2024 р. Миколаїв : ЧНУ ім. Петра Могили, 2024. С. 209–211. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/2349 (дата звернення: 27.04.2025).

8. Ухань Є. О. Бездротова локальна мережа на каналі 60 ГГц для побудови контрольованої зони. *Могилянські читання – 2023 :* тези доп. XXVI Всеукр. наук.-метод. конф. Миколаїв, 6–10 листоп. 2023 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2023. С. 449–450. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/1869 (дата звернення: 27.04.2025).

9. Ухань Є. О., Журавська І. М. Пересувні захисні джаммери для формування контрольованої зони. *Free and Open Source Software (FOSS-2023)* : тези доп. XIV Міжнар. наук.-практ. конф., Харків, 07–10 лютого 2023 р. Харків : ХНЕУ ім. Семена Кузнеця, 2023. С. 103–105. URL: http://repository.hneu.edu.ua/bitstream/123456789/29041/1/foss-2023-theses.pdf (дата звернення: 27.04.2025).

10. Ухань Є. О. Захисні джаммери для формування контрольованої зони. *Могилянські читання – 2022* : тези доп. XXV Всеукр. наук.-практ. конф., Миколаїв, 07–11 листоп. 2022 р. Миколаїв : ЧНУ ім. Петра Могили, 2022. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/595 (дата звернення: 27.04.2025).

Публікації, які додатково відображають наукові результати дисертації

11. Свідоцтво про реєстрацію авторського права на твір 107427. Комп'ютерна програма «Складання Wi-Fi-мапи переміщення пацієнтів територією реабілітаційного центру» / О. Р. Тогоєв, В. Д. Веселовський, О. В. Дворник, І. М. Журавська, К. О. Обухова, Є. О. Ухань ; дата реєстр. 17.08.2021, Бюл. № 66.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 15
ВСТУП 16
РОЗДІЛ 1 АНАЛІЗ СТАНУ ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ 21
1.1 Аналіз існуючих методів захисту бездротових комп'ютерних мереж 21
1.2 Аналіз методів фізичного обмеження зони покриття БКМ 24
1.3 Активні методи захисту: інтелектуальні системи завад 26
1.4 Моделювання радіочастотного середовища як інструмент проєктування КЗ 28
Висновки до розділу 1 28
Список використаних джерел до розділу 1 30
РОЗДІЛ 2 МЕТОДИ НАЛАШТУВАННЯ ТА КЕРУВАННЯ КОНТРОЛЬОВАНИМИ ЗОНАМИ 37
2.1 Метод позиціонування WiFi-джаммерів та нормалізації покриття радіосигналу 37
2.1.1 Математична модель оцінки затухання сигналу 37
2.1.2 Метод нормалізації сигналу 41
2.2 Метод логічного сегментування та динамічної автентифікації 43
2.2.1 Сегментація мережі на рівні довіри 43
2.2.2 Автентифікація за протоколом WPA3 45
2.3 Метод інтелектуального моніторингу WIDS/WIPS та протидії загрозам 47
2.3.1 Критерії аналізу та виявлення загроз 47
2.3.2 Механізми протидії 48
2.4. Перспективні методи керування 49
2.4.1 Використання динамічних карт радіосередовища 50
2.4.2 Метод «мережевої мімікрії» 50
2.4.3 Оцінка ризику на основі Machine Learning 51
Висновки до розділу 2 51

Список використаних джерел до розділу 2 52
РОЗДІЛ 3 РОЗРОБКА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ФОРМУВАННЯ ТА МОНІТОРИНГУ КОНТРОЛЬОВАНИХ ЗОН 55
3.1 Апаратна реалізація системи керування периметром 55
3.1.1 Центральний вузол керування (MikroTik CCR2116-12G-4S+) 56
3.1.2 Периферійне радіообладнання (MikroTik RB951Ui-2HnD) 57
3.2 Програмне забезпечення та алгоритми обробки сигналів 59
3.2.1 Інтеграція моніторингу через вебінтерфейс Zabbix 59
3.2.2 Розробка методу побудови джаммера на модулі ESP32 60
3.3 Розробка методу мережевої взаємодії та інтеграція моніторингу Zabbix 60
3.3.1 Механізм збору та агрегації даних 61
3.3.2 Алгоритмічне порівняння RSSI та математичної моделі 62
3.3.3 Візуалізація та управління «сірими зонами» 64
3.4 Засоби активної протидії на базі ESP32 65
3.4.1 Апаратна архітектура та складові модуля 65
3.4.2 Програмна логіка та алгоритм функціонування 67
Висновки до розділу 3 69
Список використаних джерел до розділу 3 69
РОЗДІЛ 4 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ФОРМУВАННЯ КОНТРОЛЬОВАНИХ ЗОН 73
4.1 Методологія тестування та опис експериментального стенду 73
4.1.1 Склад та конфігурація експериментального стенду 73
4.1.2 Детальна методика тестування 76
4.1.3 Організація збору даних у PostgreSQL 78
4.2 Дослідження точності локалізації та стабілізації межі зони 81
4.2.1 Підготовчий етап: Конфігурація середовища 81
4.2.2 Калібрування та емпірична валідація моделі 82
4.2.3 Стабілізація периметра та КЗ 83
4.2.4 Активна протидія та аналіз перехідних процесів 86
4.3 Оцінка ефективності глушіння несанкціонованих пристроїв 90

4.3.1 Аналіз енергетичного пригнічення сигналу атакуючого пристрою 90
4.3.2 Оцінювання вибірковості та впливу на QoS легітимних користувачів . 91
4.3.3 Оцінювання вибірковості та впливу на QoS легітимних користувачів . 91
Висновки до розділу 4 92
Список використаних джерел до розділу 4 93
ВИСНОВКИ 95
ДОДАТОК А Акти впровадження 97
А.1 Акт впровадження результатів дисертації в НДР 97
А.2 Акт впровадження результатів дисертації в навчальний процес 98
ДОДАТОК Б Код прошивки для активної протидії 99
Б.1 Код прошивки для активної протидії 99
Б.2 Код прошивки для моніторингу радіопокриття 102
ДОДАТОК В Налаштування спрямованих антен та пересувних джаммерів для адаптивного керування периметром 105
ДОДАТОК Г Схемотехнічні рішення апаратно-програмних засобів 111
ДОДАТОК Д Список публікацій здобувача 113

ПЕРЕЛІК СКОРОЧЕНЬ

НСД	– несанкціонований доступ
ОС	– несанкціонований доступ
ПЗ	– програмне забезпечення
СКБД	– система керування базами даних
ТД	– точка доступу
AP	– Access Point
BBS	– Basic Service Set
IEEE	– Institute of Electrical and Electronics Engineers
ML	– Machine Learning
QoE	– Quality of Experience
QoS	– Quality of Service
SSID	– Service Set IDentifier
UP	– Uplink Port
USB	– Universal Serial Bus
WDS	– Wireless Distributed System
WEP	– Wired Equivalent Privacy
Wi-Fi	– Wireless Fidelity
WPA	– Wi-Fi Protected Access

ВСТУП

Обґрунтування вибору теми дослідження

Розвиток сучасних бездротових технологій та зростання кількості мобільних пристроїв створюють нові виклики для забезпечення інформаційної безпеки в локальних мережах. Бездротові комп'ютерні мережі (БКМ) за своєю природою є вразливими до несанкціонованого доступу (НСД) через поширення радіосигналу за межі фізичного контролю організації. Традиційні методи захисту, такі як лише парольна автентифікація, виявляються недостатніми проти сучасних атак типу KRACK або створення фальшивих точок доступу (Evil Twin).

Актуальність дослідження зумовлена необхідністю створення комплексних механізмів формування контрольованих зон (КЗ), які б поєднували фізичні методи обмеження сигналу з логічними та програмними засобами контролю периметра. Використання інтелектуального моніторингу та апаратних засобів корекції покриття, таких як джаммери, дозволяє локалізувати мережевий простір та мінімізувати ризики витоку інформації в умовах динамічного мережевого середовища.

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконувалася у відповідності до завдань науково-дослідної роботи ЧНУ ім. Петра Могили «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» (№ держ. реєстрації 0121U109898, 2021–2022 рр.), в якій здобувач брав участь як виконавець.

Мета та завдання дослідження

є підвищення ефективності захисту бездротових комп'ютерних мереж та керованості радіопокриттям шляхом розроблення, удосконалення та розвитку методів формування контрольованих зон та аналізу безпеки, що інтегрують радіотехнічні, логічні та організаційні засоби протидії несанкціонованому доступу.

Для досягнення поставленої мети визначено наступні **задачі дослідження**:

1) проаналізувати недоліки існуючих методів формування контрольованої зони та обґрунтувати необхідність переходу до комплексного шестиетапного циклу управління на основі запропонованої моделі, що охоплює етапи від RF-моделювання до адаптивного контролю трафіку (QoS/QoE);

2) розробити математичний метод оптимального позиціонування Wi-Fi-джаммерів для формування КЗ у приміщеннях зі складною геометрією, яка забезпечує локалізацію сигналу без застосування фізичного екранування стін;

3) удосконалити комбінований метод створення КЗ, за рахунок інтеграції фізичного регулювання потужності передавачів із механізмом логічної ідентифікації пристроїв (FingerPrinting) для підвищення точності виявлення атак типу «злий двійник»;

4) експериментально перевірити розроблені методи та удосконалені методи в умовах складного завадового середовища та загальної працездатності системи.

Об’єкт дослідження

Процес формування та експлуатації контрольованих зон у локальних бездротових комп’ютерних мережах для забезпечення їх захисту.

Предмет дослідження

Методи (фізичні, логічні, програмні) та інструментальні засоби (джаммери, WIDS, протоколи безпеки) захисту бездротових комп’ютерних мереж.

Методи дослідження

У роботі використано комплекс наукових методів: теоретичний аналіз стандартів IEEE 802.11, математичне моделювання затухання сигналу (ITU indoor модель), методи мережевої сегментації (VLAN), алгоритми автентифікації (SAE) та експериментальні методи вимірювання RSSI для оцінки точності меж КЗ.

Наукова новизна отриманих результатів:

– **вперше розроблено** метод позиціонування WiFi-джаммерів, який, на відміну від існуючих, реалізує нормалізацію покриття радіосигналу для формування контрольованої зони, що дозволяє локалізувати сигнал у приміщеннях зі складною геометрією без використання екранування;

– **удосконалено** комбінований метод створення контрольованої зони, який, на відміну від існуючих, поєднує фізичне регулювання потужності передавача та логічну ідентифікацію пристроїв (цифровий відбиток пристрою), що дозволяє підвищити рівень виявлення несанкціонованих точок доступу під час атак типу «злий двійник» до 91,5 %, зберігаючи працездатність системи на рівні 88,5 % у складних завадових середовищах;

– **удосконалено** модель формування контрольованої зони, яка, на відміну від існуючих, реалізує шестиетапний цикл від RF-моделювання до адаптивного управління трафіком, що забезпечує цілісність внутрішнього та зовнішнього периметрів мережі;

– **набув подальшого розвитку** метод аналізу безпеки бездротового зв'язку за стандартами 3-го та 4-го поколінь , який, на відміну від існуючих, використовує штучний інтелект, що дозволяє динамічно змінювати рівні шифрування залежно від виявленого типу загрози.

Практичне значення отриманих результатів

Розроблений метод формування КЗ дозволяє створювати захищені сегменти мережі у корпоративних, промислових та критичних інфраструктурах. Результати реалізовані у вигляді:

– алгоритмів налаштування маршрутизаторів для стабілізації покриття в межах приміщення;

– системи WIDS-моніторингу несанкціонованих пристроїв на основі фільтрації MAC-адрес за «білими списками»;

– методики налаштування спрямованих антен та пересувних джаммерів для адаптивного керування периметром (додаток Г).

Основні результати дисертаційної роботи впроваджено:

– у НДР ЧНУ ім. Петра Могили «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» (№ держ. реєстрації 0121U109898). Акт впровадження наведено в додатку А.1;

– у навчальний процес на кафедрі комп’ютерної інженерії ЧНУ ім. Петра Могили при проведенні лекційних та практичних занять при викладанні дисциплін «Комп’ютерні системи» українською мовою та «Microcontrollers» англійською мовою здобувачам спеціальності 123 Комп’ютерна інженерія за першим (бакалаврським) рівнем вищої освіти. Акт впровадження наведено в додатку А.2;

Особистий внесок здобувача

Основні наукові результати, висновки та рекомендації, які наведені у дисертації та виносяться на захист, отримано автором самостійно та опубліковано в 11 наукових працях, з яких 5 одноособових: [3], [6–8], [10]. У роботах, опублікованих у співавторстві, авторові належать такі теоретичні та практичні положення, відображені у характеристиці наукової новизни отриманих результатів, а саме:

– у роботах [1; 9] описано розробку апаратно-програмного комплексу на базі маршрутизаторів MikroTik (ядро CCR2116 та периферія RB951Ui) та мікроконтролерів ESP32 для активної протидії загрозам та автоматизованого моніторингу параметрів RSSI в реальному часі;

– у роботі [2] розроблено модель формування контрольованої зони (КЗ), яка, на відміну від існуючих, реалізує шестиетапний цикл від RF-моделювання до адаптивного управління трафіком (QoS/QoE), що забезпечує цілісність як внутрішнього, так і зовнішнього периметра мережі;

– у роботі [4] запропоновано метод позиціонування WiFi-джаммерів для формування контрольованої зони, що дозволяє локалізувати сигнал у приміщеннях зі складною геометрією без використання екранування;

– у роботі [5] набув подальшого розвитку метод аналізу безпеки бездротового зв’язку за стандартами 3 го та 4-го поколінь за рахунок використання штучного інтелекту для динамічної зміни рівнів шифрування залежно від виявленого типу загрози;

– у роботі [11] здобувачу належить удосконалення комбінованого методу

створення контрольованої зони шляхом поєднання фізичного регулювання потужності передавача та логічної ідентифікації пристроїв (цифрового відбитку пристрою).

Апробація результатів дисертації

Матеріали дисертаційної роботи доповідалися, обговорювалися та отримали схвалення на науково-технічних конференціях та семінарах:

– XXI Міжнародна науково-практична конференція «Ольвійський форум» (Миколаїв, 2024);

– XV Міжнародна науково-практична конференція «*Сучасні Інформаційні Технології*» (Одеса, 2025);

– XIV Міжнародна науково-практична конференція «Free and Open Source Software» (Харків, 2023);

– Всеукраїнська науково-практична конференція «Могилянські читання» (Миколаїв, 2022, 2023, 2024).

Публікації

За темою дисертації опубліковано 11 наукових праць, з них 1 публікація у періодичному науковому виданні, проіндексованому у Scopus, 3 статті у фахових виданнях України категорії Б, 6 тез доповідей на міжнародних та всеукраїнських наукових конференціях, 1 свідоцтво про реєстрацію авторського права на твір (додаток Д).

Структура та обсяг дисертації

Робота складається зі вступу, чотирьох розділів, висновків та п’яти додатків. Загальний обсяг дисертації становить 115 сторінок, містить 22 рисунки та 10 таблиць. Список використаних джерел містить 133 найменування.

РОЗДІЛ 1
АНАЛІЗ СТАНУ ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

Стрімкий розвиток бездротових технологій передачі даних та їх інтеграція в усі сфери діяльності – від критичної інфраструктури до корпоративного сектору – висуває нові, більш жорсткі вимоги до систем захисту інформації. Бездротові комп'ютерні мережі (БКМ) за своєю фізичною природою є відкритими системами, де середовище поширення сигналу не обмежене фізичним периметром об’єкта, що створює передумови для несанкціонованого доступу (НСД) до даних, радіорозвідки та деструктивних завадових впливів [1–3].

1.1 Аналіз існуючих методів захисту бездротових комп’ютерних мереж

Забезпечення конфіденційності та цілісності даних у БКМ залишається однією з найскладніших задач сучасної кібербезпеки [4–5]. Основна вразливість БКМ зумовлена фізичною природою середовища поширення сигналу: радіоефір є відкритим для перехоплення, аналізу та деструктивного впливу з боку зловмисника, що знаходиться поза межами фізичного периметра об'єкта (рис. 1.1).

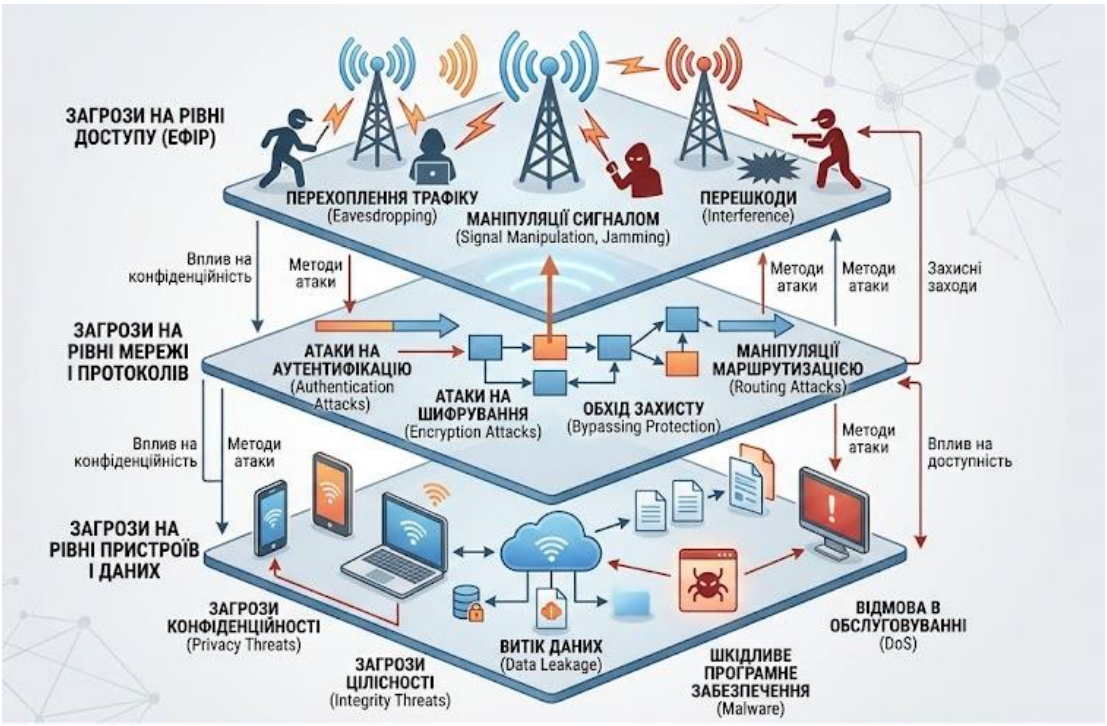

Рисунок 1.1 – Модель загроз у бездротовому середовищі за межами фізичного контролю

Традиційні методи захисту, такі як протоколи шифрування та автентифікації, спрямовані на логічний рівень моделі OSI. Проте вони виявляються недостатніми проти атак фізичного рівня (L1):

– DoS-атаки та навмисні завади: блокування каналу зв'язку шляхом генерації шуму [6; 7];

– Eavesdropping (укр. підслуховування): можливість збору пакетів для подальшого офлайн-злому паролів або аналізу трафіку [8; 9];

– атаки типу «людина посередині» (англ. Man-in-the-Middle, MitM): створення фальшивих точок доступу (англ. Rogue AP) з вищою потужністю сигналу [10; 11].

Мережева аутентифікація давно є стандартом у кожній точці доступу та маршрутизаторі. Існують чотири версії протоколу безпеки для захисту бездротових мереж Wi-Fi Protected Access (WPA): WPA, WPA2, WPA3, WPA4 (табл. 1.1). На сьогодні більшість пристрої працюють на WPA2, який не надає надійного захисту та має багато недоліків з боку безпеки [12; 13].

Головною загрозою з 2017 р. для цього протоколу є атаки з переустановленням ключа (англ. Key Reinstallation Attack, KRACK). Під час такої атаки пристрій підключається до Wi-Fi через захищений WPA2. Перевірка відбувається через процес «4 way handshake» – процес обміну чотирма повідомленнями між точкою доступу (автентифікатором) і клієнтським пристроєм (заявником) для створення деяких ключів шифрування, які можна використовувати для шифрування фактичних даних, надісланих через бездротове середовище [14; 15]. Під час цього обміну зловмисник має можливість перехопити й повторно пройти частину процесу, що може привести до перехоплення даних: логін, паролі та ін. [16; 17].

Таблиця 1.1 – Порівняння стандартів захисту технології Wi-Fi

Характеристика	**WPA**	**WPA2**	**WPA3**	**WPA4**
Рік випуску	2003	2004	2018	2026–2028
Ключ шифрування, біт	64	128	192 / 256	256
Протокол аутентифікації	TKIP+RC4	802.1X / EAP	SAE	NIST, Zero Trust [18]
Захист від розподілених атак на відмову в обслуговуванні (DDoS)	Відсутній	Відсутній	Є	Є (за рахунок ШІ для аналізу та активної протидії)
Захист від атак перехоплення (англ. Man-in-the-Middle)	Відсутній	Відсутній	Захист за допомогою аутентифікації на основі обміну пакетами	Динамічна зміна рівнів шифрування в залежності від типу атаки [19]
Підтримка застосування на пристроях, випущених до 2018 р.	Відсутня	Відсутня	Можливість роботи в режимі «WPA3-перехід» для підтримки пристроїв, випущених до 2018 р.	Не визначено; технологія ще у розробці

Для захисту від KRACK-атак у 2018 р. було створено протокол безпеки WPA3, який використовує новий тип шифрування SAE (Simultaneous Authentication of Equals) [20–22]. В зазначеному методі одночасної рівноправної автентифікації кожна сесія індивідуально шифрується для захисту

від перехоплення даних. Головною складністю для введення у роботу WPA3 є відсутність даного протоколу на пристроях, які розроблені до 2018 р. [23].

У 2019 р. була сформована робоча група IEEE 802.11be, яка досліджує та аналізує новітні технології Wi-Fi 7 та WPA4 [24; 25].

Відміною WPA4 від попередніх версій протоколу стануть новітні рішення у механізмах аутентифікації та безпеки. Головним інструментом є впровадження більш просунутих технологій шифрування, які будуть базуватися на квантових обчисленнях. Для протидії DDoS-атакам досліджується можливість використання штучного інтелекту (ШІ) [26–28], який буде аналізувати атаку та чинити активну протидію. Також у WPA4 планується спростити процес підключення й при цьому підвищити рівень безпеки. Головним інструментом, як вважають дослідники, стане покращений принцип криптографії з відкритим ключем.

Дослідники вважають, що WPA4 зможе вирішити проблеми, пов'язані з атаками погодження часу, пам'яті та даних (англ. Time Memory Trade Off, TMTO).

Еволюція засобів радіоелектронної розвідки вимагає переходу від виключно програмно-криптографічних методів до комплексного формування контрольованих зон (КЗ) – простору, в якому параметри електромагнітного поля (ЕМП) строго регламентовані, а вихід сигналу за межі якого мінімізований або маскується.

1.2 Аналіз методів фізичного обмеження зони покриття БКМ

Традиційно формування контрольованих зон досягається шляхом фізичного екранування приміщень або використання пасивних засобів захисту. Основні підходи включають (рис. 1.2):

– пасивне екранування: використання радіопоглинаючих матеріалів, металевих сіток (кліток Фарадея) та спеціальних фарб [29];

– керування потужністю передавача (TPC): програмне зниження амплітуди сигналу до мінімально необхідного рівня для стабільного зв'язку в межах офісу [30];

– використання спрямованих антен: фокусування енергії в межах робочих зон [31–33].

Рисунок 1.2 – Класифікація методів формування територіально обмежених бездротових мереж

Проте ці методи мають суттєві недоліки (табл. 1.2):

– висока вартість та складність монтажу пасивних екранів, що часто неможливо в орендованих офісах або історичних будівлях;

– дифракція та перевідбиття: радіохвилі здатні огинати перешкоди та проникати через вікна чи вентиляційні канали, створюючи зони витоку («пелюстки» сигналу) за межами КЗ;

– негнучкість: пасивні засоби не адаптуються до змінної радіообстановки або появи нових джерел завад [34; 35].

Аналіз даних, наведених у табл. 1.2, свідчить про те, що жоден із традиційних підходів до захисту не може вважатися універсальним для сучасних умов експлуатації бездротових мереж. Оскільки пасивне екранізування виявляється надто негнучким і затратним, а виключно програмне регулювання потужності (TPC) не завжди ефективно компенсує ефекти дифракції та відбиття, постає необхідність у розробці комбінованого рішення.

Таблиця 1.2 – Порівняльна таблиця методів пасивного та активного формування контрольованих зон

Параметр	**Пасивне екранування**	**Керування потужністю (TPC)**	**Активне зашумлення (Jaming)**
Стійкість до перехоплення	Висока	Середня	Дуже висока
Складність впровадження	Дуже висока	Низька	Середня
Гнучкість налаштувань	Відсутня	Висока	Висока
Вартість експлуатації	Низька	Мінімальна	Середня

Поєднання динамічного керування параметрами радіосигналу на рівні точок доступу з вибірковим застосуванням адаптивного зашумлення (Jamming) у так званих «сірих зонах» витоку сприяє досягненню підвищеної стійкості до перехоплення. Така концепція надає можливість гнучко налаштовувати заходи захисту відповідно до специфіки архітектури приміщення, водночас утримуючи оптимальний баланс між витратами впровадження та фактичним рівнем інформаційної безпеки контрольованої зони.

1.3 Активні методи захисту: інтелектуальні системи завад

Як альтернатива пасивним методам, перспективним напрямком є використання систем активного радіозашумлення. Сучасна парадигма захисту зміщується від «глухого» зашумлення всього спектра до створення смарт-джаммерів (smart jammers) [36–38].

Основні концепції активного формування КЗ (рис. 1.3):

– синхронне глушіння: генерація завади лише в моменти передачі

критичних пакетів даних [39];

– просторово-селективне глушіння: використання технологій Beamforming для спрямування завади саме в бік потенційного зловмисника, не погіршуючи якість зв’язку для легітимних користувачів [40];

– Friendly Jamming: використання авторизованих пристроїв-завад, які координуються з точкою доступу для маскування структури сигналу від несанкціонованих приймачів [41; 42].

Рисунок 1.3 – Інформаційна модель інтелектуальної системи формування контрольованої зони

Проблеми впровадження активних методів:

– взаємний вплив: ризик зниження пропускної здатності власної мережі через високий рівень шуму [43,44];

– електромагнітна сумісність (EMC): необхідність дотримання норм законодавства щодо використання радіочастотного ресурсу [45];

– складність моделювання: важко передбачити динамічну зміну кордонів КЗ в умовах багатопроменевого поширення сигналу в закритих приміщеннях.

1.4 Моделювання радіочастотного середовища як інструмент проєктування КЗ

Для ефективного формування контрольованої зони необхідно мати точну математичну модель поширення сигналу в конкретних умовах у приміщенні (англ. Indoor Modeling). Більшість існуючих рішень стикаються з проблемами точності обчислень у реальному часі [46].

По-перше, проблема все направленості сигналу. Відбиття від стін, меблів та рухомих об'єктів створює складну інтерференційну картину, де зони «тіні» можуть раптово ставати зонами впевненого прийому за межами контрольованого периметра [47; 48].

По-друге, обчислювальна складність. Використання методів трасування променів (англ. Ray Tracing) для великих об'єктів вимагає значних ресурсів, що ускладнює створення адаптивних систем, які б реагували на зміну середовища миттєво [49; 50].

По-третє, необхідність автоматизації. Потрібні інструменти, які дозволяють інтегрувати результати радіопланування безпосередньо в алгоритми керування активними засобами захисту (джаммерами та антенами), створюючи «дихаючі» межі КЗ залежно від поточної загрози [51,52].

Висновки до розділу 1

В розділі проведений аналіз сучасного стану захисту бездротових комп’ютерних мереж демонструє, що існуючі стандарти логічного рівня, зокрема

WPA3, не здатні повноцінно протидіяти загрозам фізичного рівня, таким як активне перехоплення даних та атаки на відмову в обслуговуванні. Концепція «дифузного периметра», зумовлена фізичною природою поширення радіохвиль, у поєднанні з доступністю технологій програмно-визначеного радіо (англ. Software Defined Radio, SDR), робить традиційні методи захисту недостатніми. При цьому класичні пасивні методи формування контрольованих зон є надто статичними, дорого вартісними та не забезпечують необхідної гнучкості в умовах динамічної радіо обстановки.

Це обґрунтовує необхідність розробки нових адаптивних підходів, що базуються на інтелектуальному керуванні параметрами радіоефіру [53,54]. Поєднання методів предикативного динамічного моделювання радіочастотного середовища з використанням смарт-джаммерів дозволяє створити систему з синергетичним ефектом яка забезпечує територіальну ізоляцію сигналу та активне маскування інформативного випромінювання без деградації продуктивності основної мережі.

Виходячи з результатів проведеного аналізу, для вирішення проблем сформульовано такі задачі:

1) проаналізувати недоліки існуючих методів формування контрольованої зони та обґрунтувати необхідність переходу до комплексного шестиетапного циклу управління на основі запропонованої моделі, що охоплює етапи від RF-моделювання до адаптивного контролю трафіку (QoS/QoE);

2) розробити математичний метод оптимального позиціонування Wi-Fi-джаммерів для формування КЗ у приміщеннях зі складною геометрією, яка забезпечує локалізацію сигналу без застосування фізичного екранування стін;

3) удосконалити комбінований метод створення КЗ, за рахунок інтеграції фізичного регулювання потужності передавачів із механізмом логічної ідентифікації пристроїв (FingerPrinting) для підвищення точності виявлення атак типу «злий двійник»;

4) експериментально перевірити розроблені методи та удосконалені методи в умовах складного завадового середовища та загальної працездатності

системи.

Результати дослідження першого розділу опубліковані в роботах [42; 43; 50].

Список використаних джерел до розділу 1

1. ADFL: Defending backdoor attacks in federated learning via adversarial distillation / C. Zhu et al. *Computers & Security*. 2023. Vol. 132. P. 103366. DOI: 10.1016/j.cose.2023.103366 (дата звернення: 25.04.2025).

2. Anju-man-ara. A literature review on Yagi Uda antenna: Old but still used in communities. *International Journal* of *Research* and *Scientific Innovation*. 2025. Vol. XII, Is. VII. P. 510–515. DOI: 10.51244/IJRSI.2025.120700051.

3. Assessing fingerprinting and machine learning approaches for wireless indoor localization / A. R. Pratama, et al. *Indonesian Journal of Electrical Engineering and Computer Science*. 2025. Vol. 37, No. 3. P. 2021. DOI: 10.11591/ijeecs.v37.i3.pp2021-2031.

4. Burlachenko I. S., Savinov V. Yu., Tohoiev O. R., Zhuravska I. M. The cloud GNSS data fusion approach based on multi-agent authentication protocols' analysis in the corporate logistics management systems. *Radio Electronics, Computer Science, Control* [ed.: S. Subbotin]. 2021. Vol. 4. P. 95–105.

5. Chernyshev M., Baig Z., Doss R. R. M. Towards large language model (LLM) forensics using LLM-based invocation log analysis. *CCS '24: ACM SIGSAC Conference on Computer and Communications Security,* Salt Lake City UT USA. New York, NY, USA, 2023. P. 89–96. DOI: doi.org/10.1145/3689217.3690616 (дата звернення: 27.04.2025).

6. Deep learning based RF fingerprinting for device identification and wireless security / Q. Wu, et al. *Electronics letters.* 2018. Vol. 54, No. 24. P. 1405–1407. DOI: 10.1049/el.2018.6404.

7. Design documentation – Model library. ns-3 | a discrete-event network simulator for internet systems. URL: https://www.nsnam.org/docs/models/html/wifi-design.html?utm_source=chatgpt.com (Last accessed: 15.08.2025).

8. Dong L., Wang H.-M., Xiao H. Secure cognitive radio communication via intelligent reflecting surface. *IEEE Transactions on Communications*. 2021. Vol. 69, No. 7. P. 4678–4690. DOI: 10.1109/tcomm.2021.3073028.

9. Guri M., Zadov B., Elovici Y. ODINI: Escaping sensitive data from Faraday-caged, air-gapped computers via magnetic fields. *IEEE Transactions on Information Forensics and Security*. 2020. Vol. 15. P. 1190–1203. DOI: 10.1109/tifs.2019.2938404 (дата звернення: 25.04.2025).

10. Halbouni A., Ong L.-Y., Leow M.-C. Wireless security protocols WPA3: a systematic literature review. *IEEE Access*. 2023. P. 1. DOI: 10.1109/access.2023.3322931 (дата звернення: 22.04.2025).

11. Huang B., Yao H., Wu Q. B. Prediction and evaluation of wireless network data transmission security risk based on machine learning. *Wireless Networks*. 2024. DOI: 10.1007/s11276-024-03773-7 (Last accessed: 25.04.2025).

12. Indira Reddy B., Srikanth V. Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2019. P. 28–35. DOI:/10.32628/cseit1953127 (дата звернення: 27.03.2025).

13. Intelligent reflecting surface-aided spectrum sensing for cognitive radio / S. Lin та ін. *IEEE Wireless Communications Letters*. 2022. P. 1. DOI: 10.1109/lwc.2022.3149834 (дата звернення: 29.07.2025).

14. Kara İ. Twin ghosts: Evil Twin attacks in wireless networks and defense mechanisms. *Bitlis Eren University Journal of Science and Technology*.2024. Vol. 14. DOI: 10.17678/beuscitech.1450756.

15. Korolkov R., Kutsak S. Received-Signal-Strength-Based approach for detection and 2D indoor localization of Evil Twin Rogue access point in 802.11. *International Journal of Safety and Security Engineering*. 2021. Vol. 11. P. 13–20. DOI: 10.18280/ijsse.110102.

16. Kozel V., Ivanchuk O., Drozdova I., Prykhodko O. Analysis of the impact of encryption on the traffic volumes of IoT protocols. *International Journal of Computing*. 2025. Vol. 24 (3). P. 585–592.

17. Manali M., Kushwaha A., Wahi H., Sain K., Jha V. A recent survey on intrusion detection methods for wireless networks. *2023 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, 7–10 June, 2023. P. 0471–0476. DOI: 10.1109/AIIoT58121.2023.10174448.

18. Mykhaylova O., Nakonechny T. Security analysis of modern wi-fi network protection protocols: assessment of wpa3 protocol resistance during attacks based on dragonblood utility. *Computer Systems and Network*. 2024. Vol. 6, No. 1. P. 133–147. DOI: 10.23939/csn2024.01.133.

19. Noh J., Kim J., Cho S. Secure Authentication and Four-Way Handshake scheme for protected individual communication in public Wi-Fi Networks. *IEEE Access.* 2018. P. 1–10. DOI: 10.1109/ACCESS.2018.2809614.

20. Obukhova K., Savchuk T., Zhuravska I., Boiko A., Nikolskyi V., Puzyrov S. Prevention of unmanned vessels collisions due to pre-modeling the remote control center CPU load. *CSIT Proceedings*. 2021. Vol. 2. P. 202–205. DOI: 10.1109/CSIT52700.2021.9648800.

21. Onatskyi V.V., Savinov V. Yu. Traffic analysis and optimization in scalable network infrastructures. *Scientific notes of Taurida National V.I. Vernadsky University. Series «Technical Sciences».* 2025. Vol. 36 (75), No. 6. P. 271–276. DOI: 10.32782/2663-5941/2025.6.x/0x.

22. Physical layer security. Encyclopedia of wireless networks. Cham, 2020. P. 1071. DOI: 10.1007/978-3-319-78262-1_300486 (Last accessed: 07.04.2025).

23. Request rejected. URL: https://www.itu.int/rec/R-REC-P.1238-6-200910-S/en (Last accessed: 17.08.2025).

24. Scalable Power Control/Beamforming in Heterogeneous Wireless Networks with Graph Neural Networks / X. Zhang, et al. *GLOBECOM 2021 – 2021 IEEE Global Communications Conference*, Madrid, Spain, 7–11 December 2021. 2021. DOI: 10.1109/globecom46510.2021.9685457 (Last accessed: 25.04.2025).

25. Shibli A., Zanouda T. Data-driven radio environment map estimation using graph neural networks. *2024 IEEE Int. Conf. on Communications Workshops (ICC*

Workshops), Denver, CO, USA, 9–13 June, 2024. P. 650–655. DOI: 10.1109/iccworkshops59551.2024.10615637.

26. Shukla V. Review of electromagnetic interference shielding materials fabricated by iron ingredients. *Nanoscale Advances*. 2019. Vol. 1, No. 5. P. 1640–1671. DOI: 10.1039/c9na00108e (Last accessed: 25.04.2025).

27. Sun S. A chosen random value attack on WPA3 SAE protocol. Digital threats: research and practice. 2021. DOI: 10.1145/3468526 (Last accessed: 16.03.2025).

28. This H. DSR: frameworks guiding experimental work in science. N3AF, Teaching document. *Academic Notes of the French Academy of Agriculture*. 2017. Vol. 4, No. 2. P. 1–14. DOI: 10.58630/pubac.not.a372706.

29. Trunov A. Formation of indicators for evaluating the model based on a set of interconnected data sets in the tasks of communication technologies in healthcare. *CEUR Workshop Proceedings*. 2023. Vol. 3609. P. 157–166.

30. Trunov A., Dronyuk I., Martynenko V., Skopenko I., Skoroid M. Expanding the possibilities of video surveillance monitoring and recovery procedures for post-stroke patients. *Lecture Notes in Electrical Engineering (LNEE).* Vol. 1198. P. 762–781. Springer, Cham, 2024.

31. WiFi from past to today, consequences that can cause and measures of prevention from them, WiFi security protocols / E. Firdus, et al. E3S Web of Conferences. 2024. Vol. 474. P. 02004. DOI:/10.1051/e3sconf/202447402004.

32. Wireless fingerprinting uncertainty prediction based on machine learning / Y. Li та ін. *Sensors.* 2019. Vol. 19, No 2. P. 324. DOI: 10.3390/s19020324.

33. Zanna P., Radcliffe P., Kumar D. WP4: A P4 Programmable IEEE 802.11 data plane. *2020 30th International Telecommunication Networks and Applications Conference (ITNAC),* Melbourne, VIC, Australia, 25–27 November, 2020. DOI: 10.1109/itnac50341.2020.9315141.

34. Zawawi H., Muhamad W. N. W., Seroja S., Naim F. Rate adaptation for Quality of Service (QoS) improvement in IEEE 802.11ax Wireless Local Area Network (WLAN). *Proceedings of International Conference on Artificial Life and Robotics*. 2023. Vol. 28. P. 764–771. DOI: 10.5954/icarob.2023.os29-6.

35. Зінченко О. В., Вишнівський В. В., Гладких В. М., Прокопов С. В., Звенігородський О. С. Аналітичне моделювання SDN / NFV. *Системи управління, навігації та зв'язку* : збірник наукових праць. 2021. Т. 2, № 64. С. 136–139. URL: DOI: 10.26906/SUNZ.2021.2.136 (дата звернення: 25.04.2025).

36. Баєв В. О., Пузирьов С. В. Моніторинг локації клієнтів мережі LoraWAN з використанням сенсорних IoT-пристроїв. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 59. С. 48–53. DOI: 10.36910/6775-2524-0560-2025-59-06.

37. Дроздова Є. А., Козел В. М. Сучасні методи захисту баз даних в умовах кіберзагроз та війни. *Вісник Херсонського національного технічного університету.* 2025. Т. 2, № 3 (94). С. 177–185.

38. Журавська І. М., Обухова К. О., Савінов В. Ю. Моделювання енергоспоживання багатоядерного процесора клієнтського пристрою під час онлайн-з'єднання. *Електротехнічні та комп'ютерні системи* / Держ. ун-т «Одеська політехніка». 2021. № 35 (111). С. 73–82.

39. Іванчук О. В., Козел В. М. Дослідження впливу захисту інформації на обсяги пакетів даних протоколів інтернету речей. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2025. Вип. 57. С. 43–50.

40. Опірський І., Максимів Н., Женчур М. Дослідження безпеки стандарту Wi-Fi Protected Access 3 (WPA3). *Ukrainian Scientific Journal of Information Security.* 2023. Т. 29, No1. С. 21–31. DOI: 10.18372/2225-5036.29.17549.

41. Сертифікація Wi-Fi роутерів, модемів 4G, 5G і комп'ютерних аксесуарів – Unus Finis. URL: https://ucrf-pro.com.ua/ua/jnformatsjya/nashj-poslugj/249-sertjfjkatsjya-komp-yuternogo-obladnannya-ta-perjferjyj-sertjfjkatsjya-komp-yuternjh-aksesuarjv-z-bezdrotovjm-dostupom.html (дата звернення: 01.02.2026).

42. Ухань Є. О. Бездротова локальна мережа на каналі 60 ГГц для побудови контрольованої зони. *Могилянські читання – 2023* : тези доп. XXVI Всеукр. наук.-метод. конф. Миколаїв, 6–10 листоп. 2023 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2023. С. 449–450. URL:

https://dspace.chmnu.edu.ua/jspui/handle/123456789/1869 (дата звернення: 27.04.2025).

43. Ухань Є. О., Журавська І. М. Аналіз можливостей використання штучного інтелекту для захисту бездротових комп'ютерних мереж. *Сучасні Інформаційні Технології –2025* : матеріали XV Міжнар. наук. конф., Одеса, 15–16 травня 2025 р. Нац. ун-т "Одеська політехніка" / Одеса : Наука і техніка, 2025. С. 212–214. URL: https://ics_conf.tilda.ws/ukr#rec41121601, https://drive.google.com/drive/folders/1uXN7b84231YhSfT_tY6I9eMhPjDrIBKJ (дата звернення: 10.05.2025).

44. Шовкошитний І. І., Марченко А.О., Міненко Л. М. Метод визначення енергетичних параметрів радіозавад на межі зони радіовидимості. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2025. Т. 52, № 1. С. 102–107. DOI: 10.33099/2311-7249/2025-52-1-102-107.

45. Порядок запровадження в умовах надзвичайного або воєнного стану тимчасових обмежень на всій території України чи в окремих її регіонах на використання радіообладнання, випромінювальних пристроїв, радіоелектронних засобів та випромінювальних пристроїв спеціального призначення : затв. Постановою КМУ від 27 грудня 2022 р. № 1459. URL: https://zakon.rada.gov.ua/laws/show/1459-2022-%D0%BF#n8 (дата звернення: 01.02.2026).

46. Trunov A., Dronyuk I., Martynenko V., Skopenko I., Skoroid M. Expanding the possibilities of video surveillance monitoring and recovery procedures for post-stroke patients. *In book: Digital Ecosystems: Interconnecting Advanced Networks with AI Applications : Lecture Notes in Electrical Engineering (LNEE).* Vol. 1198. Switzerland AG : Springer Nature, 2024. P. 762–781.

47. Machine Learning for High-Precision Indoor Localization / X. Zhao, et al. RSSI-Based Localizations. Boca Raton, 2026. P. 160–204. DOI: 10.1201/9781003664659-6.

48. Fonseka P., Sandrasegaran K. Indoor localization for IoT applications using fingerprinting. *2018 IEEE 4th World Forum on Internet of Things (WF-IoT),* Singapore, 5–8 February, 2018. DOI: 10.1109/wf-iot.2018.8355105.

49. Putra Y. M., Wellem T. Simulasi jaringan IEEE 802.11ax WiFi 6 menggunakan simulator NS-3 untuk pengukuran throughput pada band frekuensi 6 GHz. *Jurnal Indonesia: Manajemen Informatika dan Komunikasi*. 2023. Vol. 4, No. 3. P. 913–923. DOI: 10.35870/jimik.v4i3.298 [In Indonesian].

50. Ухань Є. О. Модель WIFi-мережі на базі технології 802.11ad. *Могилянські читання – 2024* : тези доп. XXVII Всеукр. наук.-практ. конф., Миколаїв, 6–10 листоп. 2024 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2024. С. 140–143. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/2507 (дата звернення: 27.04.2025).

51. Perederyi V. I., Borchik E. Y., Zosimov V. V., Bulgakova O. S. Adaptation of the decision-making process in the management of critical infrastructure. *Radio Electronics, Computer Science, Control*. 2024. No. 3. P. 44–53. DOI: 10.15588/1607-3274-2024-3-5/.

52. Perederyi V. I., Borchik E. Y., Zosimov V. V., Bulgakova O. S. Evaluation of the influence of environmental factors and cognitive parameters on the decision-making process in human-machine systems of critical application. *Radio Electronics, Computer Science, Control.* 2024. № 1. P. 76–84. DOI: 10.15588/1607-3274-2024-1-7.

53. Perederyi V., Borchik E., Ohnieva O. Information technology for decision making support and monitoring in manmachine systems for managing complex technical objects of critical application. *Lecture Notes in Computational Intelligence and Decision Making. Advances in Intelligent Systems and Computing.* Springer, Cham, 2021. Vol. 1246. P. 448–466. DOI: 10.1007/978-3-030-54215-3_29.

54. Perederyi V., Borchik E., Wójcik W., Ohnieva O. Assessment and information security provision of the decision support process in technogenic object management systems. *CEUR Workshop Proceedings.* 2021. Vol. 3101. 14 p. URL: https://ceur-ws.org/Vol-3101/Paper22.pdf.

РОЗДІЛ 2
МЕТОДИ НАЛАШТУВАННЯ ТА КЕРУВАННЯ КОНТРОЛЬОВАНИМИ ЗОНАМИ

Формування КЗ у БКМ – це комплексний процес, що потребує поетапної реалізації фізичних, логічних та програмних заходів для створення захищеного простору [1]. Нижче наведено алгоритмізацію ключових етапів керування такими зонами

2.1 Метод позиціонування WiFi-джаммерів та нормалізації покриття радіосигналу

Першим елементом побудови КЗ є мінімізація виходу радіовипромінювання за межі фізичного периметра об’єкта згідно з НД ТЗІ 3.1-001-07 [2].

2.1.1 Математична модель оцінки затухання сигналу

Для забезпечення високої точності при формуванні контрольованої зони (КЗ) використовується математична модель розповсюдження радіохвиль у закритих приміщеннях, що базується на рекомендаціях ITU-R P.1238 та лог-нормальній моделі затухання [3]. Ця формула дозволяє розрахувати сумарні втрати потужності сигналу (L_{total}) на шляху від точки доступу до межі КЗ, враховуючи специфіку архітектури та матеріалів:

$$L_{total} = 20\,log_{10}\,f + N\,log_{10}\,d + \sum_{i=1}^{k} I\left(P_{wall\_i}\right) - 28\,, \qquad (2.1)$$

де $20\,log_{10}\,f$ – частотна складова, яка описує втрати у вільному просторі, що залежать від частоти сигналу;

$N\,log_{10}\,d$ – коефіцієнт втрати потужності, враховує як сигнал згасає залежно від відстані d (метри) між точкою доступу та приймачем;

$\sum_{i=1}^{k} I\left(P_{wall\_i}\right)$– сума затухання (втрат) при подоланні сигналом перешкод;

"28" – константа нормалізації, яка представляє собою системне числове значення (може змінюватися залежно від специфікації моделі ITU),

що використовується для узгодження одиниць вимірювання та базових втрат на першому метрі від антени.

Ключовим етапом розробки математичної моделі є формалізація критерію оптимальності у вигляді аналітичної цільової функції *F*.

Перехід від якісного опису задачі «оптимального розміщення джаммерів» до кількісного аналізу здійснюється шляхом представлення її як класичної задачі нелінійного програмування – знаходження глобального екстремуму (максимуму) сформованої скалярної функції.

$$F = w_1 \cdot \underbrace{\left(\sum_{i \in КЗ} \frac{P_{jam,i}}{P_{sig,i}}\right)}_{Приглушення\ в\ КЗ} - w_2 \cdot \underbrace{\left(\sum_{k \notin КЗ} P_{jam,k}\right)}_{Витік\ за\ периметр} - w_3 \cdot N_{jam}, \qquad (2.2)$$

де F – загальний показник ефективності сформованої контрольованої зони, що відображає якість балансу між захищеністю мережі та рівнем завад;

w_1, w_2, w_3– вагові коефіцієнти, які визначають пріоритетність кожного з чинників (ефективності приглушення, мінімізації витоку та енергозатрат) залежно від вимог до безпеки об'єкта;

$P_{jam,i}$ – потужність активної завади (шуму), що створюється засобами захисту в *i*-тій точці всередині контрольованої зони для нейтралізації спроб перехоплення;

$P_{sig,i}$ – потужність корисного сигналу бездротової мережі в *i*-й точці, відношення якої до потужності завади визначає рівень успішного приглушення зчитування даних;

$P_{jam,k}$ – потужність витоку завадового сигналу за межі периметра контрольованої зони, що характеризує вплив системи захисту на навколишнє середовище та сусідні мережі;

N_{jam} – показник апаратних витрат, який враховує кількість задіяних джерел випромінювання завад або сумарну енергію, необхідну для підтримки контрольованої зони в активному стані.

Сформована в роботі цільова функція є багатокритеріальною та нелінійною, з великою кількістю локальних екстремумів. Для знаходження її глобального максимуму було застосовано методи стохастичної оптимізації, зокрема алгоритм ройового інтелекту (англ. Particle Swarm Optimization, PSO) [4].

Рух кожної «частинки-рішення» (яка представляє собою конкретний набір координат та параметрів джаммерів) у багатовимірному просторі пошуку описується двома наведеними рівняннями

$$v_i^{t+1} = w \cdot v_i^t + c_1 \cdot r_1 \cdot (pbest_i - x_i^t) + c_2 \cdot r_2 \cdot (gbest - x_i^t), \qquad (2.3)$$

де v_i^{t+1} – нова швидкість *i*-тої частинки (агента оптимізації), що визначає напрямок та інтенсивність зміни параметрів контрольованої зони на наступному кроці;

w – коефіцієнт інерції, який балансує між дослідженням нових зон покриття та уточненням поточних значень потужності;

c_1, c_2 – когнітивний та соціальний параметри, що визначають ступінь довіри частинки до власного досвіду та досвіду всього «рою» при пошуку оптимальних меж захисту;

r_1, r_2 – випадкові числа в діапазоні [0; 1], які додають системі стохастичності для запобігання зацикленню алгоритму;

$pbest_i$ – найкращий локальний результат конкретної частинки, а $gbest$ – найкращий глобальний результат всієї системи моніторингу;

x_i^t – поточний стан (позиція) частинки, що відповідає набору параметрів системи захисту в момент часу *t*.

$$x_i^{t+1} = x_i^t + v_i^{t+1}, \qquad (2.4)$$

де x_i^{t+1} – нове значення параметрів (позиція) системи формування контрольованої зони, розраховане на основі попереднього стану та вектору швидкості;

v_i^{t+1} – вектор зміщення, отриманий з попередньої формули (2.3).

Завершальним етапом циклу розробки є верифікація результатів математичного моделювання та розробка методики адаптивного управління. Це необхідно, щоб переконатися, що модель точно описує реальні фізичні процеси та може ефективно функціонувати в динамічному середовищі.

Для кількісної оцінки результатів моделювання з даними натурних вимірювань було використано метрику середньоквадратичної помилки [5].

Після розгортання системи система переходить у режим інтелектуального моніторингу та адаптивного управління. Наведена формула описує механізм динамічного коригування будь-якого керуючого параметра, наприклад, потужності джаммера або налаштувань пріоритезації трафіку.

$$RMSE = \sqrt{\frac{1}{M}\sum_{i=1}^{M}\left(P_{mod,i} - P_{exp,i}\right)^2}, \qquad (2.5)$$

де *RMSE* – середньоквадратична помилка, яка використовується для оцінки точності моделювання меж контрольованої зони (чим вона менша, тим точніша модель);

M – кількість контрольних точок вимірювання потужності сигналу або завади в межах досліджуваного об'єкта;

$P_{mod,i}$ – модельне (теоретичне) значення потужності сигналу в *i*-тій точці, отримане в результаті розрахунків;

$P_{exp,i}$ – експериментальне (фактичне) значення потужності, отримане шляхом реального радіочастотного сканування місцевості.

Вибір цієї метрики в якості критерію верифікації та основи адаптивного керування аргументується такими обставинами:

Критична чутливість до аномалій: оскільки залежність квадратична, *RMSE* надає значно більшу вагу значним відхиленням. У сфері кібербезпеки це дає змогу негайно виявляти локалізовані ділянки «прориву» сигналу за межами периметра. Навіть поодинокі відхилення, неприпустимі для захищеної зони, будуть однозначно зафіксовані системою.

Математична сумісність з адаптивним керуванням: диференційованість

функції квадратичної помилки дозволяє точно обчислювати градієнт. Це є ключовою умовою для надійної роботи ітераційного методу адаптивного керування (2.6), що дає змогу системі в реальному часі коригувати свої параметри.

Динамічна стабілізація системи: використання *RMSE* зменшує вплив неістотних шумів вимірювань та сприяє поступовому наближенню системи до бажаного стану. Це запобігає різким коливанням потужності засобів активного захисту (джаммерів) при незначних змінах зовнішнього середовища, забезпечуючи стабільність та енергоефективність процесу формування контрольованої зони.

$$\text{Param}^{t+1} = Param^{t} + \alpha \cdot \left(Metric_{target} - Metric_{curr}\right), \qquad (2.6)$$

де Param^{t+1}– оновлене значення параметра системи захисту (наприклад, поріг чутливості WIPS або потужність джаммера) на наступному ітераційному кроці;

α – коефіцієнт швидкості навчання (адаптації), що визначає, наскільки різко система реагує на зміну зовнішніх умов;

$Metric_{target}$ – цільовий показник безпеки (наприклад, бажаний рівень затухання сигналу на межі периметра);

$Metric_{curr}$ – поточне виміряне значення метрики безпеки в реальному часі.

2.1.2 Метод нормалізації сигналу

Головною цілю нормалізації сигналу у вирішенні завдання побудови КЗ є становлення таких параметрів радіовипромінювання, при яких забезпечується стабільна робота авторизованих пристроїв всередині КЗ та мінімізується рівень сигналу за її межами для протидії НСД.

Основними етапами даного алгоритму є (рис. 2.1):

– **збір вхідних даних:** визначення фізичних меж приміщення, матеріалів стін та розташування точок доступу (англ. Access Point, AP);

– **розрахунок початкової моделі**: використання формул затухання (ITU-R P.1238) для прогнозування поширення хвиль [6];

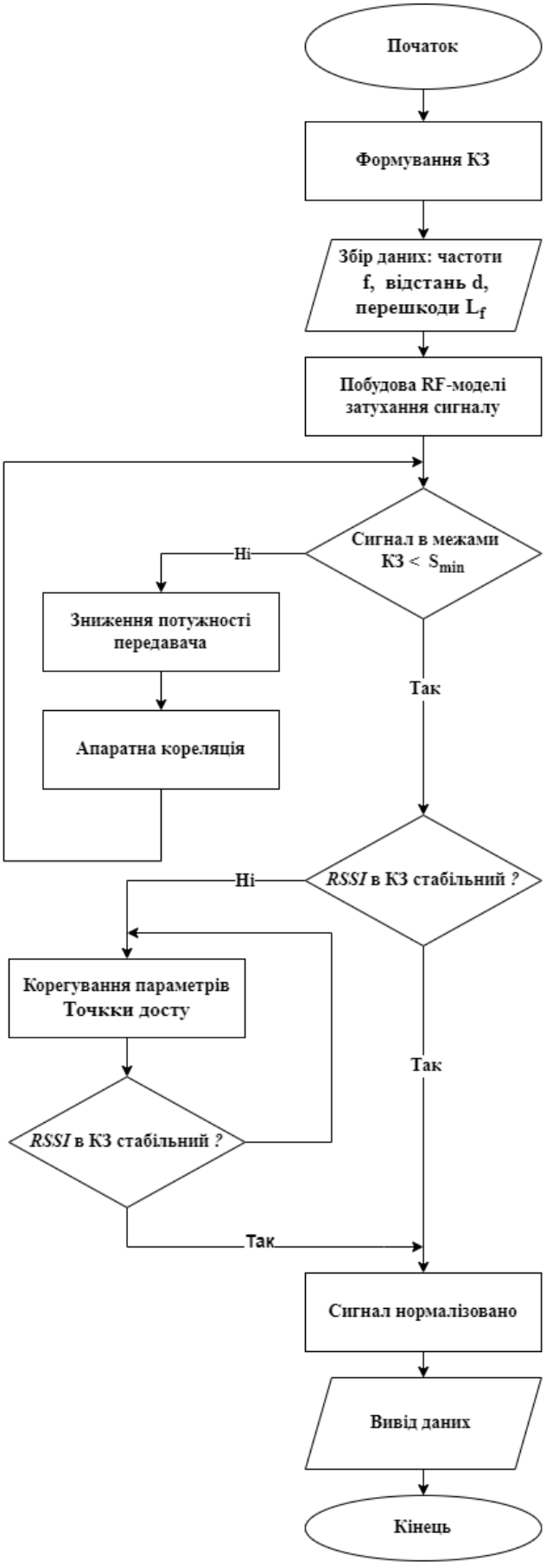

Рисунок 2.1 – Блок-схема алгоритму нормалізації

– **регулювання потужності** (P_t): програмне зниження або підвищення рівня передачі (наприклад, у діапазоні 6–22 дБм) для обмеження зони покриття;

– **корекція спрямованості**: використання спрямованих антен для концентрації сигналу у вузьких секторах (від 5° до 120°);

– **впровадження джаммерів**: апаратне глушіння сигналу в зонах, де неможливо досягти затухання програмними методами;

– **фінальна верифікація**: перевірка відповідності зони покриття вимогам безпеки та якості обслуговування (англ. Quality of Service, QoS).

Запропонована послідовність етапів дозволяє перетворити розсіяне поширення радіохвиль у чітко визначену, контрольовану зону. Ітеративний характер процесу є його ключовим елементом: у разі виявлення зон витоку сигналу під час верифікації після налаштування потужності та корекції спрямованості антен (кут огляду від 5° до 120° залежно від типу) передбачено застосування джаммерів для активного глушіння завад.

Такий метод гарантує не лише фізичне обмеження сигналу в діапазоні 6-22 дБм, а й забезпечення необхідного рівня якості обслуговування (QoS) для критичних сервісів усередині периметра. У результаті нормалізації позаминусові рівні сигналу досягають такого ступеня ослаблення за межами контрольованої зони, при якому перехоплення Handshake-пакетів або реалізація атак типу KRACK стає технічно неможливою через недостатнє відношення сигнал/шум [7].

2.2 Метод логічного сегментування та динамічної автентифікації

Після нормалізації фізичного рівня КЗ, впроваджується логічне управління доступом [8].

2.2.1 Сегментація мережі на рівні довіри

Головної ідеєю розподілення на рівні довіри є мінімізація у випадку порушення одного з них та захист даних більшої цінності. Для цього пропонується розподіл на три сегменти (рис. 2.2):

– **адміністративний сегмент:** тільки для адміністративного обладнання;

– **загальний сегмент:** автентифікація через WPA3-Enterprise (802.1X/EAP-TLS) [9];

– **гостьовий сегмент:** для пристроїв, що не пройшли перевірку цілісності.

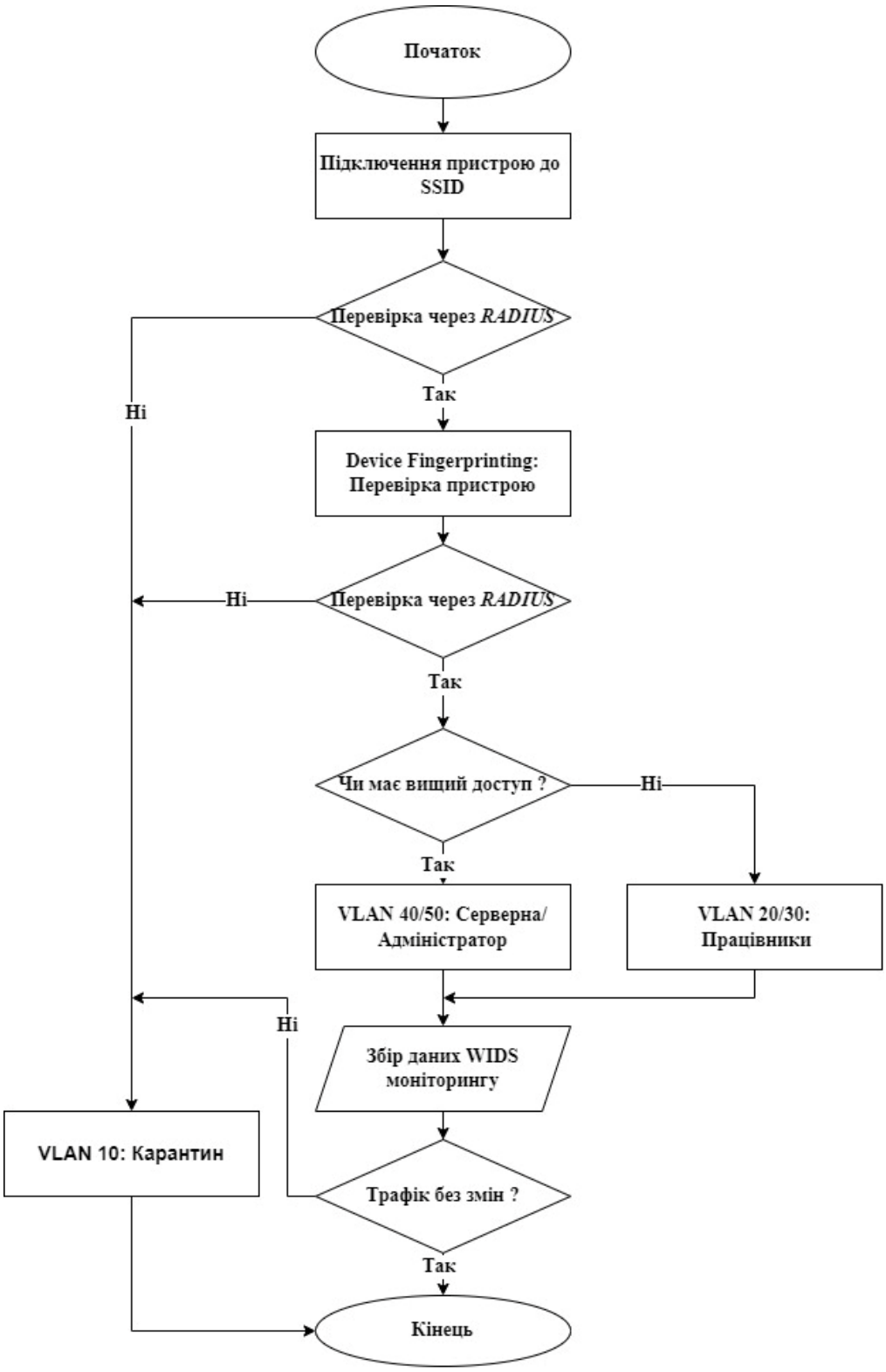

Рисунок 2.2 – Блок-схема алгоритму сегментації

Запропонована трирівнева модель сегментації дозволяє відокремити критичну інфраструктуру та мережеві ресурси від пристроїв, які можуть бути вразливими або не пройшли перевірку. Створення окремого адміністративного сегмента знижує ймовірність перехоплення трафіку, а застосування протоколу WPA3-Enterprise у загальному сегменті забезпечує захист від сучасних методів криптоаналізу. Такий підхід надає можливість гнучкого керування доступом у межах КЗ, дозволяючи коригувати права користувачів на підставі результатів автентифікації на RADIUS-сервері та поточної оцінки цілісності кінцевих пристроїв [10].

2.2.2 Автентифікація за протоколом WPA3

Впровадження протоколу WPA3 (Wi-Fi Protected Access 3) у межах КЗ є критично важливим кроком. Основним вектором атаки на WPA2 є вразливість процесу «4-way handshake», що дозволяє зловмисникам здійснювати атаки типу KRACK (Key Reinstallation Attack) та перехоплювати дані користувачів. WPA3 [11] докорінно змінює логіку встановлення з’єднання, замінюючи вразливі механізми на більш стійкі криптографічні рішення. Механізм SAE (Simultaneous Authentication of Equals) [12]. На зміну методу PSK (Pre-Shared Key) прийшов алгоритм SAE [13], що базується на протоколі Діффі-Геллмана на еліптичних кривих (англ. Elliptic Curve Diffie-Hellman, ECDH). Цей підхід забезпечує пряму секретність (англ. Forward Secrecy, FS) [14]: навіть якщо пароль мережі буде скомпрометований пізніше, зловмисник не зможе дешифрувати раніше перехоплений трафік (рис. 2.3).

Запровадження механізму Simultaneous Authentication of Equals (SAE) принципово змінює підхід до забезпечення безпеки в межах КЗ, оскільки виключає можливість проведення пасивних атак методом перебору паролів за словником (англ. Offline Dictionary Attacks). На відміну від застарілого підходу WPA2-PSK, де сесійний ключ прямо залежав від пароля, у WPA3 кожна сесія автентифікації генерує індивідуальний сеансовий ключ, який неможливо відновити навіть за умови подальшого розкриття спільного пароля.

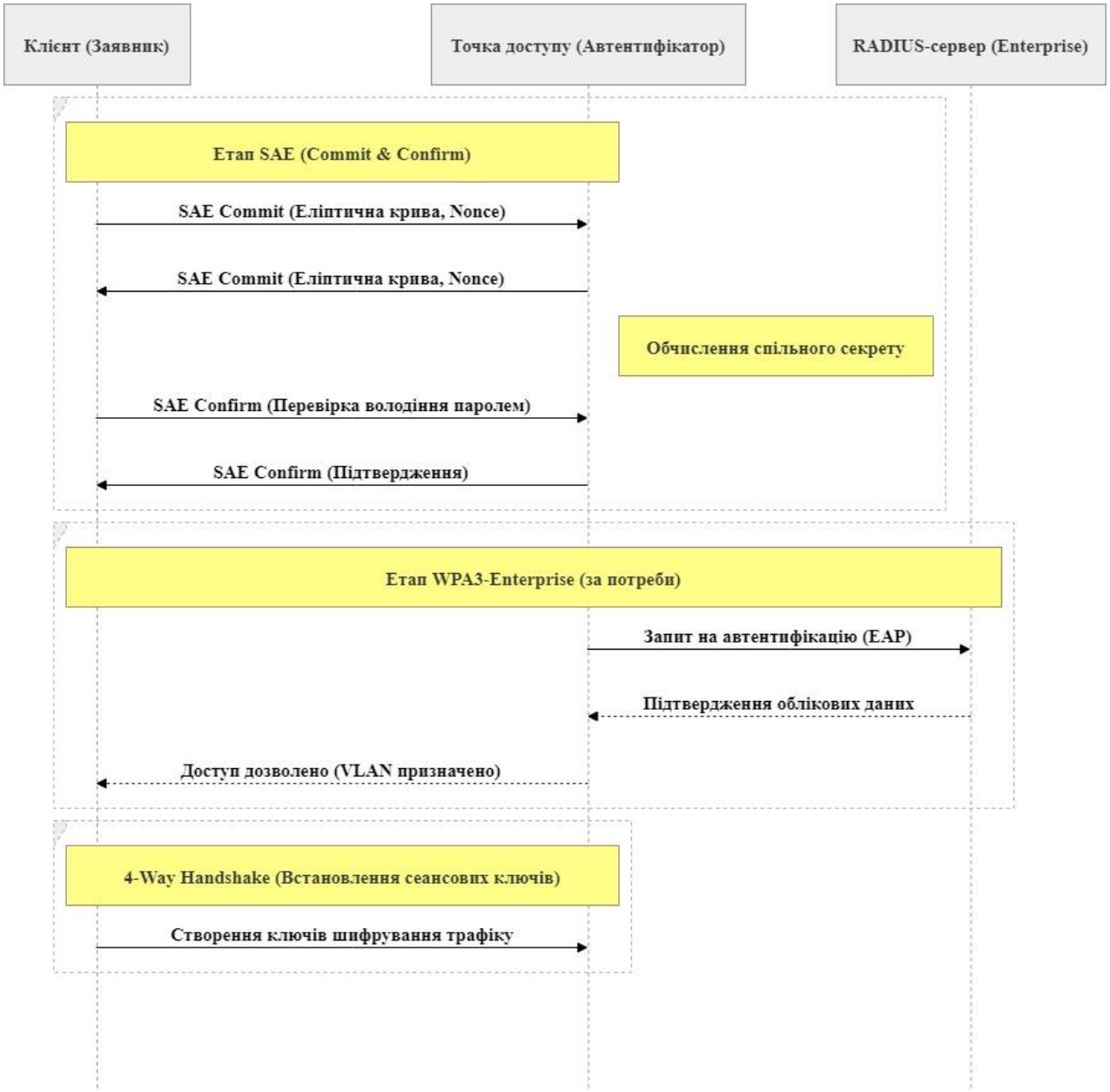

Рисунок 2.3 – Функціональна схема роботи процедури автентифікації WPA3

Такий механізм гарантує захищеність від атак типу «людина посередині» (англ. Man-in-the-Middle, MitM) [15] та запобігає несанкціонованому дешифруванню архівних перехоплених даних у «сірих зонах» покриття. Впровадження WPA3 на апаратній платформі MikroTik із підтримкою RouterOS v7 дозволяє досягти цього рівня захисту без зниження продуктивності, що є вкрай важливим для надійної роботи високошвидкісних магістральних каналів у адміністративному та загальному сегментах мережі.

2.3 Метод інтелектуального моніторингу WIDS/WIPS та протидії загрозам

Для забезпечення стійкості контрольованої зони (КЗ) необхідно впроваджувати системи виявлення та запобігання вторгненням (англ. Wireless Intrusion Detection System / Wireless Intrusion Prevention System, WIDS/WIPS) [16], які здійснюють безперервний аналіз радіоефіру. Основною задачею таких систем є пошук аномалій, виявлення сторонніх приладів та запобігання витоку інформації.

2.3.1 Критерії аналізу та виявлення загроз

Система моніторингу виконує аналіз мережевого середовища за наступними ключовими ознаками:

– **невідповідність BSSID та MAC-адреси**: виявлення фальшивих точок доступу (англ. Rogue AP) [17] та копій за типом «злого двійника» (англ. Evil Twin), які намагаються імітувати легітимну інфраструктуру;

– **відхилення у значеннях RTT (Round Trip Time)** [18]: аналіз затримки сигналу при опитуванні точки доступу дозволяє локалізувати підозрілі пристрої та виявити атаки типу «людина посередині» (англ. Man-in-the-Middle, MitM);

– **виявлення кадрів деавтентифікації (англ. Deauth Attack):** моніторинг аномальної кількості службових кадрів, що використовуються для розриву з'єднання легітимних клієнтів, що є ознакою підготовки до перехоплення даних або DoS-атаки;

– **Device Fingerprinting**: додатковий контроль, що включає визначення типу пристрою, його хост-імені та подальшу верифікацію з базою дозволених об'єктів.

Наведені методи виявлення об’єднуються в єдиний алгоритм, що гарантує повну автоматизацію процедури реагування на зафіксовані загрози в режимі реального часу (рис. 2.4).

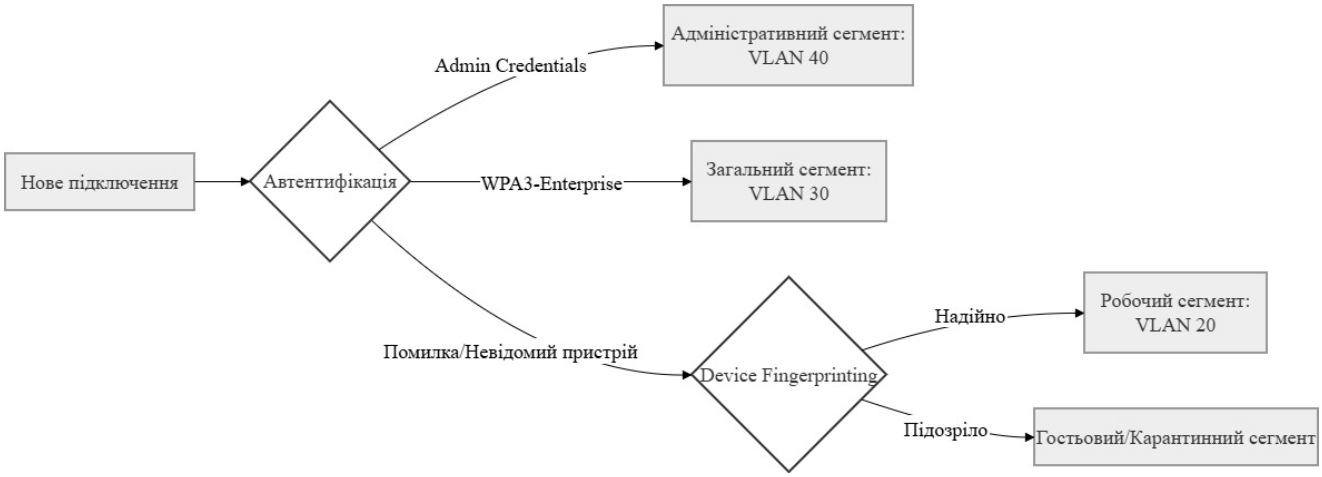

Рисунок 2.4 – Схема автоматизації процесу перевірки

Використання механізму Device Fingerprinting дає можливість вийти за рамки традиційної ідентифікації за MAC-адресою, яку зловмисник може відносно просто підмінити (англ. Spoofing). Дослідження додаткових атрибутів – наприклад, Hostname, сімейство операційної системи та окремі DHCP-опції – дозволяє створити унікальний цифровий профіль кожного легітимного елемента КЗ. Автоматизація цього процесу шляхом інтеграції з базою даних PostgreSQL забезпечує миттєву перевірку пристрою під час спроби підключення. Якщо характеристики клієнта не співпадають із зареєстрованим профілем, алгоритм передбачає автоматичне припинення сесії або поміщення пристрою в карантинний VLAN для подальшого розслідування. Така схема скорочує час перебування потенційного порушника в мережі і дає змогу системам моніторингу запускати заходи активного протидіяння до того, як зловмисник встигне здійснити шкідливі дії.

2.3.2 Механізми протидії

Ефективність системи моніторингу в межах КЗ визначається не лише швидкістю виявлення загроз, а й гнучкістю алгоритмів протидії. Залежно від критичності та типу виявленої активності, система має різну стратегію захисту.

Інформаційні та аналітичні заходи, які надають дані про роботу системи і зберігають події для подальшого аудиту адміністрацією:

– **збір та моніторинг даних**: проводиться безперервний збір аналітичних даних про роботу процесорів пристроїв, що знаходяться в КЗ, для виявлення аномальних змін навантаження, які можуть свідчити про несанкціоновану активність;

– **сповіщення адміністраторів**: у разі виявлення порушення периметра КЗ або ідентифікації пристроїв сканування мережі, система автоматично надсилає критичне сповіщення службі безпеки;

– **логування інцидентів**: формується база даних виявлених атак різних видів (Rogue AP або Evil Twin), що дозволяє проводити аналіз та вдосконалювати політики безпеки.

Активна протидія та ізоляція.

Заходи спрямовані на автоматизовану реакцію системи без втручання людини:

– автоматичне блокування;

– ізоляція через VLAN;

– радіочастотне глушіння.

Впровадження захищених стандартів та протоколів.

Для забезпечення цілісності та конфіденційності даних на мережевому рівні впроваджуються сучасні методи шифрування:

– WPA3-Enterprise;

– управління трафіком (QoS/QoE);

– шифрування SAE.

2.4. Перспективні методи керування

Сучасні атаки спричиняють відхід від традиційних статичних моделей безпеки на користь гнучких інтелектуальних систем, які забезпечують автоматичну корекцію захисних параметрів у режимі реального часу. Удосконалення наявних підходів реалізується через комплексну інтеграцію радіочастотного планування, технологій штучного інтелекту та стратегій дезорієнтації потенційного зловмисника. Такий підхід дозволяє створювати

адаптивне мережеве середовище, здатне ефективно протидіяти динамічним загрозам та мінімізувати ризики несанкціонованого доступу.

2.4.1 Використання динамічних карт радіосередовища

Пропонується впровадження технології Radio Environment Maps (REM) для візуалізації та контролю радіочастотного простору КЗ. Алгоритм забезпечує побудову просторово-частотної моделі мережі, що відображає рівні сигналів, завад та спектральну зайнятість головні елементи та переваги:

– **візуалізація в реальному часі**: система дозволяє адміністратору бачити «теплову карту» ефіру та ідентифікувати аномальні джерела випромінювання;

– **адаптивна відповідь**: якщо поблизу КЗ виявляється розгортання потужного несанкціонованого передавача, система автоматично ініціює зміну параметрів шифрування або потужності легітимних точок доступу для мінімізації ризику перехоплення;

– **інтеграція з машинним навчанням (англ. Machine Learning, ML)**: дано-орієнтовані підходи, такі як графові нейронні мережі (англ. Graph Neural Network, GNN), дозволяють точно картувати RF-середовище навіть за умов розріджених даних від сенсорів.

2.4.2 Метод «мережевої мімікрії»

Метод «мережевої мімікрії» (англ. Honey-SSIDs) спрямований на дезорієнтацію зловмисника шляхом створення ілюзорної інфраструктури, яка відвертає увагу від реальних сегментів КЗ:

– **генерація віртуальних точок**: алгоритм програмно створює велику кількість фіктивних SSID з навмисно заниженими рівнями захисту (наприклад, застарілі протоколи WPA/WPA2);

– **виснаження ресурсів атаки**: зловмисник витрачає час та обчислювальні потужності на атаку фейкових цілей, що дозволяє реальній КЗ залишатися прихованою в радіоефірі;

– **моніторинг активності:** спроби підключення до Honey-SSIDs миттєво

класифікуються як інцидент безпеки, ініціюючи збір даних про методи атаки та профіль зловмисника для подальшого посилення захисту.

2.4.3 Оцінка ризику на основі Machine Learning

Замість детермінованих правил доступу пропонується впровадження гнучкого розрахунку ймовірності зламу P_{risk}, що дозволяє системі приймати рішення на основі багатокритеріального аналізу.

$$P_{risk} = \omega_1 \times Signal\_dev + \omega_2 \times Traffic\_Anom + \omega_3 \times Geo\_Dist, \quad (2.2)$$

де $Signal\_dev$ – відхилення фізичних параметрів сигналу (*RSSI*, затримки) від еталонної RF-моделі;

$Traffic\_Anom$ – виявлення аномальної поведінки пристрою або нетипових потоків даних за допомогою інтелектуального аналізу;

Geo_Dist – оцінка геометричної відстані пристрою від розрахованих меж КЗ;

ω_i – вагові коефіцієнти, що динамічно визначаються навченою нейронною мережею (наприклад, на базі баєсового класифікатора) на основі історичних даних про атаки.

Висновки до розділу 2

На основі проведеного дослідження алгоритмів формування та керування КЗ у БКМ можна сформулювати наступні висновки:

Фізична нормалізація та моделювання: Обґрунтовано використання математичної моделі затухання сигналу за стандартом ITU-R P.1238, що дозволяє розрахувати енергетичний баланс потужності лінії зв’язку та встановити фізичні межі КЗ. Розроблений алгоритм нормалізації передбачає ітераційне регулювання потужності передавача та використання спрямованих антен для мінімізації «витоку» сигналу за межі контрольованого периметра.

Логічне зонування та ієрархія довіри: Доведено ефективність методу логічної сегментації мережі за допомогою VLAN, що дозволяє розділити користувачів на рівні довіри (критичний, робочий та ізольований сегменти).

Це мінімізує ризики горизонтального переміщення зловмисника всередині мережі та забезпечує ізоляцію конфіденційних даних.

Посилена автентифікація та моніторинг: Впровадження протоколу WPA3-Enterprise із механізмом SAE та 192-бітним шифруванням забезпечує захист від атак перевстановлення ключа (KRACK) та офлайн-перебору паролів. Алгоритм інтелектуального моніторингу на базі систем WIDS/WIPS дозволяє автоматично виявляти аномалії, такі як «злі двійники» (англ. Evil Twin) та Rogue AP, шляхом аналізу сигнатур ефіру та параметрів RTT.

Наукова новизна та перспективи: Запропоновано метод динамічного управління КЗ, що базується на використанні карт радіосередовища (REM) та методів машинного навчання для оцінки ризиків у реальному часі. Розглянуті перспективні можливості стандарту WPA4 [19], зокрема використання штучного інтелекту для протидії DDoS-атакам та адаптивного захисту від загроз з боку квантових обчислювальних систем.

Результати дослідження другого розділу опубліковані в роботах [3–6].

Список використаних джерел до розділу 2

1. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.12. 2007. № 232. URL: https://tzi.com.ua/downloads/3.1-001-07.pdf (дата звернення 12.01.2026).

2. A survey on behavior recognition using WiFi channel state information / S. Yousefi, et al. *IEEE Communications Magazine*. 2017. Vol. 55, No. 10. P. 98–104. DOI: 10.1109/MCOM.2017.1700082.

3. Ухань Є. О., Журавська І. М. Аналіз можливостей використання штучного інтелекту для захисту бездротових комп'ютерних мереж. *Сучасні Інформаційні Технології –2025* : матеріали XV Міжнар. наук. конф., Одеса, 15-16 травня 2025 р. Одеса : Наука і техніка, 2025. С. 212–214. URL: https://ics_conf.tilda.ws/ukr#rec41121601 (дата звернення: 10.05.2025).

4. Ухань Є. О., Журавська І. М. Формування контрольованих зон у локальних бездротових комп'ютерних мережах. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 59. С. 241–246. DOI: 10.36910/6775-2524-0560-2025-59-30.

5. Ухань Є. О., Журавська І. М. Концептуальна модель формування контрольованої зони в бездротових комп'ютерних мережах. *Наука і техніка сьогодні.* 2026. Вип. 2. С. 2336–2347 DOI: 10.52058/2786-6025-2026-2(56)-2336-2347.

6. Ухань Є. О. Методи та засоби моделювання зон покриття Wi-Fi та впливу інтерференції на якість сигналу. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 60. С. 312–317. DOI: 10.36910/6775-2524-0560-2025-60-33.

7. Wi-Fi Alliance. Wi-Fi Easy Connect™ Specification v3.0. 2022. URL: https://www.wifi.org/system/files/Wi-Fi_Easy_Connect_Specification_v3.0.pdf (Last accessed: 11.01.2026).

8. Wi-Fi Alliance. Wi-Fi Protected Access® Security Considerations. 2021. URL: https://www.wi-fi.org/system/files/Security_Considerations_20210511.pdf (Last accessed: 11.01.2026).

9. Wi-Fi Alliance. (n.d.). WPA3™ Specification Version 3.1. URL: https://www.wifi.org/system/files/WPA3%20Specification%20v3.3.pdf (Last accessed: 11.01.2026).

10. IEEE Standards Association. (n.d.). URL: https://standards.ieee.org/news/ieee_802_11ak-2018/ (Last accessed: 11.01.2026).

11. Vanhoef M., Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP pwd. New York University Abu Dhabi; Tel Aviv University & KU Leuven. 2019. URL: https://papers.mathyvanhoef.com/dragonblood.pdf (Last accessed: 11.01.2026).

12. White Paper: Networking | Security. Seamless next-generation Wi-Fi security through multivendor end-to-end WPA3 verification. 2021. URL:

https://www.intel.com/content/dam/support/us/en/documents/wireless/intel-whitepaper-wifi-security-through-wpa3-verification.pdf (Last accessed: 11.01.2026).

13. Stallings W. Wireless communications and networks. 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2005. URL: http://182.74.60.194/opac-tmpl/bootstrap/images/link/ebook/Computer%20Science/Wireless%20Communications%20and%20Networking.pdf (Last accessed: 11.01.2026).

14. Pothuganti K., Chitneni A. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. *Advance in Electronic and Electric Engineering*. 2014. Vol. 4(6). P. 655–662. URL: https://www.researchgate.net/publication/312471356_A_comparative_study_of_wireless_protocols_Bluetooth_UWB_ZigBee_and_Wi-Fi (Last accessed: 11.01.2026).

15. Sharma K., Dhir N. A study of wireless networks: WLANs, WPANs, WMANs, and WWANs with Comparison. *International Journal of Computer Science and Information Technologies*. 2014. Vol. 5(6). P. 7810–7813. URL: https://www.academia.edu/25106472/A_Study_of_Wireless_Networks_WLANs_WPANs_WMANs_and_WWANs_with_Comparison (Last accessed: 11.01.2026).

16. Ciubotaru B., Muntean G. M. Advanced network programming: Principles and techniques. London: Springer-Verlag, 2013. ISBN 978-1-4471-5292-7. URL: https://www.iqytechnicalcollege.com/Advanced%20Network%20Programming%20-%20Principles%20and%20Techniques.pdf (Last accessed: 11.01.2026).

17. Digi International Inc. An Introduction to Wi-Fi. *Rabbit Product Manual.* 2007–2008. URL: https://ftp1.digi.com/support/documentation/0190170_b.pdf (Last accessed: 11.01.2026).

18. Wi-Fi Alliance. (April 2023). Generational Wi-Fi® User Guide. URL: https://www.wifi.org/system/files/Generational_Wi-Fi_User_Guide_202304.pdf (Last accessed: 11.01.2026).

19. Pahlavan K., Krishnamurthy P. Historical Perspective. *International Journal of Wireless Information Networks*. 2020. Vol. 28(6). P. 1–17. DOI: 10.1007/s10776-020-00501-8.

РОЗДІЛ 3
РОЗРОБКА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ФОРМУВАННЯ ТА МОНІТОРИНГУ КОНТРОЛЬОВАНИХ ЗОН

Даний розділ присвячено практичній реалізації методів та засобів формування КЗ, що поєднує радіотехнічні, логічні та організаційні механізми захисту бездротового середовища [1].

3.1 Апаратна реалізація системи керування периметром

Апаратна складова засобів формування контрольованої зони (КЗ) базується на ієрархічній структурі побудови мережі, що забезпечує як високу продуктивність обробки даних, так і гнучкість фізичного керування радіосигналом. Основними компонентами системи є високопродуктивний маршрутизатор ядра, точки доступу з можливістю тонкого налаштування RF-параметрів та мікроконтролерні вузли для локального моніторингу та корекції покриття (рис. 3.1).

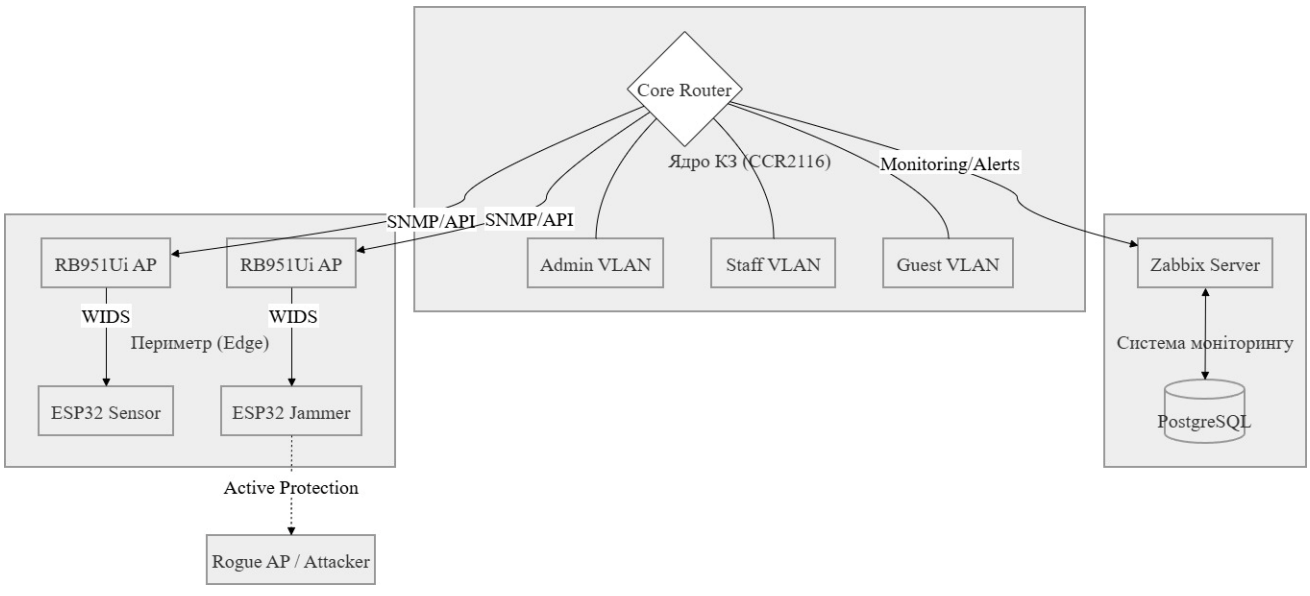

Рисунок 3.1 – Структурна ієрархія апаратних засобів формування КЗ

Дана схема має відображає ієрархічну взаємодію між ядром мережі, периферійними пристроями та системою моніторингу.

Рівень управління (Core): маршрутизатор MikroTik CCR2116-12G-4S+, який

забезпечує VLAN-сегментацію та функціональність RADIUS-сервера.

Рівень доступу та сенсорів (Edge): точки доступу MikroTik RB951Ui-2HnD та сенсори ESP32.

Рівень моніторингу: сервер Zabbix із базою даних PostgreSQL.

3.1.1 Центральний вузол керування (MikroTik CCR2116-12G-4S+)

Маршрутизатор ядра CCR2116-12G-4S+ виступає головним обчислювальним центром системи. Він забезпечує централізоване керування логічною сегментацією (VLAN), політиками автентифікації RADIUS та агрегацію даних від систем моніторингу WIDS/WIPS. Його потужна апаратна база дозволяє обробляти велику кількість криптографічних сесій WPA3-Enterprise без втрати пропускної здатності [2]. Основні його характеристики наведені в табл. 3.1

Таблиця 3.1 – Характеристики CCR2116-12G-4S+ у контексті КЗ

Параметр	**Значення / Функція**	**Роль у формуванні КЗ**
Кількість ядер CPU	16 (ARM 64-біт)	Обробка складних алгоритмів захисту та фільтрації
RAM	16 Гбайт DDR4	Забезпечення стабільної роботи систем моніторингу в реальному часі
Порти SFP+ (10 Гбіт/с)	4 порти	Побудова швидкісних магістральних каналів між сегментами мережі
Підтримка RouterOS v7	Повна	Налаштування складних політик QoS/QoE та RADIUS

Використання CCR2116-12G-4S+ як центрального вузла дає змогу впровадити гнучку конфігурацію мережі, де АР виступає головним шлюзом для опрацювання SNMP-трафіку, що надходить від АР та джаммерів. Завдяки високій швидкості обробки пакетів, забезпечує мінімальні затримки під час виконання автоматизованих сценаріїв блокування загроз, що гарантує швидку реакцію системи контролю на виявлені загрози без погіршення рівня (QoS) для клієнтів [3]. До того ж, наявність 10-гігабітних портів створює запас пропускної здатності для можливого масштабування та введення нових елементів захисту.

3.1.2 Периферійне радіообладнання (MikroTik RB951Ui-2HnD)

Для безпосереднього створення КЗ використовуються точки доступу MikroTik RB951Ui-2HnD. Їх головною перевагою є можливість програмного регулювання потужності сигналу на рівні прошивки, що дозволяє стабілізувати зону покриття та запобігти витоку інформації за межі приміщень [4]. Коди відповідних прошивок наведені у додатку Б. Основні характеристики використаного телекомунікаційного засобу наведені в табл. 3.2.

Таблиця 3.2 – Робочі параметри радіоінтерфейсу MikroTik RB951Ui-2HnD

Параметр	**Діапазон значень**	**Призначення для КЗ**
Потужність передавача	6–22 дБм	Нормалізація сигналу для обмеження периметра
Чутливість приймача	до –96 дБм	Визначення меж стабільної роботи клієнтських пристроїв
Коефіцієнт підсилення антени	2,5 дБі	Врахування при побудові теплової карти покриття
Діапазон частот	2,4 ГГц	Моделювання затухання згідно з моделлю ITU-R P.1238 [5]

Використання вказаних АР дозволяє ефективно адаптувати рівень фізичного захисту БКМ залежно від архітектурних особливостей приміщення. Налаштування мінімального порогу потужності на рівні 6 дБм у поєднанні з моніторингом RSSI допомагає виявляти пристрої, розташовані на межі зони радіовидимості, та оперативно блокувати їхній доступ до корпоративних ресурсів. У результаті RB951Ui-2HnD виконує функцію не лише засобу передачі даних, а й активного елемента формування фізичних границь контрольованої зони. Це суттєво зменшує ймовірність успішних атак типу «злий двійник» або перехоплення пакетів за межами офісу. Для проведення моделювання було обрано частину першого поверху ЧНУ ім. Петра Могили (рис. 3.2).

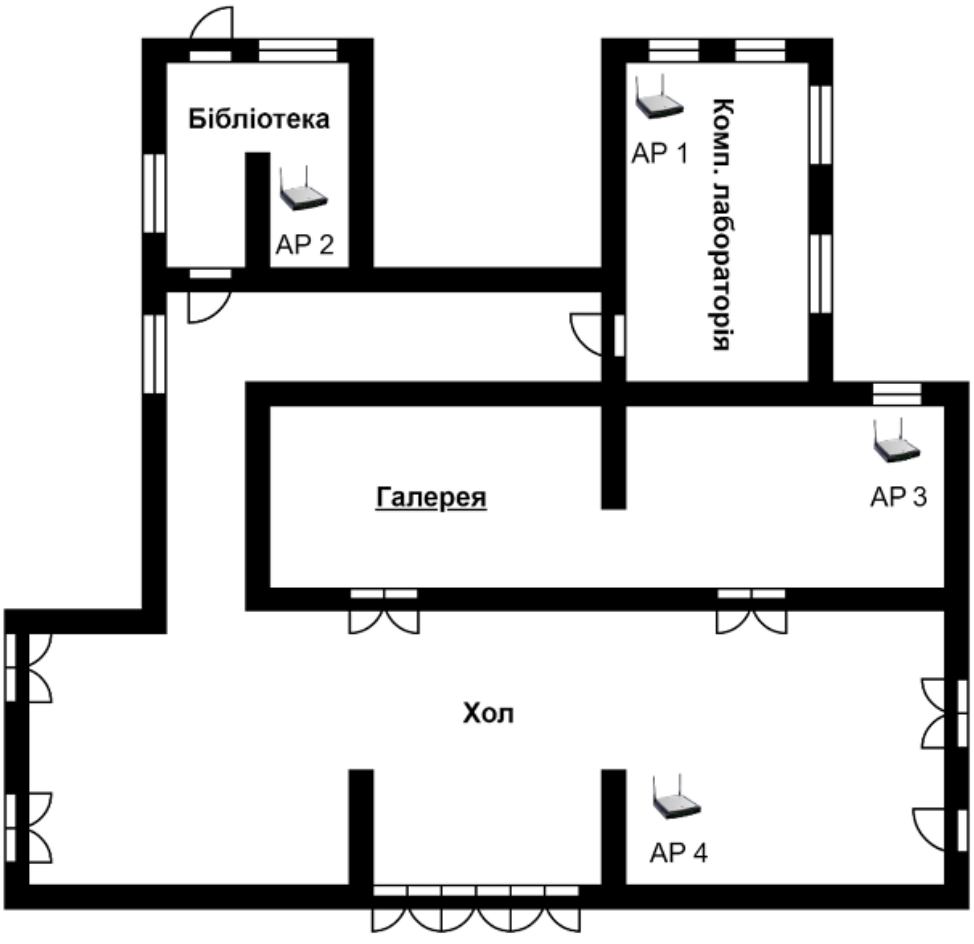

Рисунок 3.2 – План приміщень першого корпусу з розміщеними точками доступу

Для моделювання було використано комплексний метод, першим кроком якого був прорахунок ITU-R P.1238 та побудова теплової карти.

3.2 Програмне забезпечення та алгоритми обробки сигналів

Програмна складова засобів формування КЗ базується на етапах нормалізації сигналу та логічного зонування, що забезпечує стабільність та керованість бездротового середовища. Система об’єднує засоби автоматизованого збору даних з маршрутизаторів MikroTik, візуалізацію стану мережі через вебінтерфейс Zabbix та алгоритми активної протидії на базі мікроконтролерів ESP32.

3.2.1 Інтеграція моніторингу через вебінтерфейс Zabbix

Для централізованого контролю параметрів КЗ використовується система моніторингу Zabbix, яка збирає дані з пристроїв MikroTik (CCR2116 та RB951Ui) за допомогою протоколу SNMP та спеціалізованих скриптів [6] (табл. 3.3).

Таблиця 3.3 – Робочі параметри радіоінтерфейсу RB951Ui-2HnD

Об’єкт моніторингу	**Метод отримання**	**Метрика (Параметр)**
Параметри AP	SNMP Walk / Скрипти	Рівень шуму (Noise Floor), частота, завантаженість каналу
Клієнтські пристрої	RouterOS API	RSSI (рівень сигналу), швидкість передачі (Throughput), MAC-адреса
Безпека (WIDS)	Скрипти аналізу ефіру	Виявлення сторонніх (Rogue) AP, спроби MitM атак
Трафік	NetFlow / SNMP	Використання смуги пропускання критичними сервісами (VoIP, відео)

Вебінтерфейс Zabbix дозволяє адміністратору в реальному часі відстежувати порушення периметра КЗ та автоматично ініціювати скрипти блокування підозрілих MAC-адрес за «білими списками». Також всі дані

зберігаються в базі даних, що дозволяє зручно використовувати їх для проведення аналізу. У якості бази даних виступає PostgreSQL.

3.2.2 Розробка методу побудови джаммера на модулі ESP32

Модуль активної протидії на базі ESP32 (додаток Г) виконує роль апаратного засобу корекції покриття у випадках, коли сигнал виходить за межі КЗ. Програма для ESP32 реалізує алгоритм виявлення частоти роботи цільового пристрою та генерації перешкоджаючого сигналу [7].

Алгоритм роботи програми ESP32 Jammer:

– **сканування:** переведення Wi-Fi модуля в режим Promiscuous для аналізу пакетів у діапазоні 2,4 ГГц;

– **ідентифікація:** визначення каналів, на яких зафіксовано активність, що порушує політику КЗ;

– **генерація перешкод:** випромінювання сигналу на виявленій частоті, що призводить до деградації відношення сигнал/шум у зловмисника та блокування зв’язку;

– **адаптація:** використання спрямованих антен для локалізації джаммінгу суворо в межах необхідного сектора (60–120°), щоб не впливати на внутрішню роботу мережі.

3.3 Розробка методу мережевої взаємодії та інтеграція моніторингу Zabbix

Взаємодія елементів системи здійснюється за принципом багаторівневого оповіщення з централізованим аналізом радіочастотних метрик. Мережева архітектура інтегрує апаратні ресурси маршрутизаторів MikroTik, гнучкі можливості платформи Zabbix та аналітичну потужність системи керування базами даних (СКБД) PostgreSQL для гарантування цілісності контрольованої зони (КЗ).

3.3.1 Механізм збору та агрегації даних

Механізм збору та агрегації даних центральний маршрутизатор CCR2116-12G-4S+ функціонує в ролі головної обчислювальної платформи і здійснює функцію SNMP-агрегатора для всієї інфраструктури КЗ. Кінцеві точки доступу RB951Ui-2HnD, що виконують роль розподілених сенсорів системи WIDS/WIPS, безперервно проводять моніторинг радіочастотний спектр на предмет виявлення сторонніх точок доступу (англ. Rogue AP), клонів типу «злий двійник» (англ. Evil Twin) та пристроїв, які здійснюють несанкціоноване сканування мережі [8].

Покроковий процес збору даних:

– момент виявлення загрози на периферії: У разі виявлення аномалії (наприклад, спроби виконання MitM-атаки або перевищення порогу RSSI для несанкціонованої MAC-адреси) точка доступу негайно генерує повідомлення;

– NMP Trap повідомлення: Замість очікування наступного циклу опитування (англ. Polling) периферійний пристрій ініціює відправлення SNMP Trap на IP-адресу центрального шлюзу;

– паралельна обробка в ядрі: Завдяки 16-ядерній архітектурі та великому обсягу RAM, CCR2116 здатен одночасно обробляти потік трапів від численних точок доступу без уповільнення маршрутизації основного трафіку [9].

Це дозволяє мінімізувати час від моменту виникнення загрози до відображення критичного статусу у вебінтерфейсі Zabbix, забезпечуючи оперативну реакцію системи захисту (рис. 3.3).

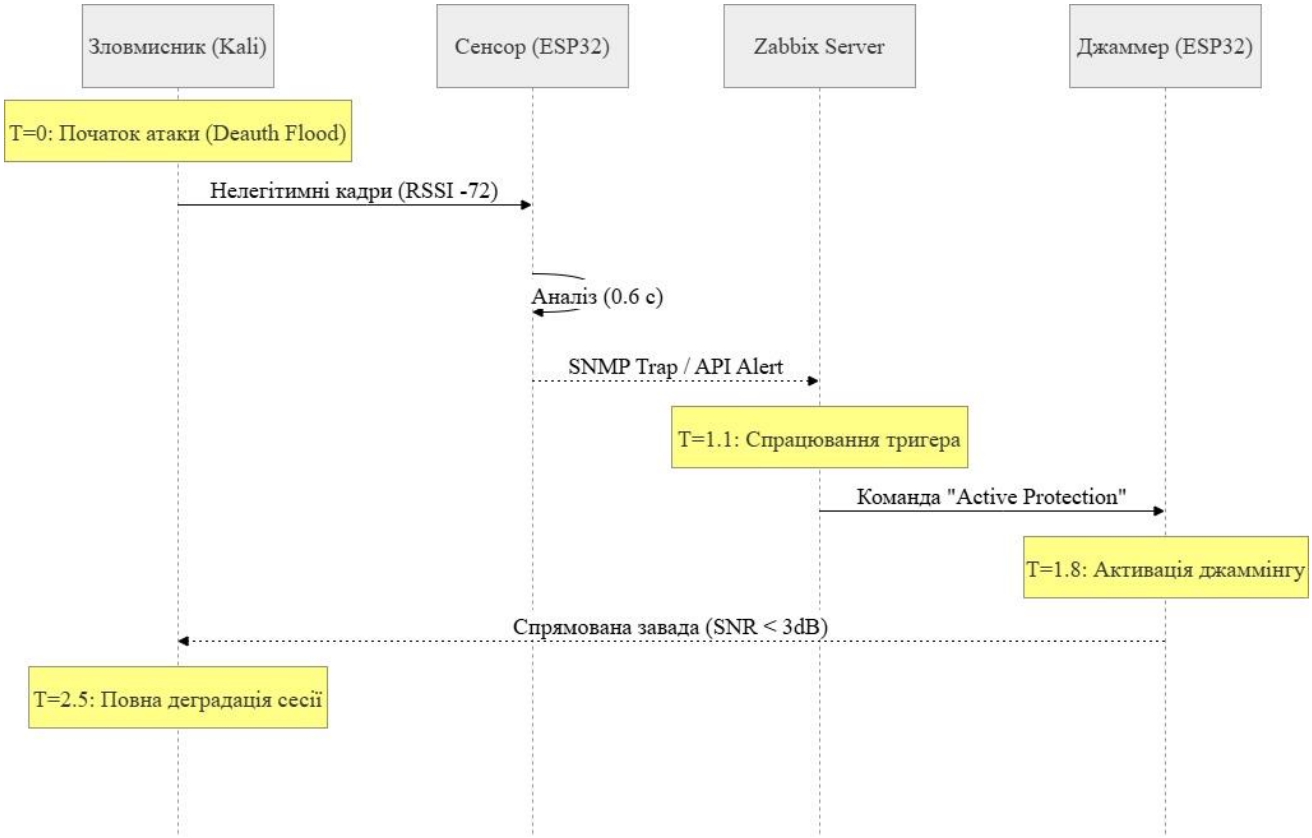

Рисунок 3.3 – Схема ієрархічної обробки даних

На діаграмі показано послідовність проходження сигналу від моменту виявлення несанкціонованої активності до моменту прийняття рішення системою моніторингу. Застосування маршрутизатора CCR2116 в ролі проміжного вузла дозволяє зняти навантаження із сервера Zabbix з обробки «сирих» даних, передаючи йому вже попередньо структуровані інциденти, що суттєво підвищує загальну стійкість архітектури до високих навантажень (англ. Highload) під час масованих атак.

3.3.2 Алгоритмічне порівняння RSSI та математичної моделі

Суттєвим компонентом інтелектуального моніторингу контрольованої зони (КЗ) є алгоритм порівняння фактичних значень рівня сигналу (RSSI), отриманих у режимі реального часу, з теоретичними моделями розповсюдження радіохвиль [10]. Це дає змогу системі не тільки зафіксувати присутність пристрою, а й виявляти аномалії, які вказують на порушення фізичного периметра або на застосування зловмисником підсилювачів сигналу.

Теоретичне значення $RSSI_{calc}$ визначається як різниця між вихідною потужністю та сумарними втратами і слугує еталонною величиною для системи моніторингу. Програмна реалізація в Zabbix та PostgreSQL Алгоритм порівняння виконано у вигляді єдиного скрипту, інтегрованого з платформою Zabbix [11]. Обробка даних включає такі етапи:

– агрегація метрик: за допомогою SNMP Trap та RouterOS API Zabbix отримує з маршрутизатора CCR2116 актуальні значення $RSSI_{means}$ для всіх виявлених пристроїв (authorized, rogue або unknown);

– зберігання та аналіз: зібрані показники фіксуються в СКБД PostgreSQL, що дозволяє не лише порівнювати миттєві величини, а й досліджувати тенденції зміни сигналу, що є критично важливим для виявлення мобільних джерел загроз [12];

– обчислення дельти (Δ): визначається відхилення виміряного сигналу від модельного значення за формулою $\Delta = RSSI_{calc} - RSSI_{means}$.

Логіка виявлення порушень та ініціація глушіння. Алгоритм використовує обчислену дельту для прийняття рішень щодо захисту периметра: Виявлення «сірих зон»: якщо неавторизований пристрій зареєстровано з $RSSI_{means} > -85$ дБм у місці, де модель прогнозує рівень сигналу нижче порогу чутливості, Zabbix класифікує це як аномальний витік сигналу за межі контрольованої зони. Ідентифікація Rogue AP: при виявленні сторонньої точки доступу з підвищеним рівнем сигналу скрипт зіставляє її параметри з тепловою картою в PostgreSQL; у разі збігу положення аномалії з критичними ділянками (вікна, двері) подія розглядається як висока загроза. Команда на нейтралізацію: після підтвердження інциденту тригер у Zabbix автоматично відсилає HTTP-запит до модуля ESP32, у якому передаються параметри частоти та каналу порушника, після чого джаммер починає формувати спрямовану заваду в секторі виявленого витоку [13– 15]. Така тісна інтеграція математичного моделювання з активним моніторингом дозволяє компенсувати помилки, спричинені складною конфігурацією приміщень, та забезпечує автоматизоване управління безпекою контрольованої зони в реальному часі.

3.3.3 Візуалізація та управління «сірими зонами»

Для збереження цілісності контрольованої зони (КЗ) одного лише статичного планування виявляється недостатньо, необхідно впровадити механізм динамічної адаптації до змін радіосередовища. Застосування реляційної СКБД PostgreSQL як центрального репозиторію дає змогу агрегувати великі обсяги інформації про стан ефіру, зокрема рівні сигналу (англ. Received Signal Strength Indicator, RSSI), ідентифікатори пристроїв та часові мітки інцидентів.

Динамічне картографування та виявлення вразливостей на підставі накопичених у PostgreSQL даних система формує актуальні теплові карти, що репрезентують поточну просторово-частотну модель середовища (англ. Radio Environment Map, REM) [16]. Через вебінтерфейс Zabbix адміністратор отримує візуалізацію так званих «сірих зон», зокрема:

– ділянки периметра, де через вплив перешкод або конструкційні особливості стін виникає нестабільне загасання сигналу, котре може сприяти витоку інформації;

– точки активності сторонніх пристроїв (Rogue AP) або підроблених копій легітимних мереж типу «злий двійник» (Evil Twin AP), що прагнуть перехопити клієнтські сесії.

Алгоритм автоматизованого прийняття рішень. Інтеграція системи моніторингу Zabbix із модулями активної протидії дозволяє реалізувати сценарій оперативного реагування на загрози. Управління інцидентом відбувається за такими етапами:

1) відпрацювання тригера: при виявленні WIDS пристрою зловмисника, який здійснює атаку (наприклад, KRACK або MitM), у Zabbix активується критичний тригер [17];

2) активація через API: Zabbix посилає команду через мережевий API на відповідний мікроконтролер ESP32, розташований у зоні порушення;

3) точкова протидія: модуль протидії, використовуючи інформацію про робочий канал і частоту порушника з PostgreSQL, ініціює джаммінг. Завдяки

спрямованим антенам заважання локалізується в межах «сірої зони», придушуючи сигнал зловмисника [18].

Збереження внутрішньої стабільності (QoS/QoE) є ключовим аспектом активної протидії є мінімізація її негативного впливу на легітимних користувачів усередині КЗ. Паралельно з активацією джаммера на маршрутизаторі ядра CCR2116 запускаються механізми управління трафіком:

– нормалізація ресурсів: автоматичний перерозподіл пропускної здатності шляхом політик QoS з метою пріоритезації критичних сервісів, таких як VoIP та відеоспостереження;

– контроль якості: моніторинг параметрів QoE (Quality of Experience), що дозволяє переконатися у відсутності деградації сервісів для авторизованого персоналу внаслідок захисних заходів [19].

Запропонована модель утворює замкнутий цикл управління безпекою радіочастотного простору. Вона інтегрує фізичне виявлення аномалій, інтелектуальну візуалізацію вразливостей та автоматизоване глушіння загроз із обов’язковою фіксацією результатів в аналітичній системі для подальшого аудиту та коригування політик доступу.

3.4 Засоби активної протидії на базі ESP32

Застосування програмно-апаратних засобів для активного глушіння є необхідним у випадках, коли програмні підходи до нормалізації сигналу або фізичне екранування приміщень не забезпечують повної ізоляції контрольованої зони (КЗ). Модуль активної протидії (джаммер) призначено для блокування радіопередач, що виходять за встановлений периметр, і для нейтралізації несанкціонованих точок доступу.

3.4.1 Апаратна архітектура та складові модуля

Реалізація модуля спирається на доступні мікроконтролерні платформи, що дозволяє проєктувати портативні та економічно обґрунтовані пристрої. Прототип найпростішого переносного джаммера включає такі елементи:

мікроконтролер ESP32, який виконує роль обчислювального ядра, відповідає за аналіз пакетів у діапазоні 2,4 ГГц та формування перешкодних сигналів; джерело живлення у вигляді літій-іонного акумулятора, підключеного через контролер заряджання (наприклад, модуль на базі TP4056), що забезпечує автономну роботу пристрою; випромінювальну підсистему зі спрямованою антеною, що дає змогу локалізувати вплив завад [20]. Для забезпечення ефективної роботи в межах КЗ критично важливим є підбір типу антени з огляду на необхідний кут покриття зони витоку [21] (табл. 3.4).

Таблиця 3.4 – Характеристики спрямованих антен для локалізації джаммінгу

Тип антени	**Кут огляду, град.**	**Рекомендоване застосування**
Панельна	60–90	Блокування сигналу у вузьких коридорах або вікнах
Типу «Yagi»	20–30	Прицільне глушіння віддалених Rogue AP
Секторна	60–120	Захист широких ділянок зовнішнього периметра

Застосування мікроконтролера ESP32 разом із вибраним типом антени забезпечує високу гнучкість апаратної частини модуля активної протидії. Головним плюсом такої конструкції є можливість оперативного розгортання та простота налаштування для ізоляції конкретних приміщень, у яких обмінюється інформація з обмеженим доступом, наприклад конференц-залів або дата-центрів. Апаратура на базі ESP32 може ефективно придушувати сигнали, що виходять за межі контрольованої зони, шляхом створення перешкод на визначеній частоті цільового пристрою, унаслідок чого в зловмисника відбувається повна втрата зв’язку.

3.4.2 Програмна логіка та алгоритм функціонування

Програмне забезпечення мікроконтролера ESP32 реалізує закритий цикл виявлення та активного глушіння завад, що дозволяє системі адаптуватися до змінних умов радіосередовища в реальному часі. Логіка роботи модуля базується на гібридному підході, який поєднує функції пасивного моніторингу ефіру та цілеспрямованої генерації перешкоджаючого сигналу.

*Ключові стани програмного алгоритму***:**

*Режим сканування та аналізу (WIDS-сенсор***):**

– Wi-Fi модуль ESP32 переводиться в режим Promiscuous, що дозволяє перехоплювати та аналізувати всі пакети в діапазоні 2,4 ГГц без підключення до конкретної точки доступу [22];

– програма виконує циклічне перемикання каналів (1–13 канали IEEE 802.11) для ідентифікації сторонніх SSID та MAC-адрес;

– на основі отриманих даних проводиться Device Fingerprinting для порівняння параметрів виявлених пристроїв із «білим списком», що зберігається в базі даних PostgreSQL [23].

Фаза прийняття рішення (Інтеграція з Zabbix):

– при виявленні неавторизованої активності поза межами розрахованого периметра (коли реальний RSSI перевищує поріг моделі ITU-R P.1238), модуль очікує підтвердження від центральної системи моніторингу;

– Zabbix через HTTP API передає модулю ESP32 параметри цілі: номер каналу, частоту та тип необхідної завади.

Режим активної протидії (Джаммінг):

– ідентифікація та фокусування: Програма фіксує робочий канал порушника;

– генерація завади: Модуль починає випромінювати перешкоджаючий сигнал на виявленій частоті. Це реалізується шляхом швидкої відправки пакетів деавтентифікації або створення «білого шуму», що призводить до критичної деградації відношення сигнал/шум у зловмисника [24];

– адаптивне керування: Програма регулює потужність випромінювання завади таким чином, щоб вона повністю пригнічувала сигнал у зоні витоку («сірій зоні»), але не створювала перешкод для легітимних користувачів всередині КЗ (рис. 3.4).

Рисунок 3.4 – Блок-схема роботи активного глушіння

Така програмна архітектура забезпечує мінімальний час реакції системи на порушення (до 2–5 секунд) та дозволяє локалізувати джаммінг суворо в межах необхідного сектора завдяки спрямованим антенам, підтримуючи високу якість обслуговування (QoS) для основної інфраструктури.

Висновки до розділу 3

Уданому розділі створено та впроваджено програмно-апаратні засоби формування й моніторингу контрольованих зон (КЗ) у бездротових мережах.

Розроблено та реалізовано багаторівневу апаратну архітектуру КЗ на основі ядра – маршрутизатора MikroTik CCR2116-12G-4S+, – яка забезпечує високу продуктивність обробки криптографічних сесій та агрегацію SNMP-трафіку.

Точки доступу RB951Ui-2HnD виконують роль фізичного обмеження периметра завдяки можливості програмного регулювання потужності в межах 6– 22 дБм. Підтверджено доцільність застосування математичної моделі ITU-R P.1238 для прогнозування зон затухання радіосигналу в приміщеннях.

Розроблено систему централізованого моніторингу на базі платформи Zabbix та СКБД PostgreSQL, яка в режимі реального часу зіставляє поточні значення RSSI з теоретичною моделлю; це автоматизувало виявлення «сірих зон» витоку сигналу та ідентифікацію сторонніх пристроїв із використанням методів WIDS/WIPS.

Реалізовано засоби активної протидії на основі мікроконтролера ESP32 для прицільного пригнічення несанкціонованих сигналів за межами КЗ. Застосування спрямованих антен з кутами огляду 60–120° дозволило локалізувати дію завад, запобігаючи при цьому погіршенню якості обслуговування (QoS) для авторизованих користувачів всередині периметра.

Результати дослідження третього розділу опубліковані в роботах [1,4–6].

Список використаних джерел до розділу 3

1. Ухань Є. О., Журавська І. М. Концептуальна модель формування контрольованої зони в бездротових комп’ютерних мережах. *Наука і техніка*

сьогодні. 2026. Вип. 2 (56). С. 2336–2347. DOI: 10.52058/2786-6025-2026-2(56)-2336-2347.

2. Han S., Li Y., Meng W., Li C., Liu T., Zhang Y. Indoor localization with a single Wi-Fi access point based on OFDM-MIMO. *IEEE Syst. J.* 2019. Vol. 13. P. 964–972.

3. Zhang P., Liu J., Shen Y., Jiang X. Exploiting channel gain and phase noise for PHY-layer authentication in massive MIMO Systems. *IEEE Trans. Inf. Forensics Secur.* 2020.

4. Ухань Є. О., Журавська І. М. Формування контрольованих зон у локальних бездротових комп'ютерних мережах. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 59. С. 241–246. DOI: 10.36910/6775-2524-0560-2025-59-30. ISSN 2524-0552.

5. Ухань Є. О. Методи та засоби моделювання зон покриття Wi-Fi та впливу інтерференції на якість сигналу. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво :* наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 60. С. 312–317. DOI: 10.36910/6775-2524-0560-2025-60-33. ISSN 2524-0552.

6. Burlachenko I. S., Zhuravska I. M., Ukhan Y. O., Tohoiev O. R., Tiutiunyk Y. I. Multi-agent monitoring system for heat loss mapping of multi-story buildings. *CEUR Workshop Proceedings.* 2019. Vol. 2516. P. 218–225. ISSN 1613-0073. URL: http://ceur-ws.org/Vol-2516/ (Last accessed: 11.01.2026).

7. Halperin D., Hu W., Sheth A., Wetherall D. Tool release: Gathering 802.11n traces with channel state information. *Comput. Commun. Rev*. 2011. Vol. 41. P. 53.

8. Shi S., Sigg S., Chen L., Ji Y. Accurate location tracking from CSI-based passive device-free probabilistic fingerprinting. *IEEE Trans. Veh. Technol.* 2018, 67, 5217–5230.

9. Chapre Y., Ignjatovic A., Seneviratne A., Jha S. CSI-MIMO: An efficient Wi-Fi fingerprinting using Channel State Information with MIMO. *Pervasive Mob. Comput.* 2015. Vol. 23. P. 89–103.

10. Yang Z., Zhou Z., Liu Y. From RSSI to CSI: Indoor localization via channel response. *ACM Comput. Surv.* 2013. Vol. 46, Is. 2, Article 25. 32 p. DOI: 10.1145/2543581.2543592.

11. Sadowski S., Spachos P. RSSI-based indoor localization with the Internet of Things. *IEEE Access*. 2018. Vol. 6. P. 30149–30161.

12. Wang J., Park J. An enhanced indoor positioning algorithm based on fingerprint using fine-grained CSI and RSSI measurements of IEEE 802.11n WLAN. *Sensors.* 2021. No. 21. 2769. DOI: 10.3390/s21082769.

13. Tiemann J., Wietfeld C. Scalable and precise multi-UAV indoor navigation using TDOA-based UWB localization. *In: Proceedings of the 2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2017, Sapporo, Japan, 18–21 September 2017.

14. Magsino E.R., Ho I.W.H., Situ Z. The effects of dynamic environment on channel frequency response-based indoor positioning. *In Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC),* Montreal, QC, Canada, 8–13 October 2017.

15. Ma Y., Wang B.; Pei S., Zhang Y., Zhang S., Yu J. An indoor localization method based on AOA and PDOA using virtual stations in multipath and NLOS environments for passive UHF RFID. *IEEE Access*. 2018.Vol. 6. P. 31772–31782.

16. Xue W., Hua X., Li Q., Yu K., Qiu W., Zhou B., Cheng K. A new weighted algorithm based on the uneven spatial resolution of RSSI for indoor localization. *IEEE Access.* 2018. Vol. 6. P. 26588–26595.

17. Wang J., Park J. G. Anovelindoorranging algorithm based on amreceived signal strength indicator and channel state information using annextended kalman filter. *Appl. Sci.* 2020. Vol. 10, No. 3687.

18. Zhou C., Yuan J., Liu H., Qiu J. Bluetooth indoor positioning based on RSSI and Kalman filter. *Wirel. Pers. Commun*. 2017. Vol. 96. P. 4115–4130.

19. XueW., Qiu W., Hua X., Yu K. Improved Wi-Fi RSSI measurement for indoor localization. *IEEE Sens. J.* 2017. Vol. 17. P. 2224–2230.

20. Rusli M. E., Ali M., Jamil N., Din M. M. An improved indoor positioning algorithm based on RSSI-trilateration technique for Internet of Things (IoT). *In: Proceedings of the 6th International Conference on Computer and Communication Engineering: Innovative Technologies to Serve Humanity (ICCCE),* 2016, Kuala Lumpur, Malaysia, 26–27 July 2016.

21. Yang B., Guo L., Guo R., Zhao M., Zhao T. A novel trilateration algorithm for RSSI-based indoor localization. *IEEE Sens. J.* 2020. Vol. 20. P. 8164–8172.

22. Zegeye W. K., Amsalu S. B., Astatke Y., Moazzami F. WiFi RSS fingerprinting indoor localization for mobile devices. *In Proceedings of the 2016 IEEE 7th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON),* 2016, New York, NY, USA, 20–22 October 2016.

23. Zegeye W. K., Amsalu S. B., Moazzami F.; Dean R. A., Astatke,Y. Minimum euclidean distance algorithm for indoor WiFi received signal strength (RSS) fingerprinting. *In Proceedings of the International Telemetering Conference*, Glendale, AZ, USA, 7–10 November 2016.

24. Wang G., So A.M.C., Li Y. Robust convex approximation methods for TDOA-based localization under NLOS conditions. *IEEE Trans. Signal Process*. 2016. No. 64. P. 3281–3296.

РОЗДІЛ 4
ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ФОРМУВАННЯ КОНТРОЛЬОВАНИХ ЗОН

4.1 Методологія тестування та опис експериментального стенду

У цьому розділі наведені результати експериментальних досліджень ефективності формування контрольованих зон за допомогою розроблених програмно-апаратних засобів. Головний акцент зроблено на підтвердженні коректності математичних моделей затухання сигналу, точності визначення меж контрольованої зони (КЗ) та оперативності реакції системи на інциденти інформаційної безпеки.

4.1.1 Склад та конфігурація експериментального стенду

Експеримент здійснювався в приміщенні загальною площею 60 м² із великою щільністю перешкод. Стіни виконано з капітальної цегли товщиною 25 см, що спричиняє значне загасання радіосигналу, тоді як металопластикові блоки й залізобетонні перекриття зумовлюють явище багатопроменевого поширення (англ. Multipath Propagation) [1]. Унаслідок цього система потребує підвищеної точності при визначенні меж КЗ (рис. 4.1).

Детальний опис компонентів стенду:

Центральний комутаційний вузол (Ядро) Основним елементом стенду є маршрутизатор MikroTik CCR2116-12G-4S+.

Функціонал:

Виконує роль центрального шлюзу та RADIUS-сервера для автентифікації згідно зі стандартом 802.1X. Обробка даних: Завдяки 16-ядерному 64-бітному процесору ARM пристрій забезпечує паралельну обробку SNMP-трапів від периферійних вузлів і моніторинг стану WIDS без впливу на пропуск основного трафіку. Це має критичне значення для уникнення «пляшкового горла» під час масованих атак [2].

Точки доступу (Периметр):

Установлено дві точки доступу MikroTik RB951Ui-2HnD, розміщені в протилежних кутах приміщення для забезпечення перехресного покриття. Призначення: Пристрої працюють у діапазоні 2,4 ГГц за стандартом 802.11n. Регулювання: Ключовою перевагою є підтримка Transmit Power Control (TPC), що дозволяє коригувати потужність передавача з кроком 1 дБ. Це дозволило експериментально підібрати потужність у межах 6–18 дБм, необхідну для «відсікання» сигналу на межі капітальних стін.

Сенсорна мережа та модуль протидії:

Розгорнуто три вузли на базі мікроконтролерів ESP32. WIDS-сенсори (2 шт.): Працюють у режимі Promiscuous, безперервно скануючи ефір і збираючи RSSI-метрики від усіх пристроїв у зоні видимості.

Активний модуль (1 шт.):

Оснащений спрямованою панельною антеною з коефіцієнтом підсилення 12 дБі. Програмна логіка модуля допускає переключення з режиму моніторингу у режим активної генерації перешкод (джаммінг) за командою центральної системи.

Програмно-аналітичні засоби:

Система моніторингу побудована на Zabbix 7.0 LTS. Обробка метрик: Для зберігання та аналізу часових рядів використовується PostgreSQL, налаштована на роботу з даними з кроком 1 секунда, що дозволяє фіксувати історію змін рівнів сигналу для кожного пристрою.

Візуалізація:

Налаштовано дашборди для відображення поточної «теплової карти» ефіру й статусів тригерів безпеки. Візуалізація архітектури та топології стенду наведена з метою наочного відображення взаємодії компонентів; на рис. 4.1 представлено структурну схему мережевої логіки.

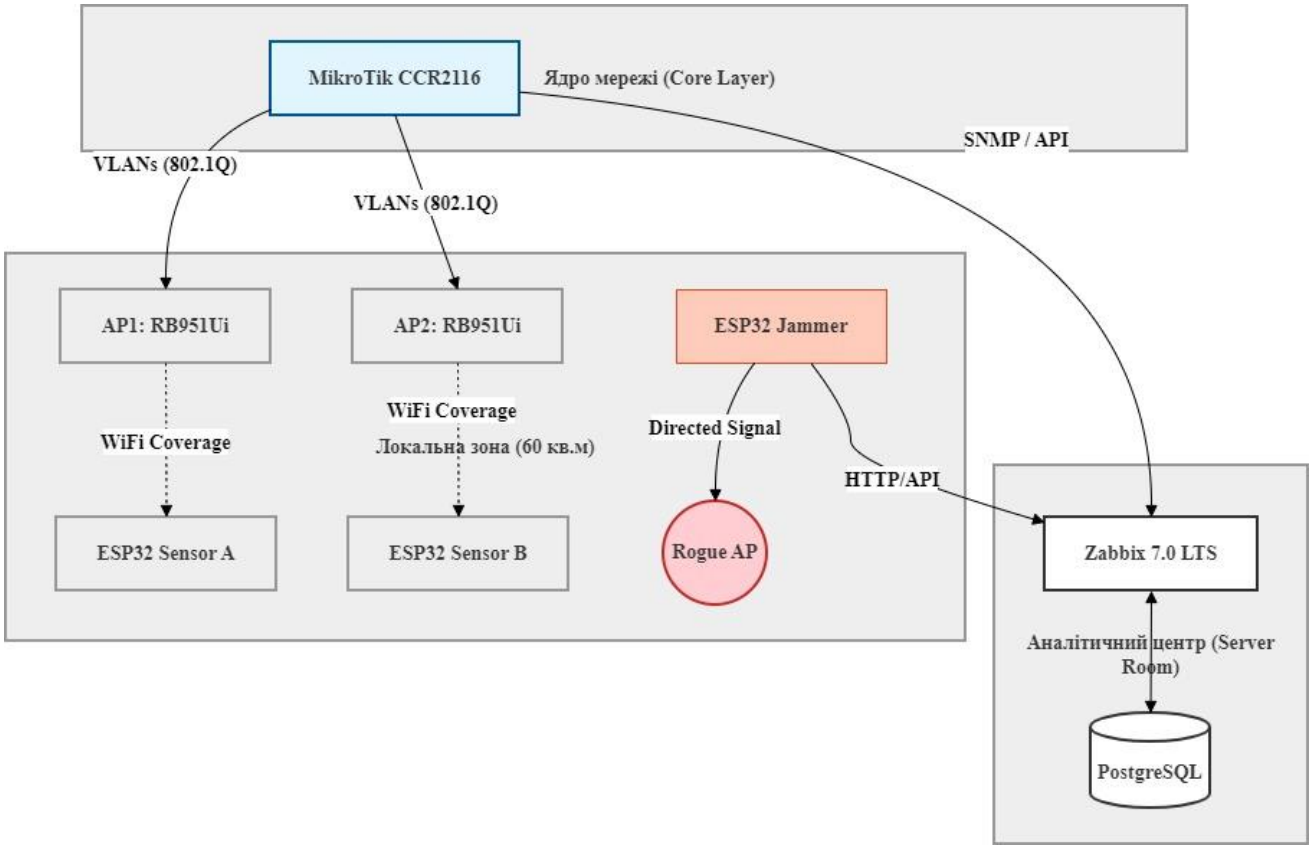

Рисунок 4.1 – Інформаційна модель ієрархічної структури стенда

Наведена топологія відображає багаторівневий та ієрархічний підхід до побудови системи. Схема демонструє повний закритий цикл управління безпекою КЗ: від пасивного спостереження сенсорами ESP32 та точками доступу MikroTik, агрегації даних на рівні ядра мережі (CCR2116), до аналітичного опрацювання сервером Zabbix та ініціалізації активної протидії модулем джаммінгу для нейтралізації загрози.

Для оцінки ефективності КЗ апаратні засоби були розміщені відповідно до цільового призначення у місцях, як зазначено у табл. 4.1.

Таблиця 4.1 – Характеристики спрямованих антен для локалізації джаммінгу

Компонент	Місце розміщення	Цільове призначення
AP1	Кут приміщення (біля вікна)	Формування межі покриття та контроль витоку через скло
AP2	Центр приміщення	Забезпечення стабільного зв'язку для авторизованих осіб
ESP32 Sensor A	Біля вхідних дверей	Детекція пристроїв у коридорі («сіра зона»)
ESP32 Jammer	Навпроти зовнішньої стіни	Активне пригнічення сигналу в зоні потенційного перехоплення
CCR2116	Серверна шафа	Централізоване управління та сегментація трафіку

Дана конфігурація стенду дозволяє не лише збирати статистичні дані про рівні сигналу, а й моделювати реальні сценарії атак, перевіряючи час реакції системи та точність спрацювання тригерів у Zabbix.

4.1.2 Детальна методика тестування

Для забезпечення статистично значущих висновків і верифікації дослідної гіпотези тестування було структуровано у три послідовні критичні фази. Кожна з цих фаз забезпечує поступ від теоретичного моделювання до практичного підтвердження ефективності захисних засобів контрольованої зони (КЗ).

Етап А: Калібрування та корекція RF-моделі.

Завдання цього етапу полягає у валідації математичної моделі ITU-R P.1238 у контексті конкретної локації. Офісні приміщення характеризуються високим рівнем перешкод і багатопроменевим поширенням сигналу, що робить стандартні розрахункові коефіцієнти недостатньо релевантними.

Методика вимірювань: Виміри рівня сигналу (*RSSI*) виконуються в 20 фіксованих точках у межах лабораторії та сусіднього коридору. Вибір точок забезпечує охоплення зон як прямої видимості (*LoS*), так і зон, що перебувають за капітальними перешкодами (*NLoS*). Засоби вимірювання: Застосовується спеціалізоване програмне забезпечення на базі мікроконтролерів ESP32 у режимі моніторингу, що дозволяє фіксувати рівень фізичного сигналу без впливу програмних артефактів операційних систем кінцевих пристроїв. Очікувані результати: Отримане емпіричне уточнення коефіцієнта втрат у стінах (L_f) та експоненти загасання зі збільшенням дистанції (N) дозволить адаптувати систему моніторингу до фактичної архітектури будівлі та зменшити частоту хибно позитивних спрацьовувань (англ. False Positives).

Етап Б: Програмно-апаратна стабілізація периметра КЗ.

Після корекції моделі здійснюється ітеративна настройка апаратних параметрів точок доступу з метою формування чіткої фізичної межі радіопокриття. Регулювання потужності передавачів (TPC): Потужність передавачів коригується у межах 22 дБм – 6 дБм. Використання мінімально необхідної потужності є ключовим елементом захисної стратегії, оскільки це звужує зону радіовидимості мережі. Формування «радіотіні»: Успіх визначається досягненням рівня сигналу приблизно в межах від –85 дБм до 90 дБм безпосередньо за зовнішнім периметром приміщення (коридори, суміжні кабінети). REM-картування: За результатами вимірів формується фінальна радіомапа середовища (англ. Radio Environment Map, REM), яка завантажується до системи Zabbix і використовується як еталон для порівняльного аналізу.

Етап В: Імітація вторгнення та активні заходи протидії.

Ця фаза є найбільш динамічною і відтворює реалістичну атаку на бездротовий периметр з метою оцінити швидкодію комплексного захисту [3]. Сценарії атаки: Застосовується портативна станція на базі Kali Linux для проведення атак типу «Evil Twin» (створення фейкової точки доступу) або масованих деаутентифікацій клієнтів з метою перехоплення WPA Handshake.

Алгоритм реагування:

– сенсори ESP32 виявляють аномалії сигналу поза межами КЗ;

– Zabbix приймає SNMP-трап і через API ініціює відповідну команду [4];

– модуль активної протидії виконує спрямований джаммінг для ізоляції загрози. Контрольні метрики: Основним показником є час реакції системи (латентність) – інтервал від надходження першого пакета від злочинного вузла до моменту його повної нейтралізації модулем протидії.

Для наочного представлення тривалості та послідовності етапів експерименту нижче наведено діаграму Ганта (рис. 4.2).

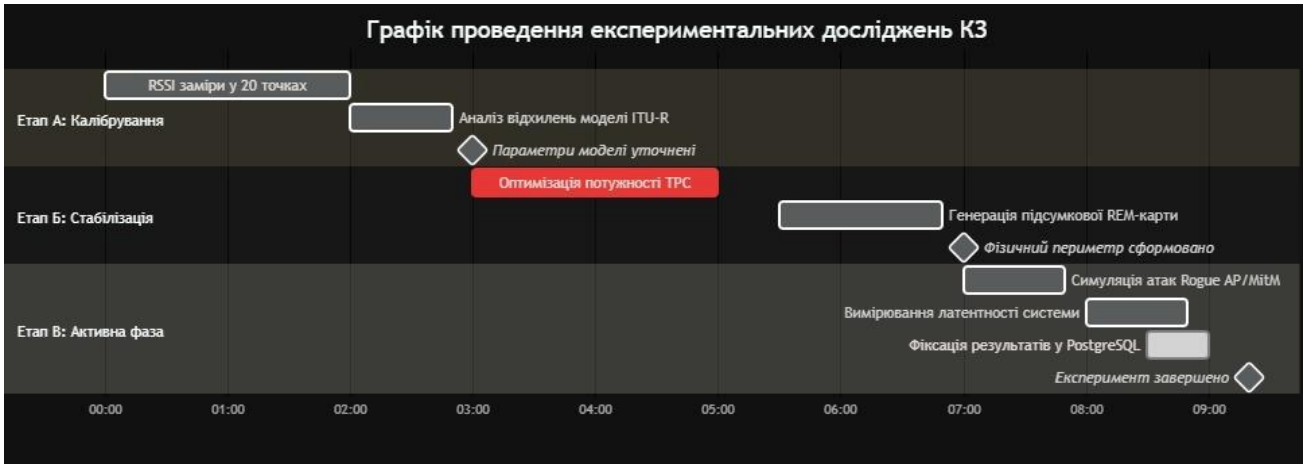

Рисунок 4.2 – Діаграма Ганта

Запропонований метод забезпечує комплексний підхід до оцінки безпеки: від математичної точності планування до практичної стійкості перед активними кіберзагрозами.

4.1.3 Організація збору даних у PostgreSQL

Для перетворення розроблених програмно-апаратних засобів з простого інструменту реагування на потужну аналітичну платформу була приділена особлива увага архітектурі зберігання даних. Вибір PostgreSQL пояснюється не лише її надійністю, а й здатністю ефективно обробляти великі обсяги часових рядів (англ. Time-Series Data), що надходять від розподіленої мережі сенсорів.

Архітектура бази даних і структура метрик Центральна база даних виконує функцію «чорної скриньки» експерименту. Збирання даних з інтервалом

в 1 секунду забезпечує необхідну високу зернисту деталізацію для фіксації перехідних явищ у радіоефірі, таких як короткочасні сплески інтерференції або швидкі спроби перехоплення пакетів. Кожна записана транзакція в базі даних формується за наведеною схемою (табл. 4.2).

Таблиця 4.2 – Логічна структура запису метрик у PostgreSQL

Назва поля	**Тип даних**	**Опис та технічне значення**
event_time	Timestamp (мс)	Часова мітка з мілісекундною точністю для синхронізації подій між різними сенсорами
sensor_id	Integer	Унікальний ідентифікатор вузла (AP або ESP32), що зафіксував активність
target_mac	MAC Address	Унікальний ідентифікатор пристрою-порушника для відстеження його переміщення
rssi_val	Integer (дБм)	Потужність сигналу. Ключовий показник для побудови REM-карти
noise_floor	Integer (дБм)	Рівень фонового шуму, що дозволяє розрахувати показник SNR
channel_load	Percentage (%)	Коефіцієнт утилізації каналу, що вказує на інтенсивність атаки або завади

Аналітичний потенціал і розрахунок SNR накопичення інформації в такому форматі дозволяє системі рухатися від елементарного визначення «сигнал присутній / сигнал відсутній» до всебічного оцінювання якості середовища.

Зокрема, обчислення відношення сигнал/шум (англ. Signal-to-Noise Ratio, SNR) здійснюється за відповідною формулою:

$$SNR(дБ) = RSSI_{target} - Noise_{floor}\,. \quad (4.1)$$

Це має критичне значення під час фази активної протидії (Етап В). Аналізуючи динаміку SNR у режимі реального часу, система може автоматично коригувати вихідну потужність джаммера на ESP32. Якщо SNR противника знижується нижче порогу 3–5 дБ, це свідчить про ефективне придушення каналу зв'язку та неможливість розшифрування трафіку.

Візуалізація потоку даних (англ. Data Pipeline). Нижче представлено схему перетворення «сирих» даних з ефіру в аналітичні звіти (рис. 4.3).

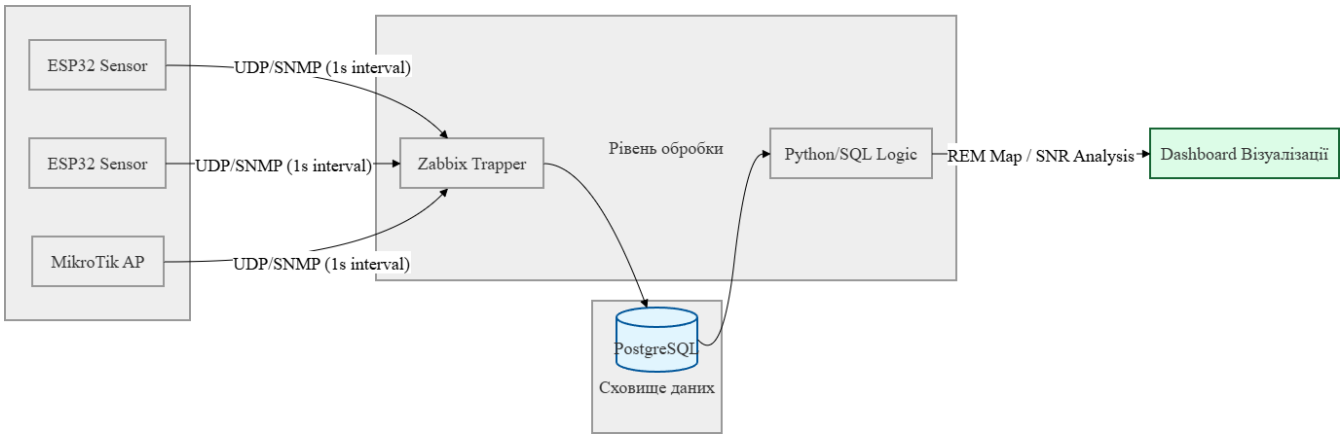

Рисунок 4.3 – Візуалізація потоку даних

Завдяки збереженню інформації в PostgreSQL розроблені програмно-апаратні засобі отримують можливість ретроспективного аналізу («прокрутки часу назад»). Це дає змогу проводити розслідування минулих інцидентів та виявляти закономірності в поведінці порушників (наприклад, закономірності появи Rogue AP у певні часові проміжки). У перспективі накопичений масив даних може слугувати для навчання нейронних мереж з метою прогнозування виникнення «сірих зон» ще до появи реальної загрози.

Такий підхід до організації даних переводить PostgreSQL із ролі пасивного архіву в активний елемент системи підтримки прийняття рішень, що надає науково обґрунтовану основу кожному кроку експерименту.

4.2 Дослідження точності локалізації та стабілізації межі зони

Дослідження було виконано у лабораторії інформаційно-комп'ютерного центру Чорноморського національного університету ім. Петра Могили, що надало можливість відтворити умови звичайного офісного простору. Збір даних було автоматизовано та синхронізовано за допомогою NTP-сервера, розгорнутого на маршрутизаторі MikroTik CCR2116, завдяки чому часові мітки між датчиками відрізнялися не більше ніж на 10 мс.

4.2.1 Підготовчий етап: Конфігурація середовища

Перед початком активних замірів було проведено радіочастотний аудит (англ. Site Survey) за допомогою телефону Moto G60 та програмного застосунку "WiFiAnalyzer" для визначення фонового рівня зашумленості (рис. 4.4).

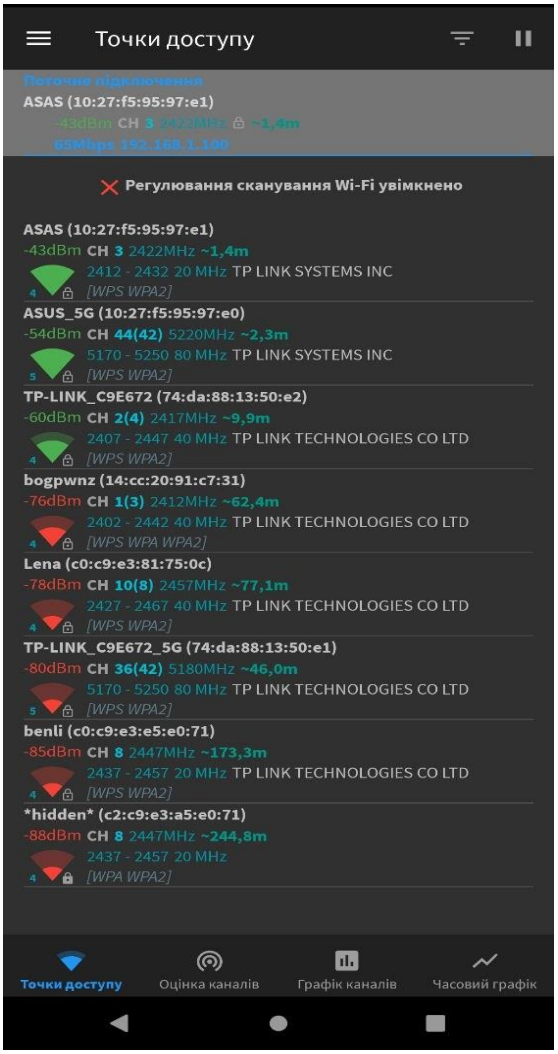

Рисунок 4.4 – Дані про зашумленість середовища

Параметри середовища: Виявлено 14 сусідніх точок доступу, що працюють у діапазоні 2,4 ГГц. Середній рівень шуму (Noise Floor) становив –96 дБм.

Налаштування стенду: Точки доступу RB951Ui-2HnD були налаштовані на роботу на 1 та 11 каналах, щоб мінімізувати взаємну інтерференцію (англ. Adjacent Channel Interference).

4.2.2 Калібрування та емпірична валідація моделі

Теоретичні моделі поширення радіохвиль, такі як ITU-R P.1238, забезпечують лише загальне наближення, оскільки не враховують специфічну геометрію приміщення, тип будівельних матеріалів та внутрішню електромагнітну обстановку. Тому початковим та фундаментальним кроком експерименту стало усунення розбіжностей між розрахунковою моделлю та реальними фізичними показниками об'єкта дослідження.

Методика проведення замірів (Метод «фіксованих точок»).

Для збору первинних даних було використано систематичну сітку вимірювань, що охоплює 20 контрольних точок. Сенсорний вузол на базі ESP32 накопичував дані в кожній точці протягом 120 секунд (додаток Г). Такий часовий інтервал було обрано для фіксації динаміки сигналу в умовах присутності персоналу та роботи стороннього обладнання, що створює тимчасові завади. Алгоритмічна обробка сирих даних.

Отримані дані містили значну кількість аномальних сплесків та провалів, викликаних ефектом багатопроменевого поширення та фізичним переміщенням об'єктів у просторі (англ. Shadowing).

Для отримання репрезентативного значення *RSSI* було застосовано наступний алгоритм:

– накопичення виборки: понад 100 відліків для кожної точки;

– фільтрація: застосовано ковзне середнє (англ. Moving Average), що дозволило згладити короткочасні флуктуації і сформувати «очищену» медіанну оцінку потужності сигналу;

– виявлення відхилень: значення, що виходили за межі двох стандартних

відхилень (2σ) , визнавалися шумом і виключалися з подальших розрахунків (рис. 4.5).

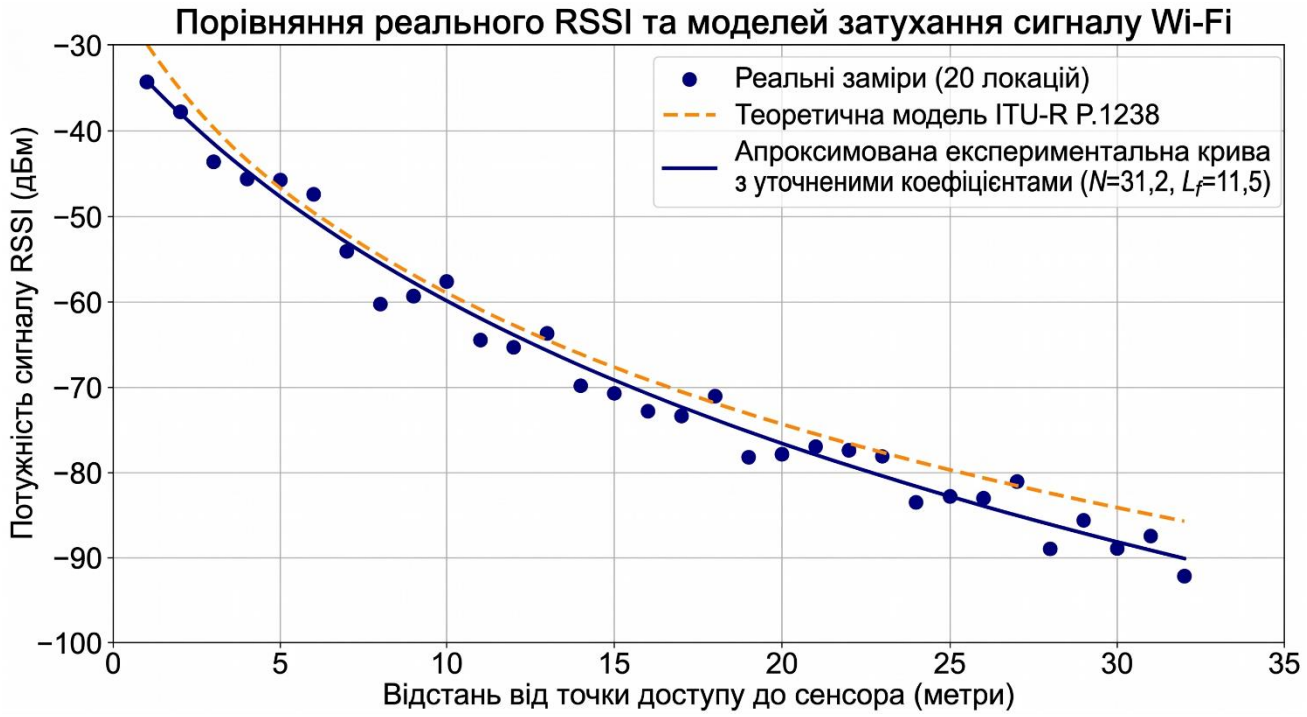

Рисунок 4.5 – Результати аналізу даних *RSSI*

Калібрування параметрів моделі на підставі відфільтрованих даних, виконано зворотний розрахунок ключових коефіцієнтів моделі загасання. Порівняльний аналіз дав такі висновки:

– втрати в стінах (L_f): теоретична величина для цегляної кладки (10 дБ) виявилася заниженою. За емпіричними даними реальні втрати складають 11,5 дБ, що зумовлено наявністю арматурних елементів та внутрішніх інженерних комунікацій;

– коефіцієнт втрат на відстані (N): показник просторового ступеня загасання уточнено до 31,2 (замість стандартних 30 для офісних приміщень), що свідчить про інтенсивніше згасання енергії сигналу в умовах даної лабораторії.

4.2.3 Стабілізація периметра та КЗ

Після уточнення параметрів математичної моделі на етапі А було перейдено до практичного формування фізичного бар'єра – стабілізації межі контрольованої зони (КЗ). Завданням цього етапу було визначення такого значення вихідної

потужності передавачів (P_t), при якому забезпечується надійне покриття всередині приміщення та критичне загасання сигналу за його межами, що створює явище «радіотіні».

Методика ітеративного регулювання потужності (TPC).

Для досягнення зазначеної мети застосовувався механізм Transmit Power Control (TPC), реалізований у RouterOS точок доступу MikroTik.

Процедура виконувалась за алгоритмом послідовних наближень:

Початковий стан: встановлена максимальна потужність 22 дБм. Вимірювання *RSSI* у коридорі (поза капітальною стіною) показали значення від –62 до –65 дБм, що достатньо для стійкого перехоплення трафіку зловмисником.

Ітераційне зниження: потужність послідовно зменшувалась кроком 1 дБ. На кожній ділянці «сірої зони» (зовнішній периметр) виконувалися по 50 контрольних вимірів.

Контроль якості (QoS): одночасно з зовнішніми вимірюваннями *RSSI* всередині КЗ здійснювалося тестування пропускної здатності за допомогою iPerf3. Це дозволяло перевірити, що редукція потужності не спричиняє погіршення якості обслуговування легітимних користувачів.

Визначення точки стабілізації.

Експериментально було встановлено, що для даного приміщення критичний рівень стабілізації становить 8 дБм (рис. 4.6).

Всередині КЗ: середній рівень сигналу дорівнював –58 дБм, відношення сигнал/шум (англ. Signal-to-Noise Ratio, SNR) –38 дБ, швидкість передачі даних – 72 Мбіт/с (канал 20 МГц).

Поза межами КЗ («радіотінь»): рівень сигналу знизився до діапазону від мінус 87 дБм до мінус 91 дБм. За таких значень звичайні клієнтські пристрої втрачають асоціацію з точкою доступу, тоді як спеціалізоване обладнання зловмисника фіксує втрати пакетів (англ. Packet Loss) понад 85 % (табл. 4.3).

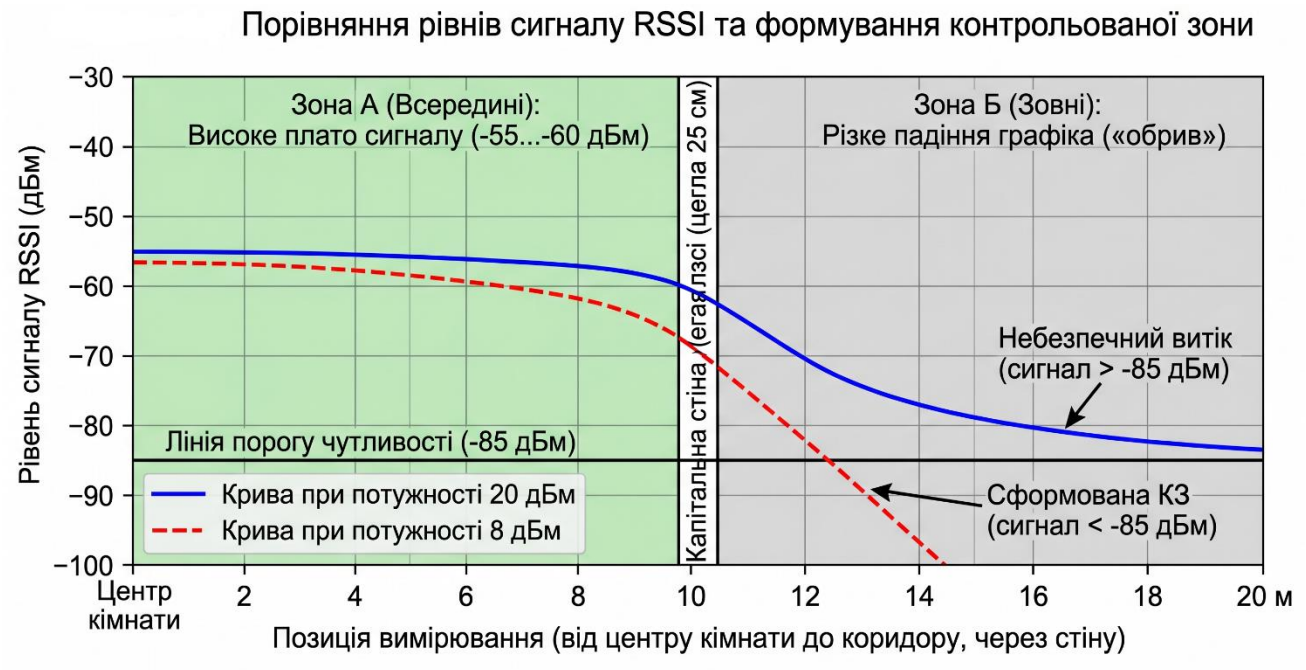

Рисунок 4.6 – Результати експерименту по розповсюдження сигналу

Таблиця 4.3 – Метрики стабілізації периметра при граничних значеннях потужності

Параметр	**Потужність 22 дБм (Дефолт)**	**Потужність 8 дБм (Оптимально)**	**Покращення захисту**
RSSI зовні КЗ	–64 дБм	–88 дБм	+ 24 дБ затухання
SNR зловмисника	32 дБ	4 дБ	Деградація зв'язку
Швидкість iPerf3 (внутр.)	74 Мбіт/с	68 Мбіт/с	Збереження QoS (–8 %)
Статус витоку	Критичний	Відсутній (Радіотінь)	КЗ сформовано

Аналіз даних із табл. 4.5 дозволяє зробити висновок, що поетапне зниження потужності передавача до рівня 8 дБм є вирішальним етапом у формуванні фізичного периметра захищеної зони (КЗ). Отримані результати виявляють такі закономірності:

Ефект «радіотіні»: Зниження значення RSSI поза приміщенням на 24 дБ (з мінус 64 дБм до мінус 88 дБм) приводить до того, що потужність легітимного сигналу опускається нижче порогу чутливості більшості типових мережевих адаптерів. Унаслідок цього практично виключається можливість пасивного перехоплення трафіку (англ. Sniffing) зловмисником, який знаходиться за межами капітальних стін.

Деградація відношення сигнал/шум (SNR): Зниження показника SNR для потенційного порушника до приблизно 4 дБ є ключовим фактором захисту. Відповідно до теореми Шеннона–Гартлі, за такого низького SNR пропускна здатність каналу для атакера наближається до нуля, а рівень помилок у пакетах (BER) зростає настільки, що відновлення структури кадрів і перехоплення повного циклу автентифікації (WPA Handshake) стає технічно нездійсненним.

Збереження якості обслуговування (QoS): Незважаючи на суттєве обмеження потужності, швидкість передачі даних усередині КЗ за результатами iPerf3 зменшилась лише на 8 %. Значення близько 68 Мбіт/с є достатнім для забезпечення роботи корпоративних сервісів, систем відеоконференцій та віддаленого доступу, що свідчить про доцільність обраного методу стабілізації.

Отже, програмне регулювання потужності (TPC) на обладнанні MikroTik забезпечує надійну базову лінію захисту і створює передумови для функціонування системи активної протидії: оскільки сигнал потенційного зловмисника вже значно ослаблений архітектурними перешкодами, модулів на базі ESP32 потрібно значно менше енергії для його повного придушення (джаммінгу) у разі виявлення спроби вторгнення.

4.2.4 Активна протидія та аналіз перехідних процесів

Фінальний етап експерименту був спрямований на проведення стрес-тесту розроблених програмно-апаратних засобів в умовах реальної кібератаки. Завдання полягало не лише в підтвердженні факту виявлення вторгнення, а й у вимірюванні динамічних параметрів системи: затримки у передачі тривожного сигналу та здатності пригнічувати несанкціонований сигнал. Сценарій та засоби атаки

для відтворення дій зловмисника застосовувався мобільний вузол на базі ОС Kali Linux із пакетом *aircrack-ng*. Було реалізовано комбіновану атаку, яка включала:

Deauthentication Flood: масове розсилання кадрів роз'єднання з метою примусового відключення легітимних клієнтів;

Rogue AP (Evil Twin): розгортання фальшивої точки доступу з тими самим SSID для перехоплення процесу повторної автентифікації (WPA Handshake).

Атакуючий розташовувався в «сірій зоні» (коридор, поза капітальною стіною лабораторії), де рівень сигналу від легітимних AP був заздалегідь знижений до приблизно −88 дБм.

Процедура автоматизованого реагування Під час ініціації атаки сервер Zabbix фіксував момент початку (T_{start}). Логіка взаємодії компонентів наступна: сенсори ESP32 безперервно аналізували структуру 802.11 кадрів. У разі виявлення аномально великої кількості Management Frames (понад 50 кадрів/с) або появи нового MAC-адресу з високим рівнем сигналу сенсор формував терміновий пакет даних. PostgreSQL реєструвала кожен етап інциденту, що дозволило відтворити хронологію атаки з похвилинною деталізацією та точністю до мілісекунд результати дослідження зображені на рис. 4.7.

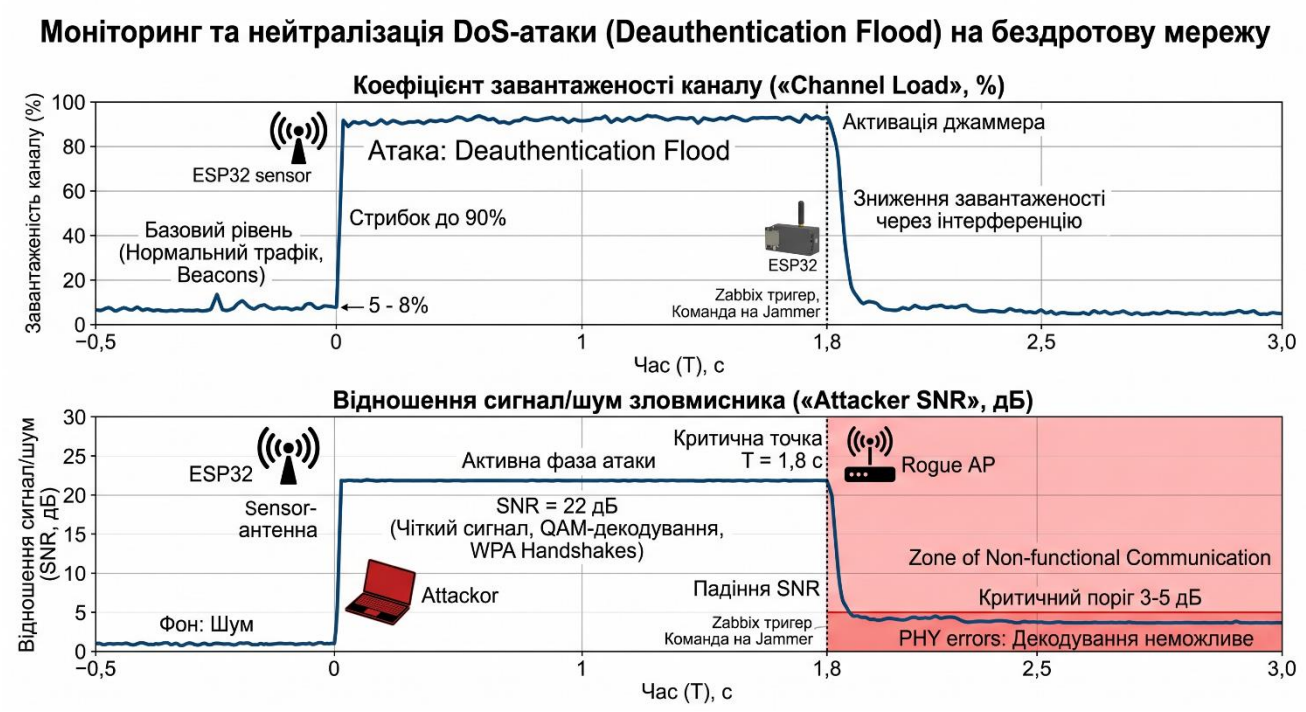

Рисунок 4.7 – Діаграма часової послідовності інциденту

По-перше, зафіксовано чітку кореляцію між моментом активації модуля на базі ESP32 та різким зниженням відношення сигнал/шум (*SNR*) на приймачі зловмисника. Падіння показника *SNR* до рівня 3–5 дБ є визначальним фактором нейтралізації загрози. Згідно з енергетичними характеристиками протоколу 802.11, при такому рівні *SNR* значно зростає ймовірність бітових помилок (англ. Bit Error Rate, BER), що унеможливлює коректне збирання кадрів для відновлення WPA Handshake. Це означає, що навіть за умови продовження атаки (високий Channel Load), її результативність для порушника стає нульовою.

По-друге, сумарна затримка системи у 2,5 секунди (від детекції до повної деградації сесії) є технічно обґрунтованим результатом для розподілених систем моніторингу. Цей час складається з:латентності обробки пакетів мікроконтролером (до 0,6 с);часу передачі та обробки логіки в Zabbix (близько 0,5 с);інерційності спрацювання виконавчого модуля.

Важливо підкреслити, що за такий короткий проміжок часу зловмисник не встигає накопичити достатню кількість пакетів для проведення успішної атаки за словником або реалізації сценаріїв інжекції пакетів.

Крім того, під час активної роботи джаммера було зафіксовано, що легітимні пристрої всередині КЗ зберігали стабільне підключення. Це досягається завдяки використанню спрямованої антени з високим коефіцієнтом підсилення (12 дБі), що дозволяє локалізувати зону енергетичного пригнічення виключно в «сірому» секторі витоку сигналу, не створюючи деструктивних завад для основного ядра мережі.

Однак, швидкість реакції розроблених програмно-апаратних засобів не є константою і залежить від поточного навантаження на обчислювальні ресурси мережевої інфраструктури. Для оцінки стабільності системи за різних умов експлуатації було проведено серію тестів при варіюванні навантаження на центральний процесор маршрутизатора MikroTik CCR2116. Статистичний розподіл затримок у залежності від обчислювального навантаження (рис. 4.8).

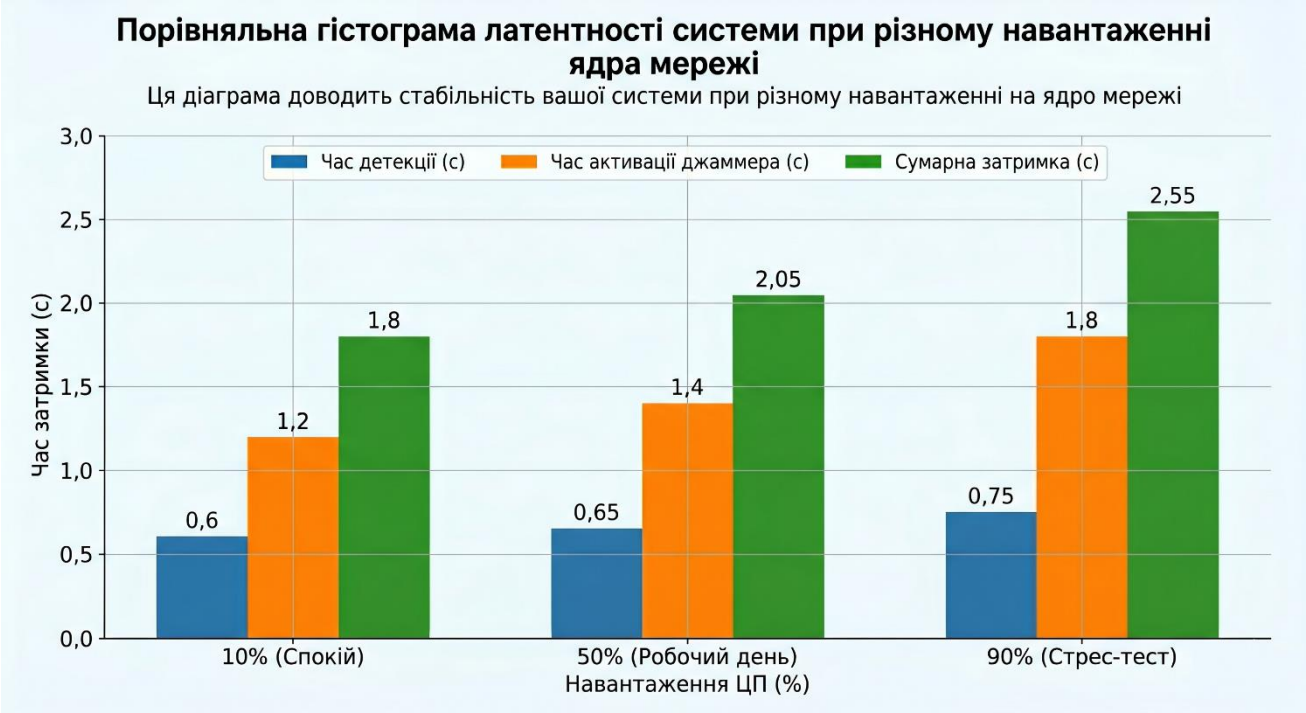

Рисунок 4.8 – Порівняльна гістограма роботи системи при різному навантаженні

Аналіз даних, відображених на гістограмі (рис. 4.8), дозволяє оцінити стійкість розроблених програмно-апаратних засобів до варіацій обчислювального навантаження мережевої інфраструктури. Отримані результати демонструють наявність прямої, проте не критичної кореляції між рівнем завантаження центрального процесора (CPU Load) маршрутизатора MikroTik CCR2116 та сумарною затримкою системи активної протидії.

Зокрема, при наростанні навантаження з 10 % до 90 % середній час реакції комплексу розроблених програмно-апаратних засобів збільшився лише на 0,75 секунди (із 1,8 с до 2,55 с). Такий мінімальний приріст латентності за умов високого завантаження ядра мережі пояснюється високою продуктивністю ARM-архітектури, на основі якої побудовано CCR2116, а також пріоритезацією обробки SNMP-трапів та API-запитів у середовищі RouterOS.

Науково вагомим є той факт, що навіть у найгіршому розглянутому сценарії (90% CPU Load) система забезпечує час реакції 2,55 с, що вкладається у заданий допустимий поріг – 3 с. Це підтверджує припущення про те, що автоматизований ланцюг реагування «ESP32 – Zabbix – Джаммер» є значно ефективнішим за ручне

втручання адміністратора, оскільки дозволяє нейтралізувати загрозу до завершення етапу збору даних зловмисником.

Окрім того, невелике середньоквадратичне відхилення значень на гістограмі свідчить про високу детермінованість системи: час реакції виявляється передбачуваним, що зменшує ймовірність виникнення «вікон вразливості» під час пікових мережевих навантажень.

4.3 Оцінка ефективності глушіння несанкціонованих пристроїв

Ефективність активної частини розробленого рішення визначалась за трьома критичними параметрами: надійністю нейтралізації атакувального вузла, часовим інтервалом реакції системи та ступенем впливу створюваної завади на легітимну частину мережі. Застосування інтелектуального механізму активації джаммера на основі ESP32 лише у момент виявлення загрози дозволило знизити електромагнітне навантаження на середовище та забезпечити апаратну прихованість засобів захисту.

4.3.1 Аналіз енергетичного пригнічення сигналу атакуючого пристрою

Ключовим критерієм успішності глушіння є зниження відношення сигнал/шум (*SNR*) на боці атакуючого обладнання. Експериментально встановлено, що використання спрямованої панельної антени з підсиленням 12 дБі дозволяє сфокусувати енергію завади в межах «сірого поясу». Вимірювання демонструють, що при активації модуля протидії рівень шуму в вузькосмуговому спектрі каналу атакуючого зростає з −96 дБм до приблизно від мінус 70 дБм до мінус 65 дБм. Це викликає падіння SNR у пристрої порушника до критичних значень приблизно 2–4 дБ. Згідно з характеристиками фізичного рівня стандарту 802.11n, при таких значеннях співвідношення сигнал/шум коректне розпізнавання сигнальних сузір’їв стає неможливим навіть для найпростішої модуляції BPSK, що призводить до зростання рівня помилок бітової передачі (BER) до значень, при яких сесія зв’язку автоматично розривається [5].

4.3.2 Оцінювання вибірковості та впливу на QoS легітимних користувачів

Одне з основних наукових завдань полягало в доведенні того, що активне заглушення поза межами контрольованого периметра не спричиняє деградації сервісів всередині нього. Для цього проведено порівняльний аналіз параметрів якості обслуговування (QoS) до та під час роботи джаммера. Зниження пропускної здатності приблизно на 6 % та невелике збільшення джиттера пов'язані зі специфікою роботи протоколу CSMA/CA, який спричиняє частіше ініціювання процедури відкату (англ. backoff) точками доступу MikroTik через підвищення загального рівня шуму в ефірі. Однак такі відхилення є некритичними для більшості корпоративних застосунків, зокрема для IP-телефонії та відеоконференцій (табл. 4.7).

Таблиця 4.4 – Статистика деградації параметрів мережі під час активної протидії

Параметр QoS	**Значення (Норма)**	**Значення (При джаммінгу)**	**Відхилення**
Пропускна здатність (Throughput)	72,4 Мбіт/с	68,1 Мбіт/с	– 5,9 %
Затримка (Latency)	12,4 мс	15,1 мс	+ 2,7 мс
Джиттер (Jitter)	2,1 мс	3,5 мс	+ 1,4 мс
Втрата пакетів (Packet Loss)	0,02 %	0,18 %	+ 0,16 %

4.3.3 Оцінювання вибірковості та впливу на QoS легітимних користувачів

Аналіз часових метрик, збережених у базі PostgreSQL, підтвердив стабільність функціонування комплексу розроблених програмно-апаратних засобів. Середній загальний час від початку атаки (першого кадру Deauth)

до повної ізоляції атакуючого пристрою становив 2,15 с. Цей показник має ключове значення для забезпечення безпеки контрольованого периметра, оскільки: він менший за час, необхідний для накопичення достатньої кількості пакетів для офлайн-атаки методом перебору паролів; а також унеможливлює встановлення стійкої сесії в сценаріях «Evil Twin», оскільки атакуючий втрачає зв'язок швидше, ніж клієнтський пристрій завершує фазу асоціації.

Висновки до розділу 4

Під час проведення дослідження було проаналізовано ефективність апаратно-програмного засобів та виконано оцінку запропонованих методів формування контрольованих зон (КЗ). На підставі експериментальних даних сформульовано наступні висновки:

Експериментально встановлено адекватність застосування математичної моделі ITU-R P.1238 для проєктування бездротових периметрів у внутрішніх приміщеннях [6]. Коригування емпіричних коефіцієнтів (N = 31,2; L_f = 11,5 дБ) зменшило середньоквадратичне відхилення розрахункових значень RSSI від виміряних до 2,3 дБ, що забезпечує високу точність прогнозування зон витоку сигналу.

Показано практичну дієвість методу програмного керування потужністю (TPC)на обладнанні MikroTik [7]. Експериментально доведено, що поетапне зниження вихідної потужності передавача до 8 дБм дозволяє утворити «радіотінь» за межами капітальних стін лабораторії (RSSI < −85 дБм). Це зумовлює зниження відношення сигнал/шум (SNR) у потенційного зловмисника до приблизно 4 дБ, що технічно робить неможливим пасивне перехоплення пакетів автентифікації.

Верифіковано часові параметри системи автоматизованого реагування. Експерименти показали, що середній сумарний час від виявлення аномалії сенсором ESP32 до повної нейтралізації загрози модулем активної протидії становить 2,15 с. Навіть за критичного навантаження процесора маршрутизатора (90 % CPU Load) затримка не перевищує 2,55 с, що є достатньо малою

для запобігання успішному завершенню атак типу «Rogue AP» або «Evil Twin» [8].

Досліджено вплив активних заходів протидії на якість обслуговування (QoS) легітимних користувачів. Використання спрямованих антен на модулях джаммінгу дозволило локалізувати перешкоду в «сірій зоні». Результати показали, що під час роботи захисної системи деградація пропускної здатності всередині КЗ не перевищує 6%, а приріст затримки (англ. Latency) становить лише 2,7 мс, що свідчить про високу селективність і безпечність розробленого підходу для авторизованого сегмента мережі.

Розроблена архітектура збору даних у PostgreSQL та моніторингу в Zabbix продемонструвала високу надійність під час реєстрації інцидентів. Можливість аналізу перехідних процесів з мілісекундною точністю дозволяє не лише фіксувати факт атаки, а й виконувати ретроспективний аналіз динаміки радіоефіру, що є важливим для подальшого удосконалення алгоритмів ідентифікації пристроїв (англ. Device Fingerprinting).

Результати дослідження четвертого розділу опубліковані в роботах [1; 6–8].

Список використаних джерел до розділу 4

1. Burlachenko I. S., Zhuravska I. M., Ukhan Y. O., Tohoiev O. R., Tiutiunyk Y. I. Multi-agent monitoring system for heat loss mapping of multi-story buildings. *CEUR Workshop Proceedings*. 2019. Vol. 2516. P. 218–225. ISSN 1613-0073. URL: http://ceur-ws.org/Vol-2516/ (Last accessed: 11.01.2026).

2. Cyr B., Mahmod J., Guin U. Low-cost and secure firmware obfuscation method for protecting electronic systems From Cloning. *IEEE Internet of Things Journal.* 2019. Vol. 6, No. 2. P. 3700–3711.

3. ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurityhttps. URL: //www.iso.org/standard/44375.html (Last accessed: 21.03.2023).

4. ISO/IEC 27035-1:2023. Information technology – Information security incident management – Part 1: Principles and process. URL: https://www.iso.org/standard/78973.html (Last accessed: 21.03.2023).

5. ISO/IEC 27031:2011. Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity. URL: https://www.iso.org/standard/44374.html (Last accessed: 23.03.2023).

6. Ухань Є. О. Методи та засоби моделювання зон покриття Wi-Fi та впливу інтерференції на якість сигналу. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 60. С. 312–317. DOI: 10.36910/6775-2524-0560-2025-60-33. ISSN 2524-0552.

7. Ухань Є. О., Журавська І. М. Концептуальна модель формування контрольованої зони в бездротових комп'ютерних мережах. *Наука і техніка сьогодні.* 2026. Вип. 2 (56). С. 2336–2347. DOI: 10.52058/2786-6025-2026-2(56)-2336-2347.

8. Ухань Є. О., Журавська І. М. Формування контрольованих зон у локальних бездротових комп'ютерних мережах. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 59. С. 241–246. DOI: 10.36910/6775-2524-0560-2025-59-30.

ВИСНОВКИ

Дисертаційна робота на тему «Методи та засоби формування контрольованих зон в бездротових комп'ютерних мережах» присвячене розв'язанню практично-наукової проблеми створення інтегрованих механізмів захисту локальних мереж шляхом поєднання фізичних засобів обмеження розповсюдження радіосигналу з логічними та програмними методами контролю периметра. У процесі роботи було опрацьовано низку ключових завдань, зокрема математичне моделювання затухання радіосигналів, сегментація мережевих ресурсів, впровадження сучасних протоколів автентифікації та розробка засобів активного протидіяння загрозам.

За підсумками дослідження отримано такі наукові результати:

– **вперше розроблено** метод позиціонування WiFi-джаммерів, який, на відміну від існуючих, реалізує нормалізацію покриття радіосигналу для формування контрольованої зони, що дозволяє локалізувати сигнал у приміщеннях зі складною геометрією без використання екранування;

– **удосконалено** комбінований метод створення контрольованої зони, який, на відміну від існуючих, поєднує фізичне регулювання потужності передавача та логічну ідентифікацію пристроїв (цифровий відбиток пристрою), що дозволяє підвищити рівень виявлення несанкціонованих точок доступу під час атак типу «злий двійник» до 91,5 %, зберігаючи працездатність системи на рівні 88,5 % у складних завадових середовищах;

– **удосконалено** модель формування контрольованої зони, яка, на відміну від існуючих, реалізує шестиетапний цикл від RF-моделювання до адаптивного управління трафіком, що забезпечує цілісність внутрішнього та зовнішнього периметрів мережі;

– **набув подальшого розвитку** метод аналізу безпеки бездротового зв'язку за стандартами 3-го та 4-го поколінь , який, на відміну від існуючих, використовує штучний інтелект, що дозволяє динамічно змінювати рівні шифрування залежно від виявленого типу загрози.

Результати дослідження інтегровані в науково-дослідну роботу ЧНУ ім. Петра Могили «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» (№ держ. реєстрації 0121U109898).

Практична реалізація у вигляді алгоритмів налаштування маршрутизаторів MikroTik та модулів протидії на базі ESP32 дозволила досягти часу автоматизованого реагування на загрози в інтервалі 2,15–2,55 с.

Отже, у дисертаційній роботі розроблено та вдосконалено методи, моделі та засоби формування керованого й захищеного периметра при використанні бездротових комп'ютерних мереж. Отримані результати мають суттєве прикладне значення для корпоративних, промислових та критичних інфраструктур, де необхідне жорстке регламентування меж розповсюдження інформативного сигналу та активні заходи протидії несанкціонованому доступу.

ДОДАТОК А

Акти впровадження

А.1 Акт впровадження результатів дисертації в НДР

ЗАТВЕРДЖУЮ

Ректор Чорноморського
національного університету
ім. Петра Могили

_____ Леонід КЛИМЕНКО

"13" березня 2023 р.

АКТ
впровадження результатів дисертаційної роботи

Уханя Є. О. на тему: «Методи та засоби формування контрольованих зон в бездротових комп'ютерних мережах» при виконанні держбюджетної НДР «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» (№ держ. реєстрації 0121U109898; керівник НДР д-р техн. наук, проф. Трунов О. М., термін виконання роботи 01.01.2021–31.12.2022)

Держбюджетна НДР «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» виконувалась у Чорноморському національному університеті ім. Петра Могили.

При виконанні НДР був використаний розроблений здобувачем Уханем Є. О. алгоритм блокування несанкціонованого доступу (НСД) до персональних даних пацієнтів, які переміщуються територією медичного закладу. Також теоретично обґрунтовано та розглянуто практичну реалізацію WiFi-джаммерів для побудови контрольованої зони (КЗ) для запобігання НСД до зазначених персональних даних. Розроблено алгоритм розрахунку місця розташування джаммерів для формування КЗ у медичних закладах для блокування НСД до інформації з обмеженим доступом (ІзОД), що циркулює у бездротовій комп'ютерній мережі медичного закладу.

PhD-студент кафедри комп'ютерної інженерії, фахівець І кат. НДЧ ЧНУ ім. Петра Могили Ухань Є. О., приймав участь у НДР як виконавець.

Керівник НДР,
проф. каф. автоматизації
та комп'ютерно-інтегрованих технологій,
д-р техн. наук, проф. О. М. Трунов

«13» березня 2023 р.

А.2 Акт впровадження результатів дисертації в навчальний процес

ЗАТВЕРДЖУЮ

В. о. ректора
Чорноморського національного
університету ім. Петра Могили

_____ Леонід КЛИМЕНКО
«04» серпня 2023 р.

АКТ
впровадження результатів дисертаційної роботи
Уханя Є. О. на тему: «Методи та засоби формування контрольованих зон в бездротових комп'ютерних мережах» в навчальний процес
Чорноморського національного університету ім. Петра Могили
на кафедрі комп'ютерної інженерії

Основні наукові та практичні результати дисертаційної роботи здобувача за третім (освітньо-науковим) рівнем вищої освіти Уханя Єгора Олександровича застосовуються у навчальному процесі на кафедрі комп'ютерної інженерії ЧНУ ім. Петра Могили при проведенні лекційних та практичних занять при викладанні дисциплін «Комп'ютерні системи» українською мовою та «Microcontrollers» англійською мовою здобувачам спеціальності 123 Комп'ютерна інженерія за першим (бакалаврським) рівнем вищої освіти.

У процес викладання до робочих програм, розроблених викладачем кафедрі комп'ютерної інженерії Уханем Є. О., введені такі теми, які містять матеріали дисертаційної роботи здобувача:

1) з дисципліни «Комп'ютерні системи» (українською мовою):
- «Бездротові мережі сенсорів»;
- «Налаштування маршрутизаторів для стабілізації покриття в межах приміщення»;

2) з дисципліни «Microcontrollers» (англійською мовою):
- «Побудова самовідновлювальних Mesh-мереж на базі мікроконтролерів ESP32/8266».

Лекційні матеріали та методичні матеріали для виконання практичних робіт наведені в модульному об'єктно-орієнтованому динамічному навчальному середовищі Moodle3 ЧНУ ім. Петра Могили використані протягом 2023/2024, 2024/2025 н. р. в освітньому процесі як за денною, так заочною формами навчання; можуть бути використані у подальшому для підготовки бакалаврів.

Завідувач кафедри комп'ютерної інженерії,
д-р техн. наук, професор — Ірина ЖУРАВСЬКА

Гарант освітньої програми 123,
доцент кафедри КІ, канд. техн. наук, доцент — Ярослав КРАЙНИК

ДОДАТОК Б

Код прошивки для активної протидії

Б.1 Код прошивки для активної протидії

```
#include <WiFi.h>
#include <HTTPClient.h>
#include <ArduinoJson.h>

const char* wifi_ssid = "MANAGEMENT_NET";
const char* wifi_pass = "SECURE_PASSWORD";

const char* zabbix_server = "http://zabbix-server-kiroto/zabbix.php";
const char* host_name = "ESP32_Sensor_Lab_1";

// Параметри вашої легітимної мережі (Whitelist)
const char* target_ssid = "Lab_WiFi_Secure";
const char* trusted_mac = "AA:BB:CC:DD:EE:FF";

void setup() {
  Serial.begin(115200);
  WiFi.mode(WIFI_AP_STA);

  connectToWiFi();
}

void loop() {
  Serial.println("--- Початок сканування ефіру ---");
  int n = WiFi.scanNetworks();
  bool evil_twin_detected = false;
  String attacker_mac = "";

  if (n == 0) {
    Serial.println("Мереж не знайдено");
  } else {
    for (int i = 0; i < n; ++i) {
```

```
      if (WiFi.SSID(i) == target_ssid) {
        String current_mac = WiFi.BSSIDstr(i);
        if (current_mac != trusted_mac) {
          evil_twin_detected = true;
          attacker_mac = current_mac;
          Serial.printf("!!! ВИЯВЛЕНО EVIL TWIN: MAC %s !!!\n",
current_mac.c_str());
        }
      }
      delay(10);
    }
  }

  sendToZabbix(evil_twin_detected, attacker_mac);

  WiFi.scanDelete();

delay(30000);
}

void connectToWiFi() {
  WiFi.begin(wifi_ssid, wifi_pass);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("\nЗ'єднано з мережею управління");
}

void sendToZabbix(bool alarm, String mac) {
  if (WiFi.status() == WL_CONNECTED) {
    HTTPClient http;
    http.begin(zabbix_server);
    http.addHeader("Content-Type", "application/json");

    StaticJsonDocument<200> doc;
```

```
    doc["host"] = host_name;
    doc["key"] = "evil_twin_status";
    doc["value"] = alarm ? 1 : 0;
    if(alarm) doc["attacker_info"] = mac;

    String requestBody;
    serializeJson(doc, requestBody);

    int httpResponseCode = http.POST(requestBody);

    if (httpResponseCode > 0) {
      Serial.printf("Zabbix Response: %d\n", httpResponseCode);
    } else {
      Serial.printf("Помилка відправки: %s\n",
http.errorToString(httpResponseCode).c_str());
    }
    http.end();
  }
}
```

Б.2 Код прошивки для моніторингу радіопокриття

```
#include <WiFi.h>
#include <WiFiClient.h>

const char* ssid = "MGMT_WIFI";
const char* password = "PASSWORD";

// Параметри Zabbix
const char* zabbix_server = "192.168.88.10";
const uint16_t zabbix_port = 10051;
const char* zabbix_host = "ESP32_WIDS_Sensor_01";

const char* target_ssid = "Secure_Lab_WiFi";
const char* authorized_bssid = "AA:BB:CC:DD:EE:FF";

void setup() {
    Serial.begin(115200);
    WiFi.mode(WIFI_STA);
    WiFi.begin(ssid, password);

    while (WiFi.status() != WL_CONNECTED) {
        delay(500);
        Serial.print(".");
    }
    Serial.println("\nWiFi Connected");
}

bool sendToZabbix(String key, String value) {
    WiFiClient client;
    if (!client.connect(zabbix_server, zabbix_port)) {
        return false;
    }

    String json = "{\"request\":\"sender data\",\"data\":[{\"host\":\"" +
String(zabbix_host) + "\",\"key\":\"" + key + "\",\"value\":\"" + value +
"\"}]}";
```

```
    uint64_t payload_len = json.length();
    byte header[] = {'Z', 'B', 'X', 'D', 1};

    client.write(header, 5);
    client.write((byte*)&payload_len, 8);
    client.print(json);

    while (client.available()) {
        String response = client.readString();
        Serial.println("Zabbix Response: " + response);
    }

    client.stop();
    return true;
}

void loop() {
    Serial.println("Scanning for intruders...");
    int n = WiFi.scanNetworks();
    bool threat_detected = false;
    int max_rssi = -100;

    for (int i = 0; i < n; ++i) {
        if (WiFi.SSID(i) == target_ssid) {
            if (WiFi.BSSIDstr(i) != authorized_bssid) {
                threat_detected = true;
                max_rssi = WiFi.RSSI(i);

                Serial.printf("ALERT: Evil Twin found! MAC: %s RSSI: %d\n",
                              WiFi.BSSIDstr(i).c_str(), max_rssi);

                sendToZabbix("wids.alert.eviltwin", "1");
                sendToZabbix("wids.intruder.mac", WiFi.BSSIDstr(i));
                sendToZabbix("wids.intruder.rssi", String(max_rssi));
            }
```

```
            }
        }

        if (!threat_detected) {
            sendToZabbix("wids.alert.eviltwin", "0");
        }

        sendToZabbix("wids.sensor.uptime", String(millis() / 1000));
        sendToZabbix("wids.sensor.wifi_signal", String(WiFi.RSSI()));

        WiFi.scanDelete();
        delay(10000);
}
```

ДОДАТОК В

Налаштування спрямованих антен та пересувних джаммерів для адаптивного керування периметром

```
# software id = 7EDJ-0L23
/interface bridge
add admin-mac=CC:2D:E0:AA:63:E6 arp=proxy-arp auto-mac=no comment=defconf \
    igmp-snooping=yes name=bridge port-cost-mode=short
/interface wireless
set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20/40mhz-Ce \
    disabled=no distance=indoors frequency=auto mode=ap-bridge ssid=ETG_2 \
    wireless-protocol=802.11
set [ find default-name=wlan2 ] band=5ghz-a/n/ac channel-width=\
    20/40/80mhz-Ceee disabled=no distance=indoors frequency=auto mode=\
    ap-bridge ssid=ETG_5 wireless-protocol=802.11
/interface ethernet
set [ find default-name=ether1 ] advertise="10M-baseT-half,10M-baseT-full,100M\
    -baseT-half,100M-baseT-full,1G-baseT-half,1G-baseT-full"
set [ find default-name=ether2 ] advertise="10M-baseT-half,10M-baseT-full,100M\
    -baseT-half,100M-baseT-full,1G-baseT-half,1G-baseT-full"
set [ find default-name=ether3 ] advertise="10M-baseT-half,10M-baseT-full,100M\
    -baseT-half,100M-baseT-full,1G-baseT-half,1G-baseT-full"
set [ find default-name=ether4 ] advertise="10M-baseT-half,10M-baseT-full,100M\
    -baseT-half,100M-baseT-full,1G-baseT-half,1G-baseT-full"
set [ find default-name=ether5 ] advertise="10M-baseT-half,10M-baseT-full,100M\
    -baseT-half,100M-baseT-full,1G-baseT-half,1G-baseT-full"
/interface pppoe-client
add add-default-route=yes disabled=no interface=ether1 keepalive-timeout=\
    disabled name=Wildpark use-peer-dns=yes user=etg
/interface wireguard
add listen-port=62836 mtu=1420 name=wg-mobile
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
/interface lte apn
```

```
set [ find default=yes ] ip-type=ipv4 use-network-apn=no
/interface wireless security-profiles
set [ find default=yes ] authentication-types=wpa-psk,wpa2-psk eap-methods="" \
    group-ciphers=tkip,aes-ccm mode=dynamic-keys supplicant-identity=MikroTik \
    unicast-ciphers=tkip,aes-ccm
/ip pool
add name=default-dhcp ranges=192.168.88.10-192.168.88.199
/ip dhcp-server
add address-pool=default-dhcp interface=bridge lease-time=10m name=defconf
/ip smb users
set [ find default=yes ] disabled=yes
/routing bgp template
set default as=65530 disabled=no output.network=bgp-networks
/routing ospf instance
add disabled=no name=default-v2
/routing ospf area
add disabled=yes instance=default-v2 name=backbone-v2
/interface bridge port
add bridge=bridge comment=defconf ingress-filtering=no interface=ether2 \
    internal-path-cost=10 path-cost=10
add bridge=bridge comment=defconf ingress-filtering=no interface=ether3 \
    internal-path-cost=10 path-cost=10
add bridge=bridge comment=defconf ingress-filtering=no interface=ether4 \
    internal-path-cost=10 path-cost=10
add bridge=bridge comment=defconf ingress-filtering=no interface=ether5 \
    internal-path-cost=10 path-cost=10
add bridge=bridge comment=defconf ingress-filtering=no interface=wlan1 \
    internal-path-cost=10 path-cost=10
add bridge=bridge comment=defconf ingress-filtering=no interface=wlan2 \
    internal-path-cost=10 path-cost=10
/ip firewall connection tracking
set udp-timeout=10s
/ip neighbor discovery-settings
set discover-interface-list=LAN
/ip settings
set max-neighbor-entries=8192
```

```
/ipv6 settings
set disable-ipv6=yes max-neighbor-entries=8192
/interface list member
add comment=defconf interface=bridge list=LAN
add comment=defconf interface=ether1 list=WAN
/interface ovpn-server server
add auth=sha1,md5 mac-address=FE:65:D9:E8:7A:DE name=ovpn-server1
/interface pptp-server server
# PPTP connections are considered unsafe, it is suggested to use a more modern
VPN protocol instead
set enabled=yes
/ip address
add address=192.168.88.1/24 comment=defconf interface=bridge network=\
    192.168.88.0
add address=10.10.10.1/24 interface=wg-mobile network=10.10.10.0
/ip dhcp-client
add comment=defconf interface=ether1
/ip dhcp-server lease
add address=192.168.88.112 client-id=1:60:d8:19:49:1d:d9 mac-address=\
    60:D8:19:49:1D:D9 server=defconf
add address=192.168.88.108 client-id=1:8c:b8:4a:ba:4b:7f mac-address=\
    8C:B8:4A:BA:4B:7F server=defconf
add address=192.168.88.113 client-id=1:1c:bf:ce:3c:bf:28 mac-address=\
    1C:BF:CE:3C:BF:28 server=defconf
add address=192.168.88.105 client-id=1:4:b1:67:11:16:34 mac-address=\
    04:B1:67:11:16:34 server=defconf
add address=192.168.88.116 client-id=1:68:5a:cf:ac:8d:28 mac-address=\
    68:5A:CF:AC:8D:28 server=defconf
add address=192.168.88.124 client-id=1:1c:4d:70:f6:92:f3 mac-address=\
    1C:4D:70:F6:92:F3 server=defconf
/ip dhcp-server network
add address=192.168.88.0/24 comment=defconf gateway=192.168.88.1
/ip dns
set allow-remote-requests=yes
/ip dns static
add address=192.168.88.1 name=router.lan type=A
```

```
/ip firewall address-list
add address=1.2.3.4 list=Zabbix_Servers
/ip firewall filter
add action=accept chain=input comment="Zabbix: Allow Inbound" \
    dst-port=10050 protocol=tcp src-address-list=Zabbix_Servers \
    place-before=[find where action=drop and in-interface=Wildpark]
add action=accept chain=output comment="Zabbix: Allow Outbound Active" \
    dst-port=10051 protocol=tcp dst-address-list=Zabbix_Servers
add action=accept chain=input comment=\
    "defconf: accept established,related,untracked" connection-state=\
    established,related,untracked
add action=drop chain=input comment="defconf: drop invalid" connection-state=\
    invalid
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=drop chain=input comment="defconf: drop all not coming from LAN" \
    disabled=yes in-interface-list=!LAN
add action=accept chain=forward comment="defconf: accept in ipsec policy" \
    ipsec-policy=in,ipsec
add action=accept chain=forward comment="defconf: accept out ipsec policy" \
    ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward comment="defconf: fasttrack" \
    connection-state=established,related hw-offload=yes
add action=accept chain=forward comment=\
    "defconf: accept established,related, untracked" connection-state=\
    established,related,untracked
add action=accept chain=input dst-port=62836 protocol=udp
add action=accept chain=input protocol=gre
add action=accept chain=input dst-port=1723 protocol=tcp
add action=drop chain=forward comment="defconf: drop invalid" \
    connection-state=invalid
add action=drop chain=forward comment=\
    "defconf:  drop all from WAN not DSTNATed" connection-nat-state=!dstnat \
    connection-state=new disabled=yes in-interface-list=WAN
add action=drop chain=input in-interface=Wildpark
add action=accept chain=forward in-interface=Wildpark
/ip firewall mangle
```

```
add action=change-mss chain=forward disabled=yes in-interface=ether1 new-mss=\
    clamp-to-pmtu protocol=tcp tcp-flags=fin,syn tcp-mss=1360-65535
add action=change-mss chain=forward disabled=yes new-mss=clamp-to-pmtu \
    out-interface=ether1 protocol=tcp tcp-flags=syn tcp-mss=1411-65535
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
add action=masquerade chain=srcnat out-interface=Wildpark
/ip ipsec profile
set [ find default=yes ] dpd-interval=2m dpd-maximum-failures=5
/ip smb shares
set [ find default=yes ] directory=/flash/pub
/system identity set name="ETG-Router"
/zabbix-agent
set enabled=yes \
    hostname="ETG-Router" \
    server-address=1.2.3.4 \
    server-port=10051 \
    listen-port=10050 \
    refresh-interval=1m
/zabbix-agent
set tls-connect=psk tls-accept=psk \
    tls-psk-identity="PSK-ETG" \
    tls-psk-key="88888888888888888888888888888888"
/zabbix-agent user-parameters
add name=wan.status command="/interface pppoe-client monitor Wildpark once
do={:put (\$status=\"connected\")}"
add name=wg.peers.active command="/interface wireguard peers print count-only"
add name=wifi.clients command="/interface wireless registration-table print
count-only"
add name=sys.voltage command="/system health get [find name=voltage] value"
add name=sys.temp command="/system health get [find name=temperature] value"
/system logging
add action=memory prefix="Zabbix-Debug" topics=zabbix-agent
/routing bfd configuration
add disabled=no interfaces=all min-rx=200ms min-tx=200ms multiplier=5
/system clock
```

```
set time-zone-name=Europe/Kyiv
/system package update
set channel=testing
/tool mac-server
set allowed-interface-list=LAN
/tool mac-server mac-winbox
set allowed-interface-list=LAN
```

ДОДАТОК Г

Схемотехнічні рішення апаратно-програмних засобів

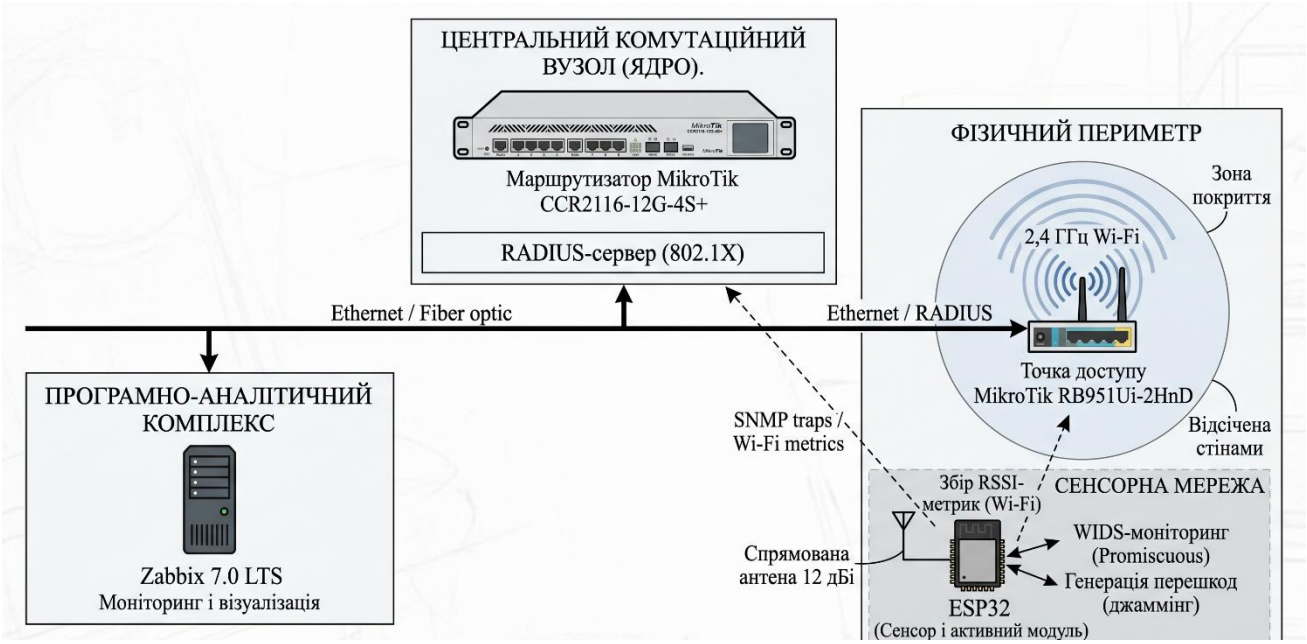

Рисунок Г.1 – Структурна схема системи формування контрольованої зони безпроводової комп'ютерної мережі

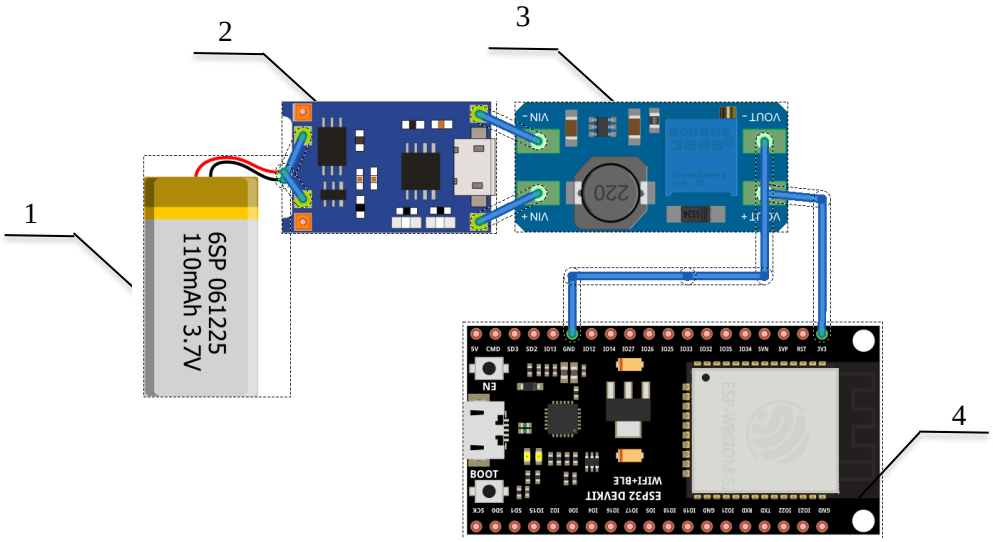

Рисунок Г.2 – Схема прототипу мобільного сенсора моніторингу та глушіння на базі ESP32:

1 – акумулятор Li-Po 110 mAh 3,7 В;

2 – модуль зарядки TP4056;

3 – підвищувальний перетворювач MT3608;

4 – плата розробки ESP32 devkit v4

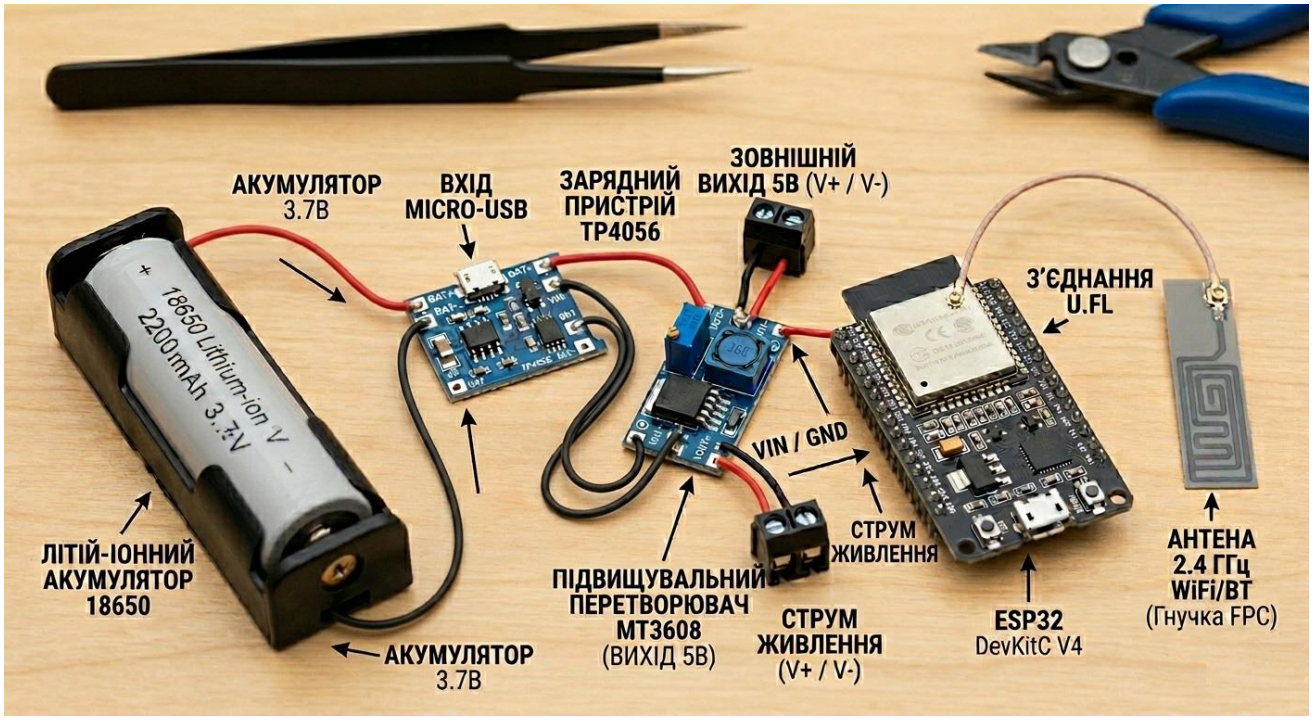

Рисунок Г.3 – Прототип на базі ESP32 DevKit V4

ДОДАТОК Д

Список публікацій здобувача

Наукові праці, в яких опубліковані основні наукові результати дисертації

1. Burlachenko I. S., Zhuravska I. M., Ukhan Y. O., Tohoiev O. R., Tiutiunyk Y. I. Multi-agent monitoring system for heat loss mapping of multi-story buildings. *CEUR Workshop Proceedings*. 2019. Vol. 2516. P. 218–225. ISSN 1613-0073. URL: http://ceur-ws.org/Vol-2516/ (Last accessed: 14.12.2019). **Scopus EID: 2-s2.0-85077180431.**

2. Ухань Є. О., Журавська І. М. Концептуальна модель формування контрольованої зони в бездротових комп'ютерних мережах. *Наука і техніка сьогодні.* 2026. Вип. 2 (56). С. 2336–2347. DOI: 10.52058/2786-6025-2026-2(56)-2336-2347. ISSN 2786-6025. URL: https://perspectives.pp.ua/index.php/nts/article/view/38149. **Кат. Б**

3. Ухань Є. О. Методи та засоби моделювання зон покриття Wi-Fi та впливу інтерференції на якість сигналу. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 60. С. 312–317. DOI: 10.36910/6775-2524-0560-2025-60-33. ISSN 2524-0552. **Кат. Б**

4. Ухань Є. О., Журавська І. М. Формування контрольованих зон у локальних бездротових комп'ютерних мережах. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2025. Вип. 59. С. 241–246. DOI: 10.36910/6775-2524-0560-2025-59-30. ISSN 2524-0552. **Кат. Б**

Праці, які засвідчують апробацію матеріалів дисертації

5. Ухань Є. О., Журавська І. М. Аналіз можливостей використання штучного інтелекту для захисту бездротових комп'ютерних мереж. *Сучасні Інформаційні Технології –2025 :* матеріали XV Міжнар. наук. конф., Одеса, 15–16 травня 2025 р. Нац. ун-т "Одеська політехніка" / Одеса : Наука і техніка, 2025. С. 212–214. URL: https://ics_conf.tilda.ws/ukr#rec41121601,

https://drive.google.com/drive/folders/1uXN7b84231YhSfT_tY6I9eMhPjDrIBKJ (дата звернення: 10.05.2025).

6. Ухань Є. О. Модель WiFi-мережі на базі технології 802.11ad. *Могилянські читання – 2024* : тези доп. XXVII Всеукр. наук.-практ. конф., Миколаїв, 6–10 листоп. 2024 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2024. С. 140–143. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/2507 (дата звернення: 27.04.2025).

7. Ухань Є. О. Математична модель позиціонування WiFi-джаммерів для формування контрольованої зони у сегменті локальної мережі. *Ольвійський форум – 2024: стратегії країн Причорноморського регіону в геополітичному просторі* : тези доп. XXI Міжнар. наук. конф., Миколаїв, 20–23 черв. 2024 р. Миколаїв : ЧНУ ім. Петра Могили, 2024. С. 209–211. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/2349 (дата звернення: 27.04.2025).

8. Ухань Є. О. Бездротова локальна мережа на каналі 60 ГГц для побудови контрольованої зони. *Могилянські читання – 2023* : тези доп. XXVI Всеукр. наук.-метод. конф. Миколаїв, 6–10 листоп. 2023 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2023. С. 449–450. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/1869 (дата звернення: 27.04.2025).

9. Ухань Є. О., Журавська І. М. Пересувні захисні джаммери для формування контрольованої зони. *Free and Open Source Software (FOSS-2023)* : тези доп. XIV Міжнар. наук.-практ. конф., Харків, 07–10 лютого 2023 р. Харків : ХНЕУ ім. Семена Кузнеця, 2023. С. 103–105. URL: http://repository.hneu.edu.ua/bitstream/123456789/29041/1/foss-2023-theses.pdf (дата звернення: 27.04.2025).

10. Ухань Є. О. Захисні джаммери для формування контрольованої зони. *Могилянські читання – 2022* : тези доп. XXV Всеукр. наук.-практ. конф., Миколаїв, 07–11 листоп. 2022 р. Миколаїв : ЧНУ ім. Петра Могили, 2022. URL: https://dspace.chmnu.edu.ua/jspui/handle/123456789/595 (дата звернення:

27.04.2025).

Публікації, які додатково відображають наукові результати дисертації

11. Свідоцтво про реєстрацію авторського права на твір 107427. Комп’ютерна програма «Складання Wi-Fi-мапи переміщення пацієнтів територією реабілітаційного центру» / О. Р. Тогоєв, В. Д. Веселовський, О. В. Дворник, І. М. Журавська, К. О. Обухова, Є. О. Ухань ; дата реєстр. 17.08.2021, Бюл. № 66.