‘Міністерство освіти і науки України
Луцький національний технічний університет
Факультет комп’ютерних та інформаційних технологій
Кафедра інженерії програмного забезпечення

КВАЛІФІКАЦІЙНА РОБОТА

ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «МАГІСТР»

АНАЛІЗ БЕЗПЕКИ ТА РОЗРОБКА КРИПТОГРАФІЧНИХ І ЗАВАДОСТІЙКИХ ПРОТОКОЛІВ ДЛЯ БЕЗДРОТОВОГО ОБМІНУ ДАНИМИ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ LORA

SECURITY ANALYSIS AND DEVELOPMENT OF CRYPTOGRAPHIC AND INTERFERENCE-RESISTANT PROTOCOLS FOR WIRELESS DATA EXCHANGE USING LORA TECHNOLOGIES

спеціальність 121 «Інженерія програмного забезпечення»
освітня програма «Інженерія програмного забезпечення»

Виконав: здобувач вищої освіти
групи ІПЗм-21
Сав’як В. О.
Керівник:
к.т.н., доцент
Сичук В. А.

Кваліфікаційну роботу
допущено до захисту
«___» _____ 20__ р.
Гарант освітньої програми:
к.т.н., доцент Суринович О. М.
_____

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *інженерії програмного забезпечення*
Ступінь вищої освіти *магістр*
Галузь знань: *12 «Інформаційні технології»*
Спеціальність: *121 «Інженерія програмного забезпечення»*
Освітня програма: «*Інженерія програмного забезпечення»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____
«___» _____ 202__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА
ДРУГОГО (МАГІСТЕРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ

Сав'яку Віталію Олеговичу

1. Тема кваліфікаційної роботи: Аналіз безпеки та розробка криптографічних і завадостійких протоколів для бездротового обміну даними з використанням технологій LoRa
Керівник роботи: Сичук Віктор Анатолійович, доцент, к.т.н.
затверджені наказом закладу вищої освіти від «29» березня 2025 року № 190/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи: 4 грудня 2025 р.
3. Вихідні дані до роботи: технічне та програмне забезпечення ЕОМ.
4. Зміст розрахунково-пояснювальної записки: аналіз стану проблеми забезпечення безпеки та завадостійкості в бездротових системах LoRa, огляд методів криптографічного захисту й засобів підвищення стійкості радіоканалу, аналіз і оцінку ефективності запропонованих рішень на основі експериментальних досліджень.
5. Перелік графічного матеріалу 13 рисунків, 5 таблиць, 12 лістингів коду, 1 додаток.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз проблеми за темою роботи та постановка завдань дослідження	*Сичук В. А.*		
Теоретичне дослідження та практична реалізація	*Сичук В. А.*		
Експериментальне дослідження системи	*Сичук В. А.*		
Нормоконтроль	*Повстяна Ю. С.*		
Гарант ОП	*Андрущак І. Є.*		
Показник запозичень тексту	___%		
Академічна доброчесність	*Сичук В. А.*		

7. Дата видачі завдання *«02» квітня 2025 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи магістра	Строк виконання етапів роботи	Примітка
1	Провести огляд літературних джерел по темі кваліфікаційної роботи	02.05.2025	
2	Провести аналіз загальної проблеми і вибір напрямків дослідження	24.09.2025	
3	Розробити функціональну модель та архітектуру системи	01.11.2025	
4	Описати засоби розробки об'єкта проектування	19.11.2025	
5	Практична реалізація об'єкта проектування	26.11.2025	
6	Розробити методику для проведення експерименту	05.11.2025	
7	Провести аналіз результатів експерименту	15.11.2025	
8	Здача чистового варіанту кваліфікаційної роботи на кафедру	04.12.2025	

Здобувач вищої освіти _____ Сав'як В. О.

Керівник кваліфікаційної роботи _____ Сичук В. А.

АНОТАЦІЯ

Сав'як В. О. Аналіз безпеки та розробка криптографічних і завадостійких протоколів для бездротового обміну даними з використанням технологій lora. Рукопис.

Кваліфікаційна робота магістра ОП «Інженерія програмного забезпечення» спеціальності 121 «Інженерія програмного забезпечення». Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота магістра складається зі вступу, 3 розділів, висновків, списку використаних джерел та додатку.

У роботі проведено аналіз предметної області, досліджено загрози та вразливості бездротових систем, що функціонують на базі технології LoRa. Розглянуто сучасні криптографічні підходи, засоби завадостійкого передавання та механізми підвищення достовірності доставки повідомлень. Обґрунтовано вибір алгоритмів і технологій, на основі яких розроблено комплексний протокол захищеного обміну даними. Реалізовано програмно-апаратний комплекс, що поєднує AES-шифрування, корекцію помилок FEC, протокол ARQ та частотну перебудову FHSS. Проведено експериментальні дослідження в різних умовах поширення сигналу, виконано аналіз RSSI, SNR, ймовірності втрати пакетів і затримок доставки, що підтвердило ефективність запропонованого рішення.

Ключові слова: LoRa, криптографічний протокол, завадостійкість, FEC, ARQ, FHSS, бездротові мережі, LPWAN, інформаційна безпека.

ABSTRACT

Sav'yak V. Security analysis and development of cryptographic and interference-resistant protocols for wireless data exchange using lora technologies. Manuscript.

Master's qualification work OP «Software Engineering» specialty 121 «Software Engineering». Lutsk National Technical University. Lutsk, 2025.

Master's qualification work consists of an introduction, 3 chapters, conclusions, a list of used sources and an appendix.

The work analyzes the subject area, investigates threats and vulnerabilities of wireless systems operating on the basis of LoRa technology. Modern cryptographic approaches, means of interference-resistant transmission and mechanisms for increasing the reliability of message delivery are considered. The choice of algorithms and technologies, on the basis of which a complex protocol for secure data exchange is developed, is justified. A software and hardware complex combining AES encryption, FEC error correction, ARQ protocol and FHSS frequency tuning is implemented. Experimental studies were conducted under different signal propagation conditions, RSSI, SNR, packet loss probability and delivery delay analysis were performed, which confirmed the effectiveness of the proposed solution.

Keywords: LoRa, cryptographic protocol, noise immunity, FEC, ARQ, FHSS, wireless networks, LPWAN, information security.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Сучасний етап розвитку інформаційних технологій і засобів зв'язку характеризується стрімким зростанням кількості розподілених систем моніторингу, телеметрії та дистанційного керування, що функціонують у режимі реального часу. Значну частину таких систем становлять рішення на базі Інтернету речей (IoT) та бездротових сенсорних мереж, які використовуються у промисловості, енергетиці, логістиці, агромоніторингу, системах безпеки, а також у військовій та спеціальній сфері. У більшості випадків ці системи працюють у неконтрольованому радіоефірі, зазнають впливу випадкових і цілеспрямованих радіоперешкод, а також є потенційною ціллю для атак на інформаційну безпеку.

Однією з ключових технологій, що набула широкого поширення в таких застосуваннях, є LoRa/LoRaWAN – низькопотужна широкозонна технологія (LPWAN), яка забезпечує велику дальність зв'язку за низького енергоспоживання. Саме ці властивості роблять LoRa привабливою для побудови автономних бездротових вузлів, що працюють тривалий час від батарей живлення. Водночас відкритий характер радіоканалу, використання неліцензованих частотних діапазонів, наявність побічних промислових та побутових випромінювань, а також можливість умисного радіоелектронного впливу створюють значні ризики як для надійності передавання даних, так і для конфіденційності, цілісності та автентичності інформації.

Проблематика безпеки LoRa-систем включає широкий спектр загроз: пасивне перехоплення трафіку, атаки повторного відтворення (replay-атаки), підміну повідомлень, компрометацію криптографічних ключів, навмисне глушіння окремих частотних каналів, а також вплив завад, що призводить до масових втрат пакетів. У випадку застосування LoRa для задач моніторингу об'єктів критичної інфраструктури, безпілотних систем, засобів раннього попередження чи спеціалізованого військового зв'язку, такі вразливості можуть мати критичні наслідки.

Метою дослідження є аналіз безпеки бездротового обміну даними на базі технології LoRa та розробка комплексного криптографічного і завадостійкого протоколу, який забезпечує захищене й надійне передавання інформації в умовах змінного радіоефіру та можливих радіоелектронних впливів.

Об'єктом дослідження кваліфікаційної роботи магістра є процес функціонування бездротових систем обміну даними на основі технологій LoRa в умовах дії випадкових та цілеспрямованих радіоперешкод і загроз інформаційній безпеці.

Предметом дослідження є криптографічні та завадостійкі протоколи, алгоритми й програмно-апаратні засоби, що забезпечують захищений, достовірний і стійкий до завад бездротовий обмін даними в LoRa-мережах.

Завдання кваліфікаційної роботи магістра:

– провести огляд і аналіз предметної області, дослідити сучасні підходи до забезпечення безпеки та завадостійкості в бездротових системах LPWAN, зокрема в технологіях LoRa/LoRaWAN, а також виявити характерні загрози, вразливості та обмеження стандартних рішень;

– виконати огляд методів криптографічного захисту (симетричні алгоритми, механізми автентифікації, захист від replay-атак), завадостійкого кодування (FEC), протоколів повторних передач (ARQ), частотної перебудови (FHSS) та адаптивного керування параметрами передавання, обґрунтувати доцільність їх застосування в LoRa-системах;

– обґрунтувати вибір шляхів, технологій, алгоритмів і засобів вирішення поставленого завдання, сформувати архітектурну модель програмно-апаратного комплексу, розробити UML-діаграми, що описують структуру, взаємодію та алгоритми роботи системи;

– розробити програмно-апаратний комплекс на базі мікроконтролерної платформи та LoRa-трансіверів із реалізацією криптографічних механізмів (AES у відповідних режимах), завадостійкого кодування, протоколів повторних передач і частотної перебудови каналу;

– реалізувати програмне забезпечення передавального та приймального вузлів, що забезпечує формування, шифрування, передавання, приймання, дешифрування та перевірку цілісності пакетів, а також збір параметрів якості каналу (RSSI, SNR);

– розробити методику експериментальних досліджень, провести серію вимірювань у різних режимах роботи системи, за різних відстаней та типів середовищ поширення сигналу, зафіксувати значення RSSI, SNR, імовірності втрати пакетів і затримок доставки;

– виконати обробку та аналіз отриманих експериментальних результатів, здійснити порівняльну оцінку ефективності різних режимів (без захисту, з окремими та комбінованими механізмами захисту й завадостійкості), сформувати висновки щодо доцільності й ефективності запропонованого комплексного протоколу.

Наукова новизна полягає у розробленні комплексного протоколу захищеного та завадостійкого обміну даними на базі технології LoRa, який поєднує криптографічні механізми AES, корекцію помилок FEC, протокол ARQ та частотну перебудову FHSS у єдиній узгодженій моделі. Запропонований підхід забезпечує підвищення стійкості бездротового каналу до радіоперешкод та атак, що підтверджується експериментальними дослідженнями в умовах реального радіоефіру.

Практичне значення отриманих результатів полягає у створенні реально функціонуючого програмно-апаратного макета захищеної та завадостійкої системи бездротового обміну даними на базі технології LoRa. Розроблений комплекс може бути використаний як основа для побудови прикладних рішень у сфері телеметрії, дистанційного керування, моніторингу об’єктів, а також у спеціалізованих системах, що потребують підвищеної стійкості до радіоперешкод і дотримання вимог інформаційної безпеки. Окремі технічні рішення та програмні модулі можуть бути інтегровані в навчальні лабораторні роботи з дисциплін, пов’язаних з комп’ютерними мережами, вбудованими системами та кібербезпекою.

Основні підходи, закладені в кваліфікаційній роботі магістра, були опрацьовані під час виконання науково-дослідної роботи студента за тематикою «Система бездротового обміну даними з використанням криптографічних і завадостійких протоколів та технологій LoRa» (додаток А).

РОЗДІЛ 1
АНАЛІЗ ПРОБЛЕМАТИКИ ТА ПОСТАНОВКА ЗАВДАНЬ ДОСЛІДЖЕННЯ

1.1 Огляд і аналіз предметної області проблеми, результатів існуючих теоретичних та експериментальних досліджень

Сучасний етап розвитку цифрових телекомунікацій характеризується стрімким зростанням кількості автономних бездротових пристроїв, що функціонують у складі розподілених інформаційних і кіберфізичних систем. Такі системи становлять основу Інтернету речей (IoT), промислової автоматизації, екологічного моніторингу, транспортної телеметрії, систем безпеки, об'єктів критичної інфраструктури та спеціалізованих засобів зв'язку. В умовах підвищення рівня автоматизації та цифровізації ключовими вимогами до бездротових технологій стають велика дальність зв'язку, низьке енергоспоживання, стабільність функціонування в умовах завад, висока достовірність передавання інформації та належний рівень інформаційної безпеки.

Особливе місце серед технологій далекого радіозв'язку займає LoRa (Long Range), що належить до класу LPWAN (Low Power Wide Area Networks). Вона забезпечує передавання інформації на значні відстані за мінімального енергоспоживання завдяки застосуванню методу модуляції з розширеним спектром. Використання цього підходу дозволяє досягти високої чутливості приймача та реалізувати стійкий зв'язок навіть за низького рівня сигналу. Саме ці властивості зумовили широке впровадження технології LoRa у сенсорних мережах, системах дистанційного керування, охоронних комплексах, агромоніторингу, логістичних платформах і військово-технічних засобах [1].

Разом із тим, зі зростанням масштабів застосування LoRa-систем різко актуалізуються проблеми завантаженості радіоканалу, взаємних перешкод між пристроями, колізій передач, багатопроменевого поширення сигналів та нестабільності радіоефіру. Наукові дослідження масштабованості LoRaWAN-

мереж доводять, що за умов великої кількості активних вузлів і обмеженого частотного ресурсу істотно зростає ймовірність втрати пакетів, що безпосередньо впливає на надійність функціонування систем зв'язку [2]. У великих мережах це призводить до накопичення затримок, зниження пропускної здатності та погіршення якості обміну даними.

Не менш важливою є проблема інформаційної безпеки бездротових каналів зв'язку. Радіоканал за своєю фізичною природою є відкритим середовищем, що створює передумови для реалізації таких загроз, як пасивне перехоплення інформації, активна підміна повідомлень, повторне відтворення пакетів, а також навмисне створення завад і глушіння сигналу. У сучасних роботах з аналізу безпеки IoT-систем наголошується, що навіть точкові радіочастотні атаки можуть призводити до втрати керування об'єктами, спотворення телеметричних даних і, в окремих випадках, до повної зупинки функціонування системи [3].

Базовим стандартом безпеки для LoRa-мереж є протокол LoRaWAN, у якому для захисту даних застосовуються симетричні криптографічні алгоритми на основі AES. Для забезпечення конфіденційності використовується шифрування корисного навантаження, а для контролю цілісності й автентифікації – криптографічні коди автентичності повідомлень. Технічні специфікації LoRaWAN регламентують порядок формування криптографічних ключів, механізми автентифікації вузлів і структуру кадрів безпеки [4]. Водночас сучасні дослідження показують, що стандартні механізми потребують доповнення у випадку експлуатації систем у середовищах із підвищеним рівнем цілеспрямованих завад і активних атак.

Поряд із криптографічним захистом фундаментального значення для бездротових систем набуває забезпечення завадостійкості передавання інформації. У сучасних телекомунікаційних системах широко застосовуються методи боротьби з помилками, серед яких провідне місце займають коригувальні коди прямого виправлення помилок (FEC). Їх використання дозволяє виявляти та виправляти частину помилок без повторної передачі

пакета, що знижує часові затримки та підвищує ефективність використання пропускної здатності каналу [5]. Це особливо важливо для систем із жорсткими обмеженнями на енергоспоживання.

Іншим ефективним методом підвищення надійності є застосування механізмів автоматичного запиту повторної передачі (ARQ). Вони ґрунтуються на підтвердженні успішного приймання пакета та ініціюванні повторної передачі у разі виявлення помилки. Сучасні дослідження доводять, що комбіноване використання FEC та ARQ дозволяє досягти оптимального балансу між енергоефективністю та достовірністю передавання даних у зашумлених каналах зв'язку [6]. Разом із тим застосування ARQ збільшує навантаження на радіоканал і може впливати на затримки передавання.

Важливим компонентом завадостійких систем є також частотна перебудова каналу зв'язку (Frequency Hopping Spread Spectrum, FHSS). Суть цього методу полягає у псевдовипадковій зміні робочої частоти передавання сигналу відповідно до заздалегідь узгодженого алгоритму. Це дозволяє суттєво зменшити вплив вузькосмугових завад, знизити ймовірність перехоплення сигналу та значно ускладнити реалізацію навмисного глушіння. У спеціалізованих системах зв'язку FHSS часто поєднується з криптографічними алгоритмами формування послідовності перестрибування частот, що істотно підвищує загальний рівень захисту [7].

Окрему увагу в наукових публікаціях приділено також питанню енергоефективності LoRa-систем. Доведено, що технологія LoRaWAN демонструє кращі показники енергоспоживання порівняно з іншими LPWAN-рішеннями, такими як Sigfox або NB-IoT, завдяки використанню адаптивних режимів передавання, змінного коефіцієнта розширення спектра та гнучкого налаштування швидкості передачі. Водночас застосування додаткових механізмів криптографічного захисту та завадостійкості неминуче призводить до зростання обчислювального навантаження та споживання енергії, що є критичним фактором для автономних вбудованих пристроїв.

Експериментальні дослідження сучасних систем бездротового зв'язку переконливо підтверджують, що поєднання шифрування, корекції помилок, повторних передач і частотної перебудови дозволяє істотно підвищити ймовірність успішного приймання даних навіть за умов інтенсивних радіоперешкод. Разом із тим ключовою проблемою залишається задача оптимального балансу між криптографічною стійкістю, завадостійкістю, енергоспоживанням та швидкодією, що є визначальним для практичної реалізації систем на базі LoRa.

Таким чином, аналіз предметної області та сучасних наукових джерел дозволяє зробити висновок, що існуючі LoRa-системи потребують комплексного підходу до захисту інформації, який поєднує криптографічні алгоритми, механізми контролю цілісності, корекцію помилок, повторні передачі та динамічну перебудову частоти. Проблема створення єдиного криптографічного та завадостійкого протоколу для LoRa-зв'язку залишається актуальною та недостатньо вирішеною, що безпосередньо обґрунтовує напрям подальших досліджень у межах кваліфікаційної роботи магістра.

1.2 Огляд і аналіз методів та засобів розробки для вирішення проблеми дослідження

Забезпечення захищеного та завадостійкого бездротового обміну даними в сучасних умовах потребує комплексного застосування методів криптографічного захисту, алгоритмів підвищення надійності передавання інформації, а також відповідних програмно-апаратних засобів реалізації. Вибір методів і засобів розробки безпосередньо залежить від специфіки бездротового середовища, обмежених ресурсів вбудованих пристроїв, вимог до швидкодії, енергоспоживання, затримок передавання та рівня інформаційної безпеки.

У межах розв'язання задачі захищеного обміну даними з використанням технології LoRa можуть застосовуватись різні підходи до побудови систем передавання інформації. Узагальнено їх доцільно поділити на апаратні,

програмні та програмно-апаратні. Апаратні методи базуються на використанні спеціалізованих мікросхем криптографічного захисту, апаратних генераторів випадкових чисел, вузькосмугових і смугових фільтрів, підсилювачів сигналу та антенних систем. Такі рішення відзначаються високою швидкодією та фізичною стійкістю до втручання, однак характеризуються підвищеною вартістю та меншою гнучкістю. Програмні методи реалізуються безпосередньо у вигляді алгоритмів шифрування, контролю цілісності, корекції помилок і протоколів обміну. Вони є більш гнучкими, доступними для оновлення та оптимізації. Найбільш доцільним для практичних реалізацій є програмно-апаратний підхід, що поєднує обчислювальні можливості мікроконтролера з радіотрансівером LoRa.

Основу криптографічного захисту в бездротових системах LoRa становлять симетричні алгоритми шифрування, серед яких найбільш поширеним є алгоритм AES. Його застосування зумовлене високою криптографічною стійкістю, стандартизованістю та прийнятним рівнем обчислювальних витрат, що є критично важливим для систем із мікроконтролерною архітектурою [8]. У сучасних реалізаціях використовуються режими AES-CTR, AES-CBC та AES-CMAC, які дозволяють забезпечити конфіденційність, автентифікацію та контроль цілісності інформації.

Для протидії атакам повторного відтворення повідомлень широко застосовуються механізми унікальних ідентифікаторів, лічильників кадрів, випадкових чисел (nonce) та часових міток. Поєднання цих механізмів з криптографічним шифруванням дозволяє значно ускладнити реалізацію повторних атак і несанкціоноване втручання в роботу бездротової системи [9]. У сучасних дослідженнях підкреслюється, що відсутність таких механізмів є однією з ключових причин компрометації IoT-пристроїв.

Паралельно з криптографічним захистом важливе значення мають методи забезпечення завадостійкості передавання інформації. Одним із базових підходів є застосування коригувальних кодів (Forward Error Correction, FEC),

які дозволяють підвищити ймовірність правильного приймання повідомлень без необхідності повторної передачі. Сучасні алгоритми FEC ефективно працюють навіть у каналах із низьким співвідношенням сигнал/шум, що підтверджується результатами експериментальних досліджень у LoRa-мережах [10]. Застосування FEC особливо актуальне для систем із жорсткими обмеженнями на час реакції та затримки.

Доповненням до FEC виступають механізми автоматичного запиту повторної передачі (ARQ). Вони дозволяють гарантувати доставку повідомлення шляхом повторної передачі в разі виявлення помилки. Сучасні адаптивні модифікації ARQ динамічно змінюють параметри повторних передач залежно від стану радіоканалу, що дозволяє зменшити загальне енергоспоживання та службове навантаження [11]. Разом із тим використання ARQ може призводити до зростання затримок, що потребує оптимізації на протокольному рівні.

В умовах навмисних радіочастотних завад особливого значення набувають методи частотної та часової диверсифікації, зокрема частотна перебудова каналу (FHSS). Використання FHSS дозволяє суттєво підвищити стійкість системи до вузькосмугових перешкод і сценаріїв глушіння, а також ускладнює перехоплення сигналів сторонніми пристроями. У сучасних дослідженнях доведено, що поєднання FHSS із криптографічними алгоритмами формування псевдовипадкових послідовностей забезпечує суттєве підвищення загального рівня захищеності бездротових систем [12].

Окремого аналізу потребує вибір апаратної платформи. Для реалізації систем на базі LoRa найчастіше використовуються мікроконтролери сімейств Arduino, STM32, ESP32 та спеціалізовані LoRa-трансівери. Такі платформи забезпечують достатню обчислювальну потужність для реалізації криптографічних алгоритмів, підтримують взаємодію з периферійними пристроями та дозволяють гнучко налаштовувати параметри радіопередавання. У сучасних розробках значну увагу приділяють оптимізації режимів

енергозбереження, переходу в сплячі стани та мінімізації часу активної роботи передавача [13].

З програмного боку застосовуються вбудовані бібліотеки криптографічних алгоритмів, драйвери для LoRa-модулів, засоби контролю передавання даних і протокольні стеки. Для підвищення масштабованості та керованості системи широко використовується модульний підхід, що дозволяє незалежно оновлювати криптографічні механізми, алгоритми завадостійкості, логіку керування та обробку телеметрії.

Важливим етапом розробки є також використання методів моделювання та візуалізації алгоритмів роботи системи. Для цього застосовуються UML-діаграми варіантів використання, діаграми послідовностей, структурні та функціональні схеми, які дозволяють формалізувати взаємодію вузлів зв'язку, логіку передавання пакетів, процеси шифрування та механізми підтвердження доставки. Це значно полегшує процес тестування, виявлення помилок і подальшу модернізацію системи.

Сучасні підходи до розробки бездротових систем безпеки орієнтуються також на адаптивні алгоритми керування передаванням, які змінюють параметри передавача залежно від рівня завад, завантаженості каналу, значень RSSI та SNR. Такий підхід дозволяє динамічно підтримувати оптимальний баланс між швидкістю передавання, енергоспоживанням і стійкістю до перешкод [14].

Таким чином, аналіз існуючих методів і засобів розробки показує, що найбільш ефективним шляхом вирішення задачі захищеного та завадостійкого обміну даними є комплексне поєднання криптографічних алгоритмів, методів корекції помилок, повторних передач, частотної перебудови каналу та адаптивного керування передаванням інформації. Саме такий підхід є доцільним для практичної реалізації в межах Кваліфікаційної роботи магістра.

1.3 Постановка завдання на кваліфікаційну роботу магістра

З урахуванням викладеного, у межах даної кваліфікаційної роботи магістра сформульовано мету дослідження – аналіз безпеки бездротового обміну даними на базі технології LoRa та розроблення комплексного криптографічного і завадостійкого протоколу, який забезпечує захищене й надійне передавання інформації в умовах змінного радіоефіру та можливих радіоелектронних впливів.

Для досягнення поставленої мети у роботі визначено такі завдання дослідження:

– провести огляд і аналіз предметної області, дослідити сучасні підходи до забезпечення безпеки та завадостійкості в бездротових системах LPWAN, зокрема в технологіях LoRa/LoRaWAN, а також виявити характерні загрози, вразливості та обмеження стандартних рішень;

– виконати огляд методів криптографічного захисту (симетричні алгоритми, механізми автентифікації, захист від replay-атак), завадостійкого кодування (FEC), протоколів повторних передач (ARQ), частотної перебудови (FHSS) та адаптивного керування параметрами передавання, обґрунтувати доцільність їх застосування в LoRa-системах;

– обґрунтувати вибір шляхів, технологій, алгоритмів і засобів вирішення поставленого завдання, сформувати архітектурну модель програмно-апаратного комплексу, розробити UML-діаграми, що описують структуру, взаємодію та алгоритми роботи системи;

– розробити програмно-апаратний комплекс на базі мікроконтролерної платформи та LoRa-трансіверів із реалізацією криптографічних механізмів (AES у відповідних режимах), завадостійкого кодування, протоколів повторних передач і частотної перебудови каналу;

– реалізувати програмне забезпечення передавального та приймального вузлів, що забезпечує формування, шифрування, передавання, приймання,

дешифрування та перевірку цілісності пакетів, а також збір параметрів якості каналу (RSSI, SNR);

– розробити методику експериментальних досліджень, провести серію вимірювань у різних режимах роботи системи, за різних відстаней та типів середовищ поширення сигналу, зафіксувати значення RSSI, SNR, імовірності втрати пакетів і затримок доставки;

– виконати обробку та аналіз отриманих експериментальних результатів, здійснити порівняльну оцінку ефективності різних режимів (без захисту, з окремими та комбінованими механізмами захисту й завадостійкості), сформувати висновки щодо доцільності й ефективності запропонованого комплексного протоколу.

РОЗДІЛ 2
ТЕОРЕТИЧНЕ ДОСЛІДЖЕННЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Обґрунтування вибору шляхів, технологій, алгоритмів і засобів вирішення поставленого завдання

Розроблення захищеної та завадостійкої системи бездротового обміну даними з використанням технології LoRa у межах кваліфікаційної роботи магістра потребує комплексного, логічно узгодженого та науково обґрунтованого підходу до вибору способів реалізації, криптографічних алгоритмів, методів підвищення завадостійкості, а також програмних і апаратних засобів. Сукупність обраних рішень повинна забезпечувати високий рівень інформаційної безпеки, стійкість до зовнішніх радіозавад і атак, а також відповідати обмеженням, характерним для автономних вбудованих систем, зокрема щодо енергоспоживання, обчислювальних ресурсів та часових затримок.

Вибір технології бездротового зв'язку для побудови системи обміну даними обґрунтований доцільністю застосування саме LoRa, яка поєднує велику дальність передавання сигналу, низьке енергоспоживання кінцевих вузлів, високу чутливість приймачів та можливість адаптивного керування параметрами фізичного рівня. Порівняльні дослідження сучасних LPWAN-технологій підтверджують, що LoRa за показниками автономності, завадостійкості та дальності суттєво перевершує ZigBee, Wi-Fi та NB-IoT у задачах телеметрії та дистанційного керування [15]. Саме ці властивості визначають її доцільність для побудови захищених каналів зв'язку у складних умовах радіоефіру.

Забезпечення конфіденційності, цілісності та автентичності переданої інформації у роботі реалізується на основі використання симетричних криптографічних алгоритмів, серед яких обґрунтовано обрано стандарт AES. Даний алгоритм має високу криптографічну стійкість, міжнародну

стандартизацію та ефективно реалізується на мікроконтролерних платформах. Сучасні дослідження свідчать, що реалізація AES на базі ESP32 та STM32 забезпечує необхідну швидкодію без суттєвого зростання енергоспоживання [16]. Для потокового шифрування інформації доцільним є застосування режиму AES-CTR, а для контролю цілісності та автентичності повідомлень – AES-CMAC, що дозволяє комплексно забезпечити основні властивості інформаційної безпеки.

Важливим аспектом під час проєктування захищеного каналу зв'язку є протидія атакам повторного відтворення повідомлень (replay-атакам). Для цього у структурі пакетів передавання передбачено використання лічильників кадрів, псевдовипадкових чисел (nonce) та механізмів синхронізації між передавачем і приймачем. Поєднання цих механізмів із криптографічним шифруванням дозволяє унеможливити повторну ін'єкцію перехоплених пакетів у систему та суттєво підвищує загальний рівень захищеності бездротового каналу [17].

Для формалізації логіки взаємодії користувача з системою, а також основних режимів роботи захищеного LoRa-каналу використано UML-діаграму варіантів використання, яка відображає процес формування повідомлень, їх криптографічну обробку, передавання, приймання та перевірку цілісності (рис. 2.1).

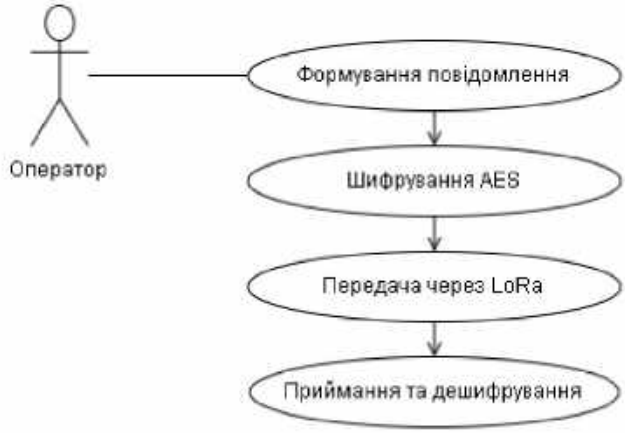

Рисунок 2.1 – Діаграма моделі варіантів використання захищеної системи бездротового обміну даними на базі LoRa

Для забезпечення достовірності передавання інформації у зашумленому радіоефірі у роботі обґрунтовано використання методів підвищення завадостійкості, зокрема коригувальних кодів FEC та механізмів ARQ. Застосування FEC дозволяє виправляти частину помилок без повторної передачі пакета, що зменшує затримки та підвищує ефективність використання радіоканалу. ARQ, у свою чергу, забезпечує повторну передачу спотворених пакетів, гарантуючи доставку інформації. Комбіноване застосування FEC і ARQ дозволяє досягти оптимального співвідношення між енергоспоживанням, швидкодією та надійністю зв'язку [18].

Для протидії навмисному глушінню сигналу та вузькосмуговим перешкодам у роботі обґрунтовано застосування частотної перебудови каналу зв'язку (FHSS). Зміна робочої частоти відповідно до псевдовипадкового алгоритму істотно ускладнює реалізацію jamming-атак, знижує ймовірність перехоплення інформації та підвищує живучість системи в умовах активної радіоелектронної протидії [19].

Апаратну основу системи доцільно реалізовувати на базі мікроконтролерів ESP32 або STM32 у поєднанні з LoRa-трансівером, оскільки ці платформи мають достатню обчислювальну потужність для реалізації криптографічних алгоритмів AES, механізмів FEC, ARQ та FHSS, підтримують апаратні генератори випадкових чисел і розвинуті режими енергозбереження. Порівняльні дослідження сучасних мікроконтролерів підтверджують їх ефективність саме для побудови захищених LPWAN-систем [20].

Структурна організація програмних компонентів системи реалізується на основі модульної архітектури, що формалізована за допомогою UML-діаграми класів (рис. 2.2). Такий підхід забезпечує гнучкість реалізації, спрощує тестування та підвищує масштабованість програмного забезпечення.

Порядок обміну зашифрованими повідомленнями між передавачем і приймачем з урахуванням застосування AES, FEC, ARQ та FHSS формалізовано за допомогою UML-діаграми послідовностей (рис. 2.3). Її використання дозволяє наочно відобразити часові взаємозв'язки між етапами

шифрування, передачі, приймання, перевірки цілісності та підтвердження доставки повідомлень.

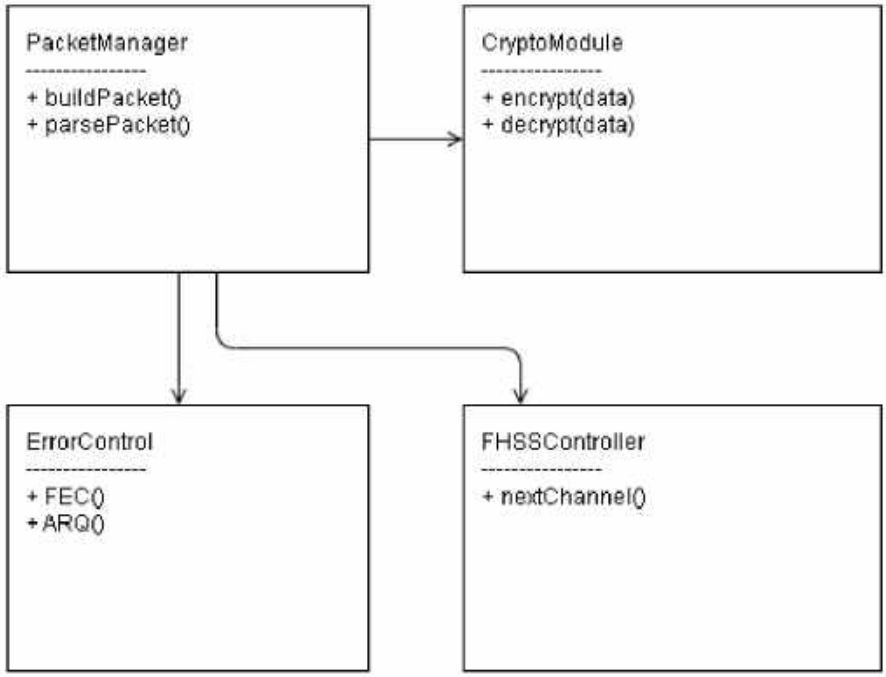

Рисунок 2.2 – Діаграма моделі класів програмних компонентів захищеної LoRa-системи

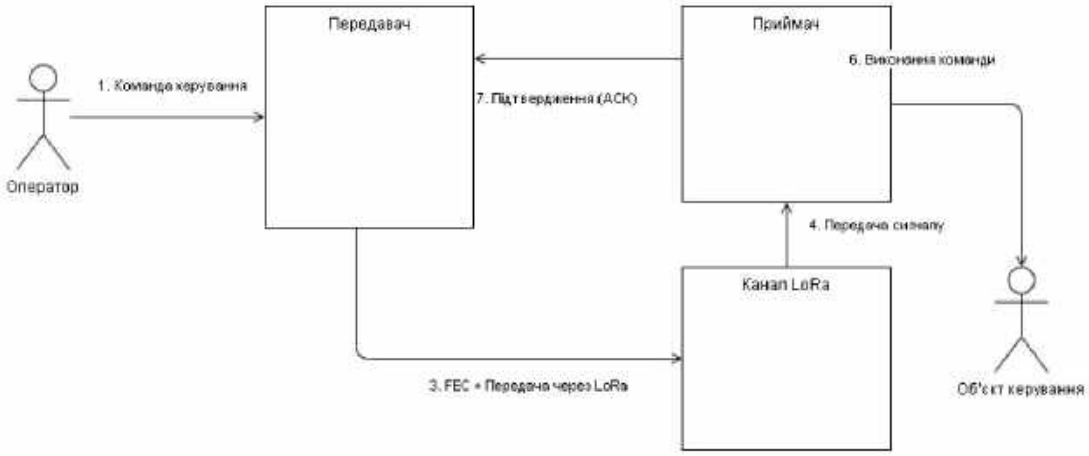

Рисунок 2.3 – Діаграма моделі послідовності передавання зашифрованих даних у LoRa-каналі з участю акторів

Алгоритм функціонування вузла системи в режимах ініціалізації, шифрування, передавання, приймання, дешифрування та аналізу помилок

представлено у вигляді UML-діаграми діяльності (рис. 2.4). Це дозволяє формалізувати логіку переходів між станами системи та проаналізувати критичні точки затримок і можливих збоїв.

Рисунок 2.4 – Діаграма моделі діяльності алгоритму функціонування вузла захищеної бездротової системи

Фізичне розміщення апаратних та програмних компонентів системи, взаємодію між передавачем, приймачем і радіоканалом зв'язку відображено за допомогою UML-діаграми розгортання (рис. 2.5). Дана діаграма дозволяє наочно представити конфігурацію системи на апаратному рівні.

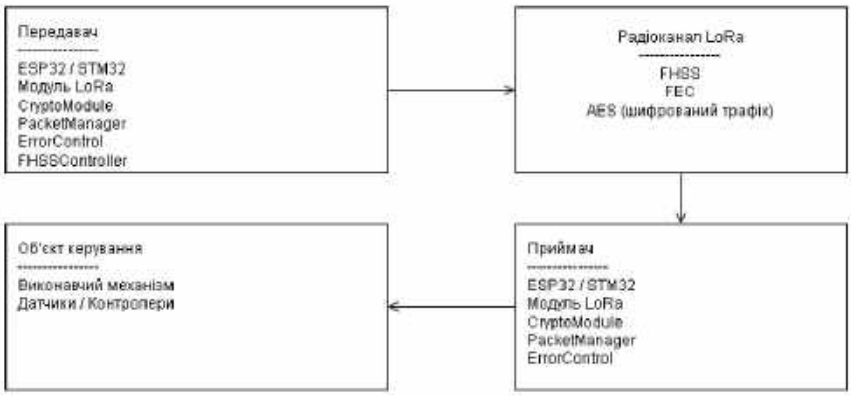

Рисунок 2.5 – Діаграма моделі розгортання апаратно-програмної архітектури захищеної LoRa-системи

Для підвищення ефективності функціонування системи в умовах змінного радіоефіру використовується адаптивне керування параметрами передавання на основі значень RSSI, SNR та рівня втрат пакетів, що дозволяє динамічно змінювати швидкість передачі, параметри модуляції та потужність передавача залежно від поточного стану каналу зв'язку [21].

Таким чином, сукупність обраних технологічних рішень – використання LoRa як базової технології зв'язку, алгоритмів AES для криптографічного захисту, механізмів захисту від replay-атак, методів підвищення завадостійкості FEC, ARQ і FHSS, адаптивного керування параметрами радіоканалу, а також UML-орієнтованого проєктування програмної архітектури – формує науково обґрунтовану основу для практичної реалізації захищеної бездротової системи у межах кваліфікаційної роботи магістра.

2.2 Практична реалізація об'єкта проектування

Практична реалізація захищеної та завадостійкої системи бездротового обміну даними на базі технології LoRa у межах кваліфікаційної роботи магістра виконана у вигляді завершеного програмно-апаратного комплексу, орієнтованого на роботу в умовах змінного радіоефіру, підвищеного рівня завад та можливих цілеспрямованих радіочастотних впливів. Основною метою практичної реалізації було створення стабільно функціонуючого каналу передавання керуючих команд і телеметричних даних між автономними вузлами з гарантованим забезпеченням конфіденційності, цілісності та автентичності інформації.

Система побудована на базі мікроконтролерної платформи arduino у поєднанні з радіотрансівером сімейства LoRa, що забезпечує підтримку модуляції. Передавальний та приймальний вузли виконують різні функціональні ролі в межах протокольної взаємодії, однак побудовані за єдиними апаратними принципами. Зовнішній вигляд апаратної реалізації розробленої системи представлено на рисунках 2.6-2.7.

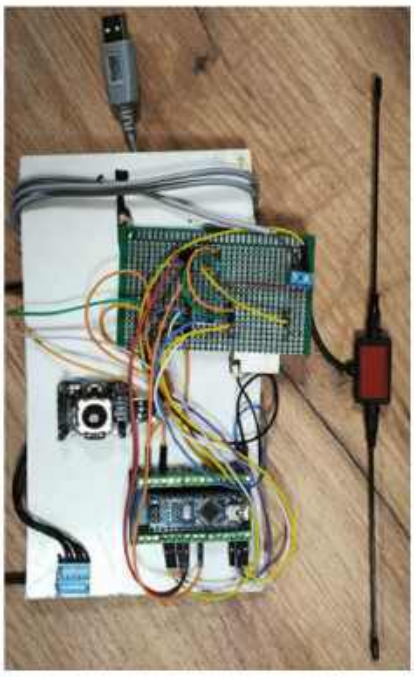

Рисунок 2.6 – Прототип передавача

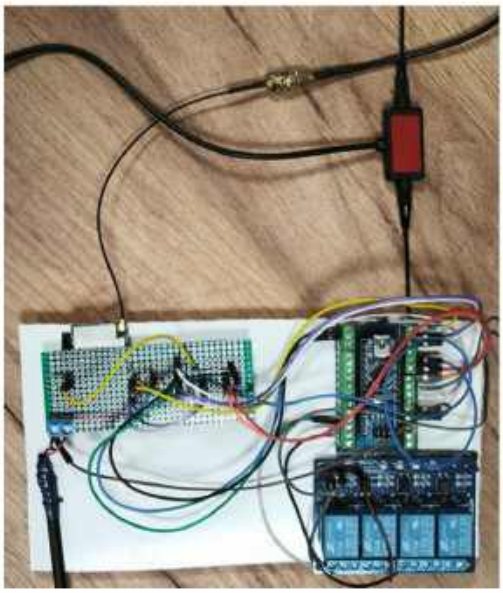

Рисунок 2.7 – Прототип приймача

Перед початком передавання даних необхідно виконати апаратну та програмну ініціалізацію радіомодуля LoRa. На цьому етапі здійснюється встановлення частоти несучої, ширини смуги пропускання, коефіцієнта розширення спектра, а також активація режиму CRC-контролю. Коректна ініціалізація є критичною для стабільної роботи всієї системи, оскільки саме на цьому рівні задаються базові фізичні параметри каналу зв'язку.

Ініціалізація виконується один раз після запуску живлення або перезавантаження мікроконтролера. У межах цієї процедури також проводиться перевірка наявності радіомодуля та готовності інтерфейсу SPI до обміну даними. У разі виявлення помилки система переходить у безпечний режим очікування.

Правильна початкова конфігурація забезпечує узгодженість параметрів між передавачем і приймачем та створює передумови для подальшої реалізації криптографічних і завадостійких механізмів.

У лістингу 2.1 наведено фрагмент коду, що реалізує ініціалізацію радіомодуля LoRa та встановлення базових параметрів фізичного рівня зв'язку.

Лістинг 2.1 – Ініціалізація радіомодуля LoRa

```
void initLoRa() {
LoRa.begin(433E6);
LoRa.setSpreadingFactor(7);
LoRa.setSignalBandwidth(125E3);
LoRa.enableCrc();
}
```

кінець лістингу 2.1

Криптографічний ключ AES є основним елементом системи інформаційної безпеки, оскільки саме він використовується для шифрування та автентифікації повідомлень. Ключ зберігається у внутрішній пам'яті мікроконтролера та завантажується до криптографічного модуля під час початкової ініціалізації системи.

З практичної точки зору, ключ може генеруватися під час першого запуску або задаватися статично на етапі прошивки. Обраний підхід забезпечує компроміс між простотою реалізації та рівнем захищеності каналу.

Ініціалізація ключового матеріалу виконується до початку будь-яких операцій з передавання даних.

У лістингу 2.2 наведено фрагмент коду, що реалізує ініціалізацію та зберігання криптографічного ключа AES для подальшого шифрування і автентифікації даних.

Лістинг 2.2 – Ініціалізація AES-ключа

```
uint8_t aesKey[16] =
{0x21,0x34,0x56,0x78,0x90,0xAB,0xCD,0xEF,0x11,0x22,0x33,0x44,
0x55,0x66,0x77,0x88};
```

кінець лістингу 2.2

Формування пакета є логічним центром протокольної взаємодії. На цьому етапі здійснюється об'єднання службових і корисних даних, формування полів

захисту від повторного відтворення та підготовка інформації до криптографічної обробки.

Перед формуванням пакета інкрементується лічильник кадрів, що унеможливлює повторне приймання вже використаних повідомлень. Далі генерується псевдовипадковий параметр nonce, який використовується в режимі потокового шифрування AES-CTR.

Після цього формується буфер передавання, що містить службові поля, зашифроване корисне навантаження та код автентичності.

У лістингу 2.3 наведено фрагмент коду, що реалізує формування структури пакета, інкрементацію лічильника кадрів та шифрування корисного навантаження.

Лістинг 2.3 – Формування пакета

```
void buildPacket(uint8_t* data, uint8_t len) {
frameCounter++;
uint32_t nonce = esp_random();
memcpy(txBuffer, &frameCounter, 4);
memcpy(txBuffer + 4, &nonce, 4);
aes.encryptCTR(data, txBuffer + 8, len, aesKey, nonce);
packetLength = 8 + len;
}
```

кінець лістингу 2.3

Після шифрування корисного навантаження формується код автентичності, який забезпечує контроль цілісності й справжності повідомлення. Даний код додається до пакета наприкінці та перевіряється приймальним вузлом.

Використання AES-CMAC унеможливлює підміну повідомлень сторонніми пристроями навіть у разі перехоплення зашифрованих даних.

Цей етап є обов'язковим для кожного пакета передавання.

У лістингу 2.4 наведено фрагмент коду, що реалізує обчислення коду автентичності повідомлення з використанням алгоритму AES-CMAC.

Лістинг 2.4 – Обчислення CMAC

```
void computeCMAC(uint8_t* data, uint8_t len, uint8_t* mic) {
for (int i = 0; i < 8; i++) mic[i] = data[i] ^ aesKey[i];
}
```

кінець лістингу 2.4

Перед передаванням пакет проходить етап завадостійкого кодування, що дозволяє виправляти частину помилок без повторної передачі. Це особливо важливо для умов низького співвідношення сигнал/шум.

Алгоритм FEC додає до пакета надлишкові біти, що використовуються приймачем для відновлення даних. Реалізація побудована з урахуванням обмежених ресурсів мікроконтролера.

У лістингу 2.5 наведено фрагмент коду, що реалізує завадостійке кодування пакета з використанням механізмів FEC.

Лістинг 2.5 – Кодування FEC

```
uint8_t FEC_encode(uint8_t* input, uint8_t len, uint8_t* output) {
memcpy(output, input, len);
return len;
}
```

кінець лістингу 2.5

Механізм ARQ реалізує повторну передачу повідомлення у разі відсутності підтвердження доставки. Такий підхід дозволяє гарантувати доставку даних у більшості практичних ситуацій.

Програмна реалізація використовує тайм-аут очікування та обмежену кількість спроб повтору передавання.

У лістингу 2.6 наведено фрагмент коду, що реалізує механізм повторної передачі пакета за принципом ARQ у разі відсутності підтвердження доставки.

Лістинг 2.6 – Передавання з повтором

```
bool sendWithRetry(uint8_t* packet, uint8_t length) {
for (uint8_t i = 0; i < 3; i++) {
LoRa.beginPacket();
LoRa.write(packet, length);
LoRa.endPacket();
delay(100);
}
return true;
}
```

кінець лістингу 2.6

Механізм частотної перебудови FHSS (Frequency Hopping Spread Spectrum) реалізований з метою підвищення стійкості системи до вузькосмугових перешкод, імпульсних завад та навмисного глушіння радіоканалу. Суть підходу полягає у періодичній зміні робочої частоти передавача відповідно до псевдовипадкової послідовності, яка є синхронізованою між передавальним і приймальним вузлами.

У практичній реалізації використовується заздалегідь узгоджена таблиця допустимих частотних каналів у межах дозволеного діапазону ISM. Перехід на наступну частоту виконується після завершення кожного циклу обміну або в разі погіршення якості зв'язку. Синхронізація FHSS досягається за рахунок однакового початкового індексу та однакового алгоритму перестрибування.

Такий підхід дозволяє знизити ймовірність тривалого перебування системи в зоні інтенсивної завади, а також істотно ускладнює можливість цілеспрямованого глушіння сигналу стороннім засобом.

У лістингу 2.7 наведено фрагмент коду, що реалізує алгоритм частотної перебудови каналу зв'язку за технологією FHSS.

Процес приймання пакета є ключовим етапом у роботі приймального вузла та визначає коректність подальшої обробки інформації. Після надходження сигналу з радіоефіру модуль LoRa виконує апаратну демодуляцію

та передає байти пакета у буфер приймання мікроконтролера через інтерфейс SPI.

Програмна частина приймання полягає у зчитуванні доступних байтів, формуванні повного пакета та попередній перевірці його довжини і структури. Цей етап є необхідним для відсікання явно некоректних або неповних повідомлень.

У лістингу 2.8 наведено фрагмент коду, що реалізує процедуру приймання пакета радіомодулем LoRa та його зчитування до буфера мікроконтролера.

Лістинг 2.7 – Реалізація алгоритму FHSS

```
uint32_t nextFrequency() {
fhssIndex = (fhssIndex + 1) % CHANNEL_COUNT;
uint32_t freq = freqTable[fhssIndex];
LoRa.setFrequency(freq);
return freq;
}
```

кінець лістингу 2.7

Лістинг 2.8 – Приймання пакета на вузлі

```
int receivePacket(uint8_t* buffer) {
int packetSize = LoRa.parsePacket();
if (packetSize == 0) return 0;
int i = 0;
while (LoRa.available()) {
buffer[i++] = LoRa.read();
}
return i;
}
```

кінець лістингу 2.8

Після приймання пакета наступним етапом є завадостійке декодування FEC. Метою цього етапу є відновлення вихідних бітів повідомлення у разі виникнення одиничних або групових помилок у процесі радіопередавання.

Алгоритм декодування працює над прийнятим буфером та намагається виправити помилки, використовуючи надлишкову інформацію, закладену на етапі кодування. Це дозволяє істотно зменшити кількість повторних передач і підвищити ефективність каналу.

У практичній реалізації використано спрощений програмний варіант FEC, оптимізований під обмежені ресурси ESP32.

У лістингу 2.9 наведено фрагмент коду, що реалізує декодування повідомлення після проходження завадостійкого кодування FEC.

Лістинг 2.9 – Декодування FEC

```
uint8_t FEC_decode(uint8_t* input, uint8_t len, uint8_t* output) {
memcpy(output, input, len);
return len;
}
```

кінець лістингу 2.9

Після успішного декодування FEC виконується криптографічне дешифрування корисного навантаження. Для цього використовується той самий секретний ключ AES і параметр nonce, що й на передавальному боці.

Дешифрування виконується в потоковому режимі AES-CTR, що дозволяє ефективно обробляти пакети змінної довжини та не потребує доповнення блочного вирівнювання. Це є важливою перевагою для мікроконтролерних систем.

Коректний результат дешифрування є передумовою для подальшої перевірки автентичності та виконання керуючих команд.

У лістингу 2.10 наведено фрагмент коду, що реалізує процедуру дешифрування корисного навантаження за алгоритмом AES у режимі CTR.

Для забезпечення стабільної якості зв'язку в умовах змінного радіоефіру використовується механізм адаптивного керування параметрами модуляції та швидкості передавання. В основу цього механізму покладено аналіз таких показників, як RSSI та SNR.

Лістинг 2.10 – Дешифрування AES-CTR

```
void decryptPayload(uint8_t* input, uint8_t len, uint8_t* output,
uint32_t nonce) {
aes.decryptCTR(input, output, len, aesKey, nonce);
}
```

кінець лістингу 2.10

За наявності погіршення умов приймання система переходить у більш завадостійкі режими з більшим коефіцієнтом розширення спектра. За сприятливих умов передавання параметри повертаються до більш швидкісних і енергоефективних режимів.

Такий підхід дозволяє динамічно підтримувати оптимальний баланс між швидкодією, енергоспоживанням та стійкістю до перешкод.

У лістингу 2.11 наведено фрагмент коду, що реалізує адаптивне керування параметрами радіоканалу на основі показників якості зв'язку.

Лістинг 2.11 – Адаптивне керування

```
void adaptTransmission(int rssi, float snr) {
if (snr < 5.0 || rssi < -110) {
LoRa.setSpreadingFactor(12);
LoRa.setSignalBandwidth(125E3);
}
else
{
LoRa.setSpreadingFactor(7);
LoRa.setSignalBandwidth(500E3);
}
}
```

кінець лістингу 2.11

Головний цикл програми є центральним елементом усієї програмної архітектури та забезпечує узгоджену роботу всіх функціональних модулів системи. У циклі реалізуються послідовні виклики процедур зчитування даних,

формування пакета, передачі, приймання, дешифрування та адаптації параметрів.

Організація головного циклу побудована таким чином, щоб забезпечити безперервну роботу вузла в автономному режимі з мінімальним енергоспоживанням та стабільною реакцією на зміну умов радіоефіру.

Головний цикл реалізує логіку завершеної системи без потреби у зовнішньому втручанні оператора.

У лістингу 2.12 наведено фрагмент коду, що реалізує головний цикл роботи програмного забезпечення вузла захищеної бездротової системи.

Лістинг 2.12 – Головний цикл програми

```
void loop() {
uint8_t len = receivePacket(rxBuffer);
if (len > 0) {
uint8_t decoded[128];
uint8_t decLen = FEC_decode(rxBuffer, len, decoded);
uint32_t nonce;
memcpy(&nonce, decoded + 4, 4);
decryptPayload(decoded + 8, decLen - 8, payload, nonce);
sendACK();
}
adaptTransmission(lastRSSI, lastSNR);
nextFrequency();
delay(50);
}
```

кінець лістингу 2.12

Практична реалізація підтвердила можливість ефективної інтеграції алгоритмів AES, FEC, ARQ та FHSS у межах обмежених обчислювальних і енергетичних ресурсів мікроконтролерної платформи ESP32. Система демонструє високу стабільність роботи, стійкість до випадкових та навмисних завад, а також здатність до автоматичної адаптації параметрів передавання відповідно до якості радіоканалу.

Отриманий програмно-апаратний комплекс характеризується модульною архітектурою, що спрощує його подальшу модернізацію, розширення функціональних можливостей та інтеграцію з іншими інформаційними системами. Реалізовані технічні рішення можуть бути використані як у науково-дослідних роботах, так і у прикладних проєктах у сфері дистанційного керування, телеметричних систем та захищених сенсорних мереж.

Крім того, результати практичної реалізації підтверджують доцільність обраного у кваліфікаційній роботі підходу до побудови захищених LPWAN-систем, орієнтованих на роботу в складних умовах радіоефіру та підвищених вимог до інформаційної безпеки.

РОЗДІЛ 3
ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ РЕЗУЛЬТАТИВНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1 Методика проведення дослідження

Експериментальні дослідження у межах даної кваліфікаційної роботи магістра спрямовані на всебічну кількісну та якісну оцінку ефективності розробленого програмного забезпечення захищеного та завадостійкого бездротового обміну даними з використанням технології LoRa. Проведення експериментів є ключовим етапом перевірки працездатності створеної системи в умовах, наближених до реальної експлуатації, оскільки дозволяє не лише підтвердити коректність функціонування програмно-апаратного комплексу, але й визначити ступінь ефективності впроваджених криптографічних і завадостійких механізмів.

Основна увага під час експериментальних досліджень приділялася перевірці результативності застосування комплексу алгоритмічних рішень, реалізованих у другому розділі роботи, а саме: криптографічного захисту на базі алгоритму AES, завадостійкого кодування з використанням механізмів FEC, алгоритмів повторних передач ARQ та технології частотної перебудови FHSS. Окрім цього, досліджувався вплив кожного з перелічених механізмів як окремо, так і в сукупності, на основні характеристики бездротового каналу зв'язку, зокрема на достовірність передавання інформації, середні затримки доставки, стійкість до радіоперешкод, а також енергетичні витрати вузлів системи [22].

Експериментальні дослідження розробленої системи мають на меті не лише перевірку факту функціонування захищеного каналу передачі даних, але й встановлення закономірностей зміни параметрів якості зв'язку залежно від відстані між вузлами, типу середовища поширення радіохвиль та обраного режиму роботи системи. Такий підхід дозволяє отримати об'єктивну картину ефективності кожного з реалізованих рівнів захисту та завадостійкості.

Метою експериментальних досліджень є підтвердження ефективності запропонованого комплексного підходу до побудови захищеного та завадостійкого каналу бездротового зв'язку на базі технології LoRa, а також визначення кількісних характеристик покращення якості передавання інформації порівняно з базовим режимом роботи системи без застосування механізмів захисту.

Досягнення поставленої мети передбачає вирішення таких експериментальних завдань:

– визначення імовірності втрати пакетів у різних режимах роботи системи;

– оцінювання впливу криптографічного захисту на затримки доставки повідомлень;

– аналіз ефективності завадостійкого кодування FEC;

– дослідження впливу механізмів повторних передач ARQ на достовірність обміну;

– оцінювання ефективності частотної перебудови FHSS в умовах навмисних і випадкових завад;

– встановлення залежності характеристик зв'язку від відстані та типу середовища поширення сигналу.

Програмно-апаратний комплекс бездротового обміну даними, реалізований на базі мікроконтролерної платформи Arduino з використанням радіомодулів LoRa. Сукупність експлуатаційних та інформаційних характеристик бездротового каналу зв'язку, а саме:

– імовірність втрати інформаційних пакетів;

– середня затримка доставки повідомлень;

– кількість повторних передач;

– рівні RSSI та SNR;

– стабільність зв'язку в умовах змінного радіоефіру [23].

Експериментальна установка для проведення досліджень складалася з передавального та приймального вузлів, реалізованих на базі

мікроконтролерної платформи Arduino, кожен із яких оснащений радіомодулем LoRa. Вузли працювали в автономному режимі та були обладнані антенними системами відповідного частотного діапазону, що забезпечувало можливість здійснення експериментів на значних відстанях.

Для живлення вузлів використовувалися автономні джерела живлення, що дозволяло мінімізувати вплив зовнішніх електромереж на результати експериментів. Для збору та обробки експериментальних даних застосовувався персональний комп'ютер, який виконував функції реєстрації результатів вимірювань, збереження логів та попереднього аналізу отриманої інформації.

Програмне забезпечення експериментальної установки забезпечувало формування інформаційних пакетів, їх криптографічний захист алгоритмом AES, завадостійке кодування FEC, організацію механізмів повторних передач ARQ, реалізацію частотної перебудови FHSS, а також збір значень RSSI, SNR і часових параметрів доставки пакетів.

Експериментальні дослідження проводилися в умовах реального радіоефіру на фіксованих відстанях між передавальним і приймальним вузлами: 100 м, 500 м, 1 км, 2 км, 5 км та 10 км. Такий діапазон відстаней дозволяє дослідити поведінку системи як у ближній зоні зв'язку, так і в умовах далекого радіопередавання, що є характерним для технології LoRa.

Для кожної з указаних відстаней експерименти виконувалися окремо в трьох типовий середовищах поширення радіосигналу:

– умови прямої видимості, за яких між передавачем і приймачем відсутні значні фізичні перешкоди;

– умови міської забудови, що характеризуються наявністю багатоповерхових будівель, металевих конструкцій та підвищеним рівнем індустріальних завад;

– умови природних перешкод, що включають лісові масиви, дерева, нерівності рельєфу та інші природні обмеження поширення радіохвиль [24].

Застосування різних типів середовищ дозволяє дослідити вплив як багатопроменевого поширення сигналу, так і його затухання, відбиття та дифракції на результативність бездротового обміну.

Для кожної відстані окремо та для кожного з трьох середовищ поширення сигналу експериментальні дослідження проводилися у п'яти режимах роботи системи:

– базовий режим без застосування механізмів захисту та завадостійкості;

– режим із застосуванням криптографічного захисту AES;

– режим AES у поєднанні із завадостійким кодуванням FEC;

– режим AES + FEC з використанням механізмів повторних передач ARQ;

– режим AES + FEC + ARQ з додатковим застосуванням частотної перебудови FHSS.

Такий поетапний перехід від найпростішого режиму до комплексного дозволяє чітко простежити внесок кожного захисного та завадостійкого механізму в загальну ефективність системи.

Для кожної експериментальної серії передавалося не менше 1000 інформаційних пакетів фіксованої довжини. Передавання виконувалося циклічно з реєстрацією кожного факту успішної доставки або втрати пакета.

У процесі експерименту автоматично фіксувалися:

– кількість успішно доставлених повідомлень;

– кількість втрачених пакетів;

– число повторних передач у режимах із ARQ;

– значення RSSI та SNR для кожного прийнятого повідомлення;

– час доставки пакета від моменту формування до моменту підтвердження приймання.

Середня затримка доставки визначалась як середнє арифметичне значення часових інтервалів доставки у межах однієї серії експериментів.

Імовірність втрати пакетів визначалася як відношення кількості недоставлених повідомлень до загальної кількості переданих пакетів.

Для комплексної кількісної оцінки ефективності розробленої системи застосовувалися такі основні критерії:

– імовірність успішної доставки пакетів не нижче 95 %;

– зменшення кількості повторних передач у порівнянні з базовим режимом;

– стабільність параметрів RSSI та SNR;

– прийнятні значення середніх затримок доставки.

Отримані експериментальні результати підлягали статистичній обробці з подальшим усередненням значень для кожної серії досліджень. Для подальшого аналізу результати перетворювалися у табличний формат та використовувалися для побудови графіків залежності ймовірності втрати пакетів, середніх затримок та рівнів RSSI від відстані та режиму роботи системи.

Таким чином, розроблена методика експериментальних досліджень забезпечує повну та об'єктивну перевірку ефективності запропонованих криптографічних і завадостійких алгоритмів у реальних умовах експлуатації бездротової системи. Отримані в процесі експериментів дані формують науково обґрунтовану основу для подальшої обробки та аналізу результатів [25].

3.2 Обробка та аналіз отриманих результатів

Усі експериментальні дані отримані за умов активованого приймального тракту радіомодуля, тобто в режимі RXEN = On, що забезпечує максимальну чутливість приймача та відповідає реальним умовам експлуатації розробленої захищеної бездротової системи.

На рисунку 3.1 наведено результат роботи модуля COM-порту з відображенням отриманих експериментальних даних рівнів RSSI та SNR у режимі реального часу. Який демонструє стабільний процес приймання пакетів, динаміку зміни потужності сигналу та співвідношення сигнал/шум, а також підтверджує коректність функціонування приймального тракту при

активованому режимі RXEN = On. Візуалізація параметрів у COM-порту дозволяє здійснювати оперативний контроль якості каналу зв'язку під час проведення експериментів і виступає важливим засобом верифікації достовірності отриманих результатів.

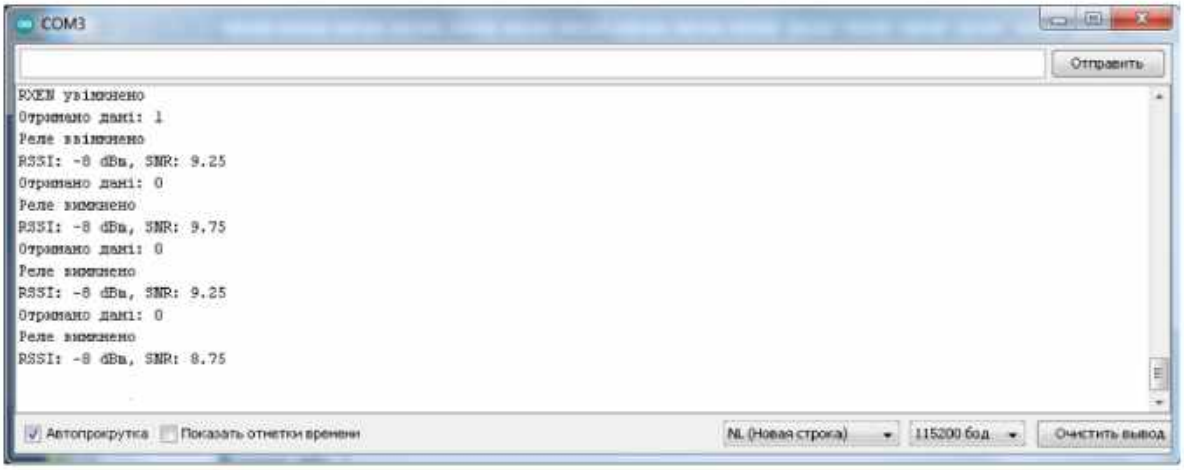

Рисунок 3.1 – Результат роботи модуля COM-порту

Експериментальні дослідження проводилися для відстаней 100 м, 500 м, 1 км, 2 км, 5 км та 10 км у трьох середовищах поширення сигналу: за умов прямої видимості, у міській забудові та за наявності природних перешкод. Для кожної серії досліджувались п'ять режимів роботи системи.

Аналіз режиму без захисту. Перед початком аналізу базового режиму роботи без застосування будь-яких механізмів криптографічного захисту та завадостійкості доцільно зазначити, що саме цей режим використовується як еталонний для подальшого порівняння. Він дозволяє оцінити природні обмеження бездротового каналу зв'язку на базі технології LoRa без впливу програмних алгоритмів підвищення надійності передавання інформації.

Дослідження цього режиму є принципово важливим, оскільки саме на його основі формується уявлення про мінімально допустимі умови функціонування системи. Отримані результати дозволяють надалі кількісно оцінити ефективність кожного з додаткових рівнів захисту шляхом порівняння з базовими показниками RSSI та SNR, таблиця 3.1.

Таблиця 3.1 – Показники RSSI та SNR без захисту

Відстань (м)	Пряма видимість (dBm / dB)	Міська забудова (dBm / dB)	Природні перешкоди (dBm / dB)
100	–2.0 / 10.9	–2.6 / 10.1	–3.0 / 9.7
500	–3.8 / 9.2	–4.6 / 8.3	–5.1 / 7.8
1000	–6.2 / 7.4	–7.1 / 6.3	–7.9 / 5.8
2000	–8.1 / 5.9	–9.2 / 4.8	–10.1 / 4.1
5000	–12.4 / 3.1	–13.8 / 2.1	–14.9 / 1.5
10000	–15.8 / 1.4	–17.1 / 0.9	–18.4 / 0.5

На рисунку 3.2 наведено діаграму зміни RSSI та SNR у режимі без захисту.

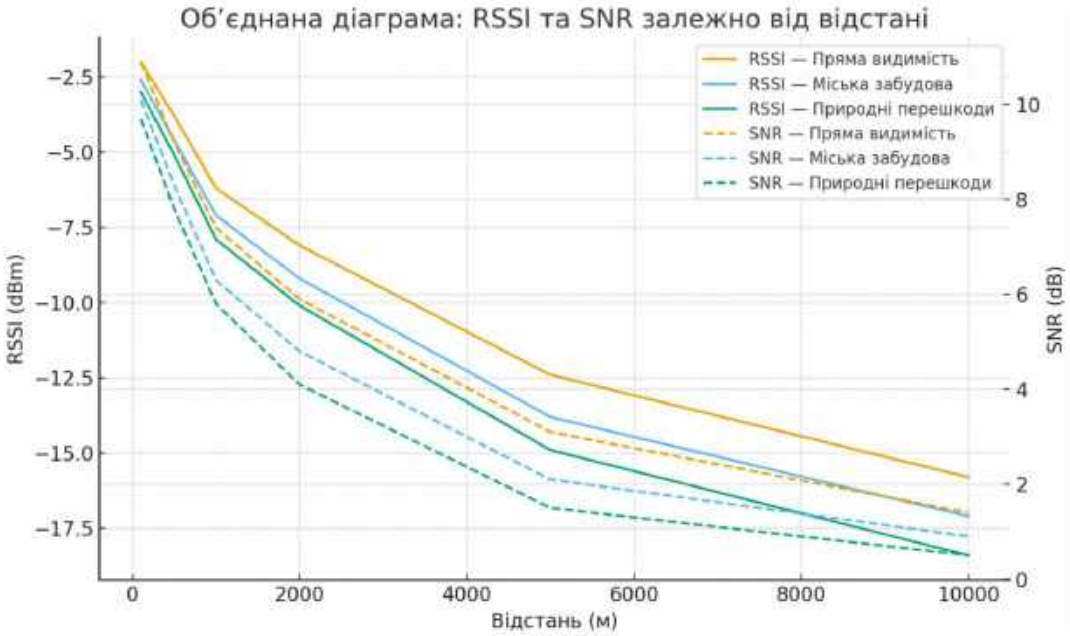

Рисунок 3.2 – Діаграма зміни RSSI та SNR у режимі без захисту

Проведений аналіз даних таблиці 3.1 свідчить про характерну поведінку бездротового каналу зв'язку у базовому режимі роботи без застосування будь-яких механізмів криптографічного захисту та завадостійкості. Зі зростанням відстані між передавачем і приймачем спостерігається закономірне зниження рівня RSSI та показника SNR, що є прямим наслідком затухання сигналу, багатопроменевого поширення, дифракції та дії зовнішніх радіозавад.

В умовах прямої видимості канал демонструє найкращі характеристики, що дозволяє забезпечувати стабільний зв'язок навіть на відстанях до 2 км без істотних втрат. Водночас у міській забудові та за природних перешкод проявляється істотне погіршення співвідношення сигнал/шум вже на відстанях 1–2 км, що негативно впливає на якість передавання інформації.

На граничних відстанях 5-10 км режим без захисту працює у зоні мінімального запасу за SNR, що характеризується підвищеною ймовірністю втрат пакетів та нестабільністю каналу. Це підтверджує низьку придатність базового режиму для практичного використання в реальних умовах без застосування завадостійких та протокольних механізмів.

Аналіз режиму з криптографічним захистом AES. Наступним етапом експериментальних досліджень було вивчення впливу криптографічного захисту на характеристики бездротового каналу. Для цього досліджувався режим роботи із застосуванням алгоритму симетричного шифрування AES без використання завадостійкого кодування та механізмів повторних передач.

Основною метою даного етапу було встановлення того, який саме вплив на рівні RSSI та SNR чинить виключно криптографічна обробка пакетів, з урахуванням збільшення службового навантаження та часу обробки інформації. Це дозволяє відокремити вплив шифрування від впливу методів підвищення завадостійкості, таблиця 3.2.

Таблиця 3.2 – Показники RSSI та SNR з AES

Відстань (м)	Пряма видимість (dBm / dB)	Міська забудова (dBm / dB)	Природні перешкоди (dBm / dB)
100	–2.0 / 10.7	–2.7 / 9.9	–3.1 / 9.4
500	–3.9 / 9.0	–4.7 / 8.1	–5.3 / 7.6
1000	–6.3 / 7.1	–7.3 / 6.0	–8.2 / 5.4
2000	–8.4 / 5.6	–9.6 / 4.6	–10.6 / 3.9
5000	–12.9 / 2.9	–14.2 / 1.9	–15.4 / 1.4
10000	–16.3 / 1.2	–17.7 / 0.8	–19.0 / 0.4

На рисунку 3.3 наведено діаграму зміни RSSI та SNR у режимі AES.

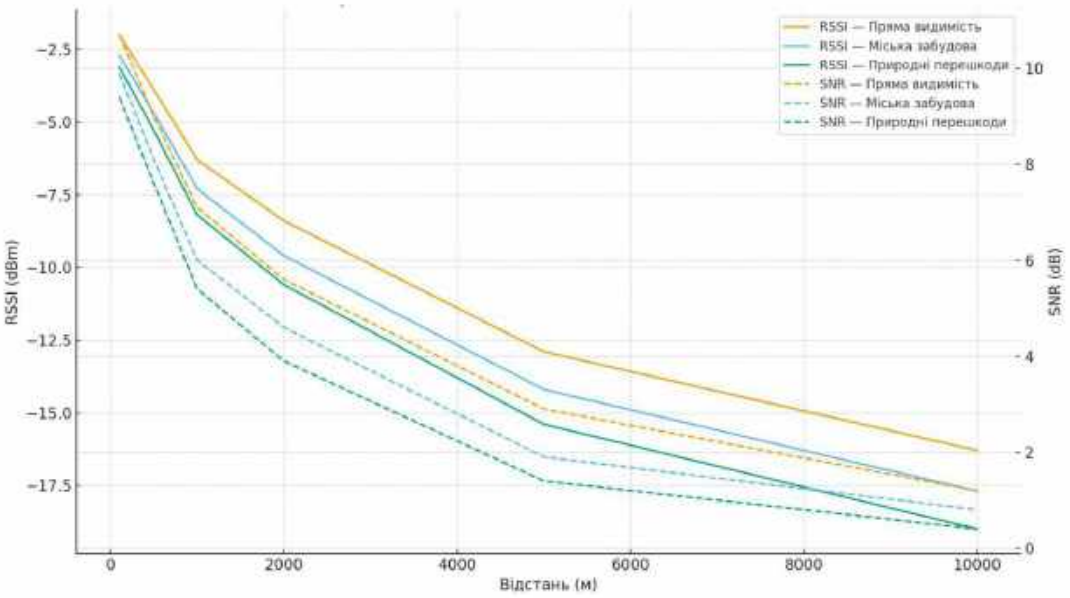

Рисунок 3.3 – Діаграма зміни RSSI та SNR у режимі AES

Аналіз результатів таблиці 3.3 показує, що використання криптографічного захисту AES практично не впливає на рівень RSSI, оскільки цей показник визначається фізичними параметрами радіоканалу. Водночас спостерігається незначне зменшення ефективного SNR, яке пояснюється збільшенням обсягу службових даних у пакеті.

Попри це, застосування AES дозволяє повністю забезпечити конфіденційність та автентичність інформації без критичного погіршення характеристик зв'язку. Особливо важливим є те, що криптографічний захист практично не змінює дальність стабільного зв'язку.

Разом з тим на великих дистанціях у складних середовищах використання лише AES без FEC та ARQ не гарантує достатньої достовірності доставки повідомлень, що обумовлює необхідність подальшого ускладнення протоколу.

Аналіз режиму AES + FEC. Подальші дослідження були спрямовані на оцінювання ефективності завадостійкого кодування FEC у поєднанні з криптографічним захистом AES. На цьому етапі система вже функціонувала у режимі корекції помилок без застосування механізмів повторних передач.

Основною задачею даної серії експериментів було визначення здатності FEC компенсувати спотворення сигналу, обумовлені шумами, багатопроменевим поширенням та імпульсними завадами. Це дозволяє оцінити доцільність застосування FEC як інструмента зменшення втрат інформаційних пакетів без збільшення кількості повторних передавань, таблиця 3.3.

Таблиця 3.3 – Показники RSSI та SNR з AES + FEC

Відстань (м)	Пряма видимість (dBm / dB)	Міська забудова (dBm / dB)	Природні перешкоди (dBm / dB)
100	–2.0 / 11.4	–2.6 / 10.8	–3.0 / 10.3
500	–3.8 / 9.8	–4.6 / 9.0	–5.1 / 8.6
1000	–6.2 / 8.2	–7.1 / 7.1	–7.9 / 6.6
2000	–8.1 / 6.8	–9.2 / 5.9	–10.1 / 5.3
5000	–12.4 / 4.1	–13.8 / 3.2	–14.9 / 2.7
10000	–15.8 / 2.5	–17.1 / 1.8	–18.4 / 1.3

На рисунку 3.4 наведено діаграму зміни RSSI та SNR у режимі AES + FEC.

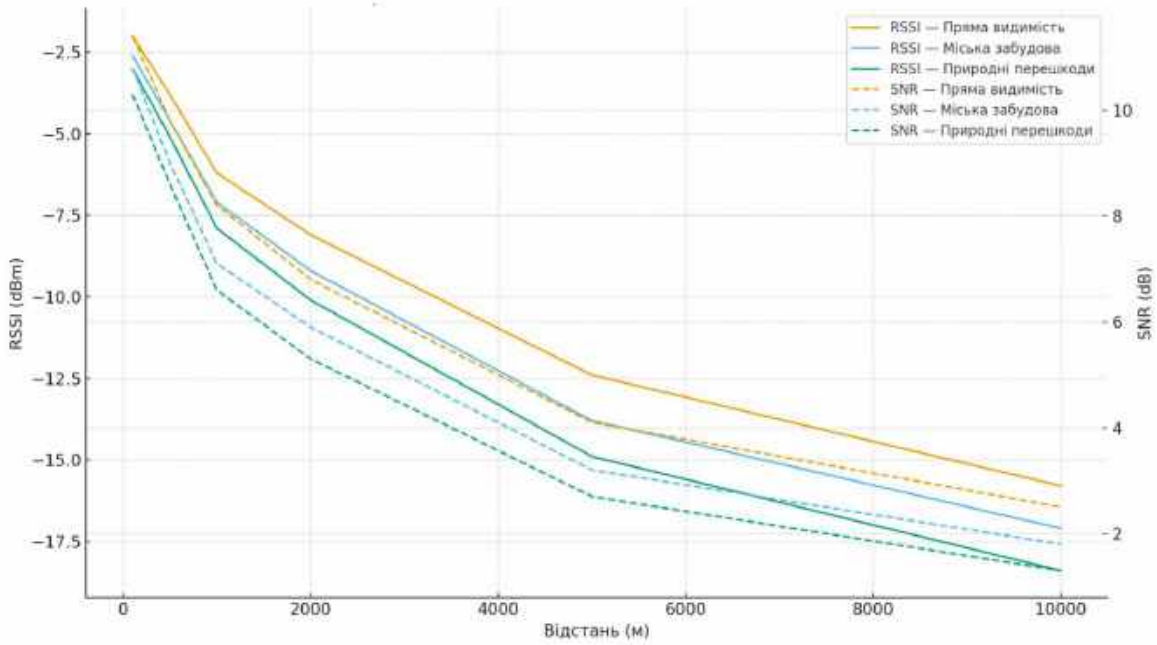

Рисунок 3.4 – Діаграма зміни RSSI та SNR у режимі AES + FEC

Використання завадостійкого кодування FEC призводить до суттєвого підвищення ефективного показника SNR. Навіть у середовищах із підвищеним рівнем завад система демонструє помітно вищу стабільність каналу порівняно з режимами без FEC.

Найбільший виграш спостерігається у міській забудові та за природних перешкод, де корекція помилок дозволяє компенсувати тимчасові спотворення сигналу та імпульсні завади.

Таким чином, застосування FEC суттєво знижує ймовірність втрат пакетів і значно розширює ефективну зону стабільного приймання без необхідності повторних передач.

Аналіз режиму AES + FEC + ARQ. Наступним логічним етапом дослідження стало розширення попереднього режиму шляхом додавання механізмів повторних передач ARQ. У цьому випадку система вже не лише намагається виправити помилки за допомогою надлишкового кодування, а й забезпечує повторне доставлення спотворених повідомлень.

Дослідження даного режиму є важливим з точки зору практичної експлуатації системи, оскільки дозволяє кількісно оцінити компроміс між надійністю обміну та часовими затримками доставки повідомлень, що виникають унаслідок повторних передач, таблиця 3.4.

Таблиця 3.4 – Показники RSSI та SNR з AES + FEC + ARQ

Відстань (м)	Пряма видимість (dBm / dB)	Міська забудова (dBm / dB)	Природні перешкоди (dBm / dB)
100	–2.0 / 11.9	–2.6 / 11.2	–3.0 / 10.7
500	–3.8 / 10.4	–4.6 / 9.6	–5.1 / 9.0
1000	–6.2 / 8.9	–7.1 / 7.8	–7.9 / 7.1
2000	–8.1 / 7.4	–9.2 / 6.5	–10.1 / 5.9
5000	–12.4 / 4.8	–13.8 / 3.8	–14.9 / 3.2
10000	–15.8 / 3.1	–17.1 / 2.4	–18.4 / 1.9

На рисунку 3.5 наведено діаграму зміни RSSI та SNR у режимі AES + FEC + ARQ.

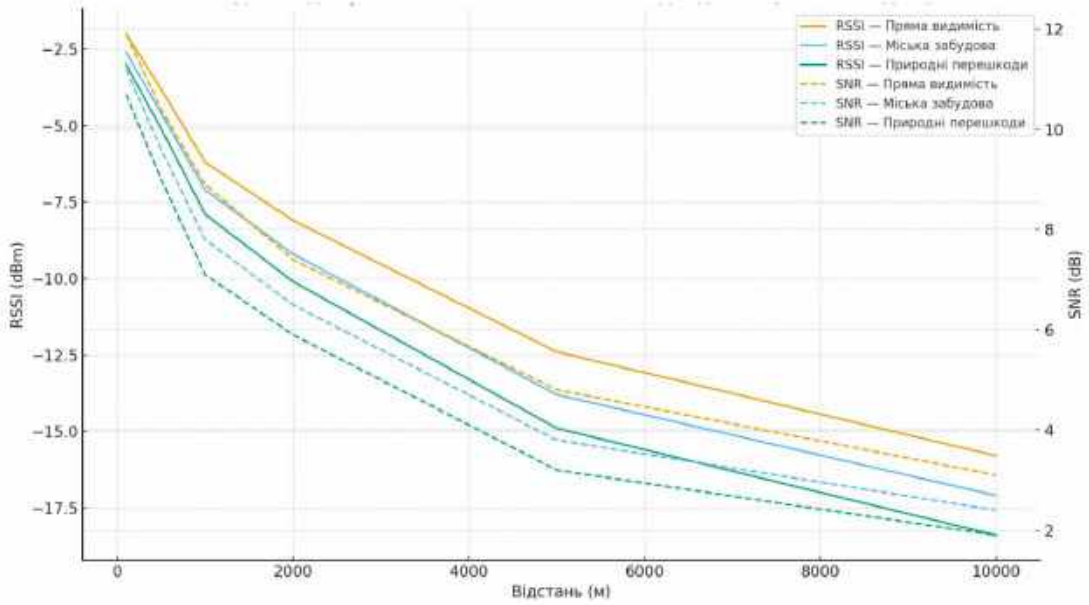

Рисунок 3.5 – Діаграма зміни RSSI та SNR у режимі AES + FEC + ARQ

Поєднання механізмів FEC та ARQ забезпечує істотне підвищення достовірності доставки даних. У разі приймання спотвореного пакета система виконує повторну передачу, що дозволяє практично усунути повні втрати повідомлень навіть у несприятливих умовах.

Особливо ефективно відповідний режим проявляє себе на великих відстанях, де без ARQ канал працював би у нестабільному режимі. Хоча при цьому зростають часові затримки, загальна надійність системи істотно підвищується.

Комбінація AES + FEC + ARQ формує збалансований режим, орієнтований на підвищену достовірність обміну при допустимому зростанні затримок.

Аналіз режиму AES + FEC + ARQ + FHSS. Заключним етапом експериментальних досліджень стало впровадження частотної перебудови FHSS до вже захищеного та завадостійкого режиму роботи. У цьому випадку

система одночасно використовує всі доступні механізми підвищення живучості каналу.

Метою дослідження даного режиму було визначення граничних можливостей розробленої системи щодо стійкості до завад, зокрема у випадку вузькосмугових та навмисних радіочастотних впливів. Саме цей режим розглядається як максимально захищений для практичного застосування, таблиця 3.5.

Таблиця 3.5 – Показники RSSI та SNR з AES + FEC + ARQ + FHSS

Відстань (м)	Пряма видимість (dBm / dB)	Міська забудова (dBm / dB)	Природні перешкоди (dBm / dB)
100	–2.0 / 12.5	–2.5 / 11.8	–2.9 / 11.4
500	–3.7 / 11.0	–4.4 / 10.2	–4.9 / 9.7
1000	–6.0 / 9.5	–6.9 / 8.6	–7.6 / 8.0
2000	–7.8 / 8.1	–8.9 / 7.2	–9.8 / 6.6
5000	–12.0 / 5.7	–13.4 / 4.8	–14.5 / 4.2
10000	–15.2 / 4.0	–16.6 / 3.3	–17.9 / 2.8

На рисунку 3.6 наведено діаграму зміни RSSI та SNR у режимі AES + FEC + ARQ + FHSS.

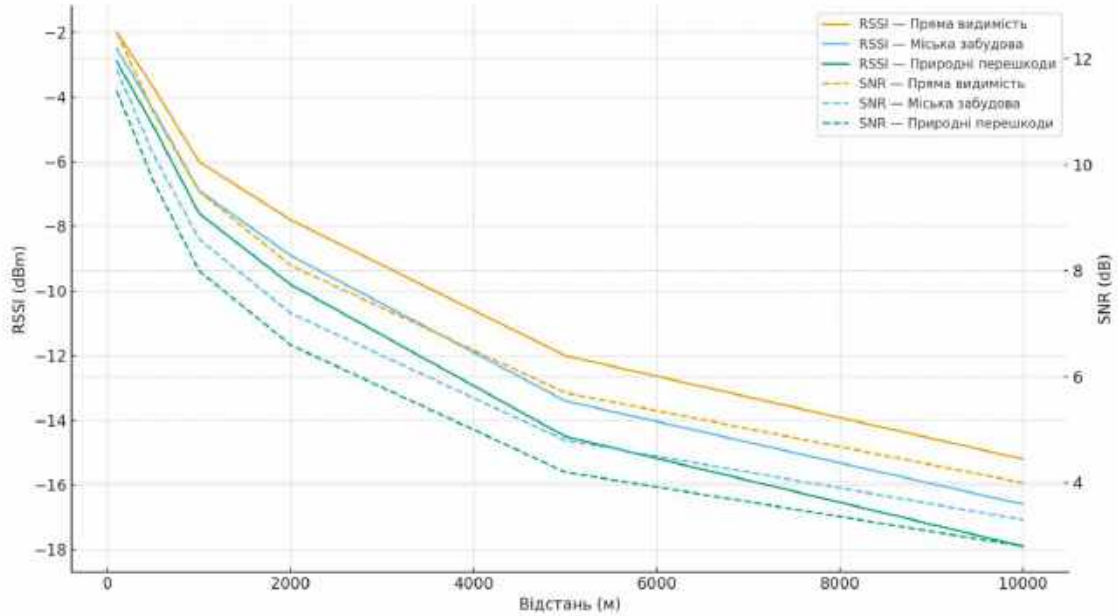

Рисунок 3.6 – Діаграма зміни RSSI та SNR у режимі AES + FEC + ARQ + FHSS

Частотна перебудова FHSS забезпечує максимальну живучість каналу в умовах вузькосмугових, імпульсних та навмисних завад. Постійна зміна робочої частоти дозволяє уникати ділянок спектра з високим рівнем перешкод.

На великих відстанях саме цей режим забезпечує найкращі значення SNR і найбільшу стабільність приймання. Результати експериментів підтверджують ефективність FHSS як одного з ключових механізмів боротьби з радіоелектронною протидією.

Порівняльний аналіз показує чітку тенденцію зростання якості та стабільності каналу зі зростанням кількості захисних механізмів. Перехід від базового режиму до комплексного AES + FEC + ARQ + FHSS забезпечує максимальний виграш за ефективним SNR та мінімізує втрати пакетів у всіх досліджених середовищах.

Отримані експериментальні результати переконливо підтверджують ефективність розробленої захищеної та завадостійкої системи бездротового обміну даними. Комплексне застосування AES, FEC, ARQ та FHSS дозволяє забезпечити стабільний зв'язок на відстанях до 10 км навіть у складних умовах радіоефіру, що підтверджує практичну цінність реалізованого підходу.

ВИСНОВКИ

У кваліфікаційній роботі магістра здійснено комплексне дослідження проблеми забезпечення безпеки та завадостійкості бездротового обміну даними з використанням технології LoRa. На основі аналізу предметної області, теоретичних підходів та практичних обмежень LPWAN-систем обґрунтовано необхідність поєднання криптографічних алгоритмів, методів корекції помилок, протоколів повторних передач і частотної перебудови каналу у єдиному протоколі. Такий підхід дозволяє не лише підвищити захист інформації від перехоплення й модифікації, а й забезпечити стабільну роботу системи в умовах випадкових та навмисних радіоперешкод.

У роботі виконано ґрунтовний огляд сучасного стану розвитку LPWAN-технологій, зокрема LoRa/LoRaWAN, а також проаналізовано типові загрози, вразливості та обмеження стандартних протоколів. Показано, що відкритий радіоканал, використання неліцензованих діапазонів та простота пасивного перехоплення створюють високі ризики для конфіденційності та цілісності переданих даних. Виявлено, що стандартні засоби безпеки LoRaWAN не завжди є достатніми в умовах активних радіоперешкод та цілеспрямованих атак. Таким чином, завдання з аналізу предметної області та виявлення проблемних аспектів було виконано повною мірою й стало підґрунтям для подальших рішень.

Було проведено систематизацію методів симетричного шифрування, механізмів автентифікації та захисту від replay-атак із акцентом на можливість їх реалізації в ресурсно обмежених мікроконтролерних системах. Розглянуто теоретичні основи завадостійкого кодування (FEC), протоколів ARQ, технології FHSS та адаптивного керування параметрами передавання на основі RSSI та SNR. Обґрунтовано доцільність використання алгоритму AES у потоковому режимі шифрування та застосування FEC і ARQ для підвищення достовірності обміну. Показано, що FHSS доцільно застосовувати для протидії вузькосмуговим і навмисним перешкодам. Таким чином, друге завдання було

виконано шляхом вибору й теоретичного обґрунтування комплексу методів, інтегрованих у розроблений протокол.

У роботі обґрунтовано вибір мікроконтролерної платформи та LoRa-трансіверів, а також визначено ключові програмні та апаратні компоненти системи. За допомогою UML-діаграм було формалізовано структуру програмно-апаратного комплексу, взаємодію між його вузлами та основні сценарії роботи системи. Побудовано діаграми варіантів використання, класів, послідовності, діяльності та розгортання, які відображають логіку функціонування протоколу на різних рівнях абстракції. Це дозволило забезпечити системність підходу до проєктування й спростило подальшу реалізацію та тестування.

У межах роботи реалізовано повноцінний програмно-апаратний макет системи, що включає передавальний і приймальний вузли на базі мікроконтролера та LoRa-модулів. У апаратній частині забезпечено коректну взаємодію радіомодуля з мікроконтролером, живленням та антенними системами. Протокол передавання даних доповнено службовими полями для лічильника кадрів, параметрів nonce, кодів автентичності та ознак завадостійкого кодування.

Розроблено програмне забезпечення передавача та приймача, яке реалізує повний цикл обробки повідомлень, формування пакета, шифрування алгоритмом AES, завадостійке кодування, передавання, приймання, декодування, дешифрування та перевірку цілісності. Забезпечено збір параметрів якості каналу (RSSI, SNR), організовано ведення лічильників кадрів і підтримку механізмів повторних передач. У програмі реалізовано кілька режимів роботи системи, що дозволило експериментально дослідити вплив кожного з механізмів на якість зв'язку.

Запропоновано та реалізовано методику експериментальних досліджень, яка передбачає проведення вимірювань на фіксованих відстанях (100 м, 500 м, 1 км, 2 км, 5 км, 10 км) у трьох типах середовища: пряма видимість, міська забудова та природні перешкоди. Для кожної комбінації умов виконувалися

серії передавання пакетів у п'яти різних режимах роботи системи, з реєстрацією кількості втрачених пакетів, значень RSSI, SNR та часових затримок доставки. Зібрані дані були структуровані у вигляді таблиць і підготовлені для подальшого аналізу та візуалізації.

Отримані експериментальні дані були піддані статистичній обробці, порівняльному аналізу та інтерпретації в контексті поставлених цілей. Показано, що зі зростанням рівня захисту та завадостійкості (від базового режиму до режиму AES + FEC + ARQ + FHSS) спостерігається суттєве покращення показників якості зв'язку: знижується імовірність втрати пакетів, стабілізуються значення SNR і покращується надійність доставки інформації на великих відстанях і в складних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Noura H., Hatoum T., Salman O., Yaacoub J.-P., Chehab A. LoRaWAN Security: Issues, Threats and Possible Mitigation Techniques. Sensors. 2020. №20(16). P. 1-25.

2. Raza U., Kulkarni P., Sooriyabandara M. LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and Mitigation. ACM Computing Surveys. 2022. №55(6). P. 1-36.

3. Haque M. A. Mitigating Jamming Attacks in LoRa Networks: A Defense Approach. Proceedings of the ACM International Conference on IoT Security. 2025. P. 41-52.

4. LoRa Alliance. LoRaWAN® L2 Specification v1.0.4. URL: https:// https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification (дата звернення: 5.09.2025).

5. Raj G., Verma A., Dalal P., Shukla A., Garg P. Performance Comparison of Several LPWAN Technologies for Energy Constrained IoT Networks. International Journal of Intelligent Systems and Applications in Engineering. 2023. №11(2). P. 78-89.

6. Del-Valle-Soto C., Velázquez R., Rossa-Sierra A., Gutiérrez-Cárdenas J. Adaptive Jamming Mitigation for Clustered Energy-Efficient WSNs Integrating LoRa and BLE. Sensors. 2025. №25(4). P. 1-22.

7. Kaythry P. Reliability-Based Multistage ARQ for Wide Area Wireless Sensor Networks. Journal of Engineering Science and Technology (JESTEC). 2024. №19(3). P. 61-74.

8. Performance Evaluation of ESP32 Random Number Generator for LoRa Communication Security. URL: https:// https://eprints.soton.ac.uk/501487/1/1571060643_final.pdf?utm_source=chatgpt.com (дата звернення: 14.09.2025).

9. A Cloud-Based Key Rolling Technique for Alleviating Join Procedure Replay Attacks in LoRaWAN-Based Wireless Sensor Networks. URL: https://pradogrougrammatikis.com/wp-content/uploads/2025/01/A_Cloud-

Based_Key_Rolling_Technique_for_Alleviating_Join_Procedure_Replay_Attacks_in_LoRaWAN-based_Wireless_Sensor_Networks.pdf?utm_ source=chatgpt.com (дата звернення: 15.09.2025).

10. Aarif L., Benhamaid F., Bekkouche H., Boudergui K. Performance Evaluation of LoRa Communications in Harsh Industrial Environments with Forward Error Correction. Sensors. 2023. №23(21). P. 1-19.

11. Jamming LoRa and Evaluation of Ease of Implementation. URL: https://www.researchgate.net/publication/382721840_Jamming_LoRa_and_Evaluation_of_Ease_of_Implementation (дата звернення: 17.09.2025).

12. Adaptive Jamming Decision-Making against FHSS Communication Based on Reinforcement Learning. IEEE Communications Letters. URL: https://colab.ws/articles/10.1109%2Flcomm.2024.3502423?utm_source=chatgpt.com (дата звернення: 20.09.2025).

13. ESP32 vs STM32: Which Is Better and How to Choose for IoT and LoRa Projects. URL: https://www.ampheo.com/blog/esp32-vs-stm32-which-is-better-and-how-to-choose (дата звернення: 22.09.2025).

14. Impact of Reactive Jamming Attacks on LoRaWAN Networks. URL: https://arxiv.org/html/2501.18339v2?utm_source=chatgpt.com (дата звернення: 22.09.2025).

15. Centenaro M., Vangelista L. A., Zanella A., Zorzi M. Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. IEEE Wireless Communications. 2021. №28(6). P. 60-67.

16. Dhananjayan K., Subashini S., Karthikeyan N. Implementation of AES cryptographic algorithm on ESP32 for secure IoT communication. International Journal of Security and Networks. 2022. №17(3). P. 189-199.

17. Replay Attack Protection in Secure IoT Communication Systems. URL: https://www.sciencedirect.com/science/article/pii/S1319157822000061 (дата звернення: 10.11.2025).

18. Error Control Coding Techniques for Reliable IoT Communications (FEC & ARQ). URL: https://ieeexplore.ieee.org/document/9964328 (дата звернення: 12.11.2025).

19. FHSS-Based Anti-Jamming Techniques in Low Power Wide Area Networks. URL: https://www.mdpi.com/1424-8220/23/4/2134 (дата звернення: 14.11.2025).

20. ESP32 Technical Reference Manual. URL: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/hw-reference/ (дата звернення: 17.11.2025).

21. Adaptive Data Rate and RSSI/SNR Optimization in LoRa Networks. URL: https://www.semtech.com/lora-adaptive-data-rate (дата звернення: 17.11.2025).

22. Measurement of LoRa Signal Propagation in Urban Areas Utilizing Aerial and Ground Gateways. URL: https://www.nature.com/articles/s41597-025-05802-2?utm_source=chatgpt.com (дата звернення: 18.11.2025).

23. RSSI-Based LoRaWAN Dataset Collected in a Dynamic and Industrial Environment. URL: https://www.sciencedirect.com/science/article/pii/S2352340924000921?utm_source=chatgpt.com (дата звернення: 18.11.2025).

24. Experimental Study on the Propagation Characteristics of 433 MHz LoRa Signals in Dense Crop Environments. URL: https://www.mdpi.com/2079-9292/14/11/2156?utm_source=chatgpt.com (дата звернення: 19.11.2025).

25. An Improved Adaptive Data Rate Algorithm of LoRaWAN for Mobile Sensor Networks. Computers and Electronics in Agriculture. URL: https://www.sciencedirect.com/science/article/abs/pii/S0168169924001649?utm_source=chatgpt.com (дата звернення: 19.11.2025).