Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Програмно-технічні засоби захисту інформації при передачі між IoT-пристроями по радіоканалу
Назва теми

КвРКІ 220036.22.01.19 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Виконав: студент 3 курсу, група КІ2с-22-1 _____ Дмитро СВЕРЗОЛЕНКО
Підпис, Ініціали, прізвище

Керівник _____ Володимир ГРИГА
Підпис, дата, Ініціали, прізвище

Нормоконтролер _____ Тетяна КИСІЛЬ
Підпис, дата, Ініціали, прізвище

До захисту допускаю:
зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Підпис, Ініціали, прізвище

«19» червня 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

" 10 " 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Дмитру СВЕРЗОЛЕНКО
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Програмно-технічні засоби захисту інформації при передачі між IoT-пристроями по радіоканалу

Керівник проекту (роботи) Володимир ГРИГА, к.т.н., доцент
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 07.02.2025 р. № 23

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз сучасного стану програмно-технічних рішень для захисту інформації в середовищі iot-пристроїв

Вибір програмно-технічних засобів захисту інформації для IoT-пристроїв

Програмно-апаратна реалізація захисту інформації при передачі між IoT-пристроями по радіоканалу

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Система захисту радіоканалів IoT

Основні етапи алгоритму захисту радіоканалу

Схема-креслення проєкту

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийня
Нормоконтроль	Тетяна КИСІЛЬ, доцент кафедри КІІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІІС		

7. Дата видачі завдання «_10_»_____01_____2025 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітк
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2025	виконан
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2025	виконан
3	Робота над розділом 1 – аналіз сучасного стану програмно-технічних рішень для захисту інформації в середовищі IoT-пристроїв	01.03.2025	виконан
4	Робота над розділом 2 – вибір програмних засобів розробки системи захисту інформації в IoT-пристроях	01.04.2025	виконан
5	Робота над розділом 3 – програмно-апаратна реалізація системи захисту інформації при передачі між IoT-пристроями по радіоканалу	29.04.2025	виконан
6	Оформлення пояснювальної записки згідно вимог	25.05.2025	виконан
7	Попередній захист кваліфікаційної роботи	26.05.2025	виконан
8	Захист кваліфікаційної роботи на засіданні ЕК	Червень 2025 року	

Студент _____ Дмитро СВЕРЗОЛЕНКО
Підпис Ініціали

Керівник роботи _____ Володимир ГРИГА
Підпис Ініціали

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 220036.22.01.19 ПЗ	Пояснювальна записка	75		
			Графічні матеріали			
2		КвРКІ 220036.22.01.19 Е8	Система захисту радіоканалів	1		
			IoT			
3		КвРКІ 220036.22.01.19 Е8	Основні етапи алгоритму	1		
			захисту радіоканалу			
4		КвРКІ 220036.22.01.19 Е8	Схема-креслення проєкту	1		

КвРКІ 220036.22.01.19 ВП

Зм	Арк	№ докум	Підпис	Дата
Розробив		Сверзоленко		19.06
Перевір.		Грига		19.06
Н. контр.		Кисіль		19.06
Затв.		Павлова		19.06

Відомість проекту

Літера	Аркуш	Аркушів
У	1	1

ХНУ, КІ2с-22-1

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Програмно-технічні засоби захисту інформації при передачі між IoT-пристроями по радіоканалу».

Автор роботи: Дмитро СВЕРЗОЛЕНКО

Керівник роботи: Володимир ГРИГА

Пояснювальна записка: 75 с., 17 рис., 9 табл., 60 джерел.

Метою дипломної роботи є розробка ефективних програмно-технічних засобів захисту інформації при передачі даних між IoT-пристроями по радіоканалу, що забезпечують високий рівень безпеки від зовнішніх атак та несанкціонованого доступу.

Об'єктом дослідження є процес забезпечення інформаційної безпеки під час обміну даними між IoT-пристроями по радіоканалу.

Предметом дослідження є програмно-технічні засоби захисту інформації, що застосовуються для забезпечення конфіденційності, цілісності та доступності даних у бездротових IoT-мережах.

Під час проведення даного дослідження використовувались методи системного аналізу, порівняння сучасних засобів захисту, а також моделювання для оцінки ефективності різних протоколів захисту.

_____ 30.05.2025

Підпис студента Дата

ЗМІСТ

ВСТУП

Сучасні тенденції розвитку цифрових технологій свідчать про стрімке зростання кількості пристроїв, що входять до екосистеми Інтернету речей (IoT). Такі пристрої активно інтегруються в побут, промисловість, охорону здоров'я, транспорт, сільське господарство та інші сфери, забезпечуючи автоматизований збір, обробку й обмін даними. Особливе значення має забезпечення безперервного зв'язку між IoT-модулями через радіоканали, що дозволяє реалізовувати гнучкі, розподілені й масштабовані системи.

У зв'язку з цим зростає попит на ефективні, гнучкі та недорогі рішення, які забезпечують захист інформації в IoT-мережах, особливо під час передачі даних бездротовими каналами зв'язку. Сучасні мікроконтролери, що використовуються в IoT-пристроях, як-от ESP32, STM32, Arduino з радіомодулями (наприклад, NRF24L01, LoRa або Wi-Fi), мають достатню обчислювальну потужність для реалізації вбудованих криптографічних алгоритмів, автентифікації та контролю доступ.

Водночас, з урахуванням масштабів використання IoT-технологій та збільшення кількості атак на бездротові мережі, постає проблема розробки енергоефективних алгоритмів шифрування, які не створюють надмірного навантаження на обчислювальні ресурси пристрою. Також актуальними є питання сумісності різних стандартів бездротового зв'язку, інтеграції хмарних платформ для централізованого управління даними та дотримання норм кібербезпеки на державному та міжнародному рівнях. Таким чином, дослідження в сфері безпеки та надійності IoT-систем є критично важливим завданням сучасної прикладної науки та інженерії.

Розробка рішень, здатних забезпечити інформаційну безпеку на рівні сенсорних вузлів і вузлів керування, дозволяє не лише знизити ризики кіберзагроз, а й підвищити довіру до IoT-рішень серед споживачів та бізнесу.

Мета роботи полягає в розробці ефективних програмно-технічних засобів захисту інформації під час бездротової передачі даних між IoT-пристроями, що

функціонують у складі розподіленої мережі. Пріоритетом є досягнення високого рівня безпеки від зовнішніх атак при збереженні енергоефективності та мінімального впливу на затримку передачі даних.

Досягнення поставленої мети передбачає поетапне виконання комплексу дослідницьких і проєктних завдань. На початковому етапі необхідно здійснити глибокий аналіз актуальних загроз, що виникають під час радіозв'язку між IoT-пристроями. Особливу увагу слід приділити практичним сценаріям застосування Інтернету речей у різних сферах, адже специфіка кожної з них формує унікальні виклики в контексті забезпечення інформаційної безпеки. Типовими загрозами є перехоплення даних, підміна повідомлень, втручання в трафік та здійснення атак типу «людина посередині».

Наступний етап полягає в детальному огляді та порівнянні наявних технічних і програмних засобів захисту даних у середовищі IoT. Оцінюється їхня ефективність щодо захисту радіоканалів, а також сумісність із обмеженими апаратними ресурсами мікроконтролерів, що широко використовуються у вбудованих системах. Особлива увага приділяється таким критеріям, як швидкодія алгоритмів, енергоспоживання, легкість інтеграції та стійкість до поширених типів атак.

Розроблене рішення спрямоване на використання в галузях, де особливо важливими є надійна передача інформації та захист від зовнішнього втручання. Зокрема, це стосується систем розумного дому, телемедицини, критично важливих об'єктів інфраструктури, систем автоматизованого керування транспортом і енергетичних мереж. Впровадження такої системи дозволяє суттєво знизити ризики витоку або модифікації інформації, запобігти кіберінцидентам і забезпечити стабільну роботу пристроїв навіть в умовах нестабільного зв'язку або цільового зовнішнього впливу.

1. АНАЛІЗ СУЧАСНОГО СТАНУ ПРОГРАМНО-ТЕХНІЧНИХ РІШЕНЬ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В СЕРЕДОВИЩІ ІОТ-ПРИСТРОЇВ

1.1 Аналіз предметної області

У сучасному ландшафті Інтернет речей (IoT) служить наріжним каменем для численних технологічних досягнень, об’єднуючи мільярди пристроїв, які миттєво передають дані. Тим не менш, поширення цих технологій породжує значні проблеми щодо забезпечення їх безпеки. Забезпечення безпеки пристроїв IoT має першочергове значення, враховуючи, що ці пристрої часто обробляють конфіденційну інформацію або керують основними системами [11, 14].

Важливою проблемою в сфері безпеки IoT є неадекватний рівень захисту, встановлений на етапі проектування. Багато виробників віддають пріоритет швидкому виходу на ринок, що призводить до ігнорування фундаментальних принципів кібербезпеки. Крім того, обмежені апаратні ресурси пристроїв IoT створюють проблеми для впровадження надійних засобів шифрування та автентифікації. Дослідження показують, що понад 70% пристроїв Інтернету речей мають принаймні одну вразливість, яка може бути використана хакерами.

Значна проблема стосується використання стандартизованих протоколів зв’язку, включаючи Wi-Fi, Bluetooth і ZigBee. Хоча ці технології пропонують значну швидкість передачі даних, вони супроводжуються різними визнаними вразливими місцями. Наприклад, мережа Wi-Fi може бути скомпрометована через атаки типу "людина посередині" або дані можуть бути перехоплені в з'єднаннях Bluetooth через неналежний захист паролем. Крім того, численні пристрої Інтернету речей, як правило, мають відкриті порти, що дозволяє хакерам отримати несанкціонований доступ. Такі недоліки в цих протоколах часто призводять до значних витоків даних і збоїв у системі.

Окрім технічних аспектів, складність безпеки IoT ще більше посилюється людськими факторами. Слабке використання пароля, недостатня обізнаність користувачів щодо заходів безпеки та ігнорування налаштувань конфіденційності

значно підвищують сприйнятливість пристроїв IoT до атак. Поширеною проблемою є наявність незмінних заводських паролів, які зловмисники використовують для швидкого проникнення на пристрої. Ці типи атак можуть призвести не лише до крадіжки даних, але й до значних збоїв у роботі мереж.

Відсутність універсальних стандартів для розробників значно впливає на поточний ландшафт безпеки IoT. У багатьох країнах створення пристроїв IoT не регулюється чіткими правилами, що призводить до різноманітних рішень безпеки. Впровадження узгоджених міжнародних стандартів може підвищити безпеку екосистеми IoT.

1.2 Аналіз наявного програмно-апаратного забезпечення

Програмне забезпечення (SW) має важливе значення для роботи пристроїв IoT, полегшуючи їх взаємодію, обробку даних і виконання завдань. Тим не менш, саме програмне забезпечення є одним із основних компонентів, схильних до ризиків і загроз, оскільки вразливі місця в програмному забезпеченні можуть поставити під загрозу цілісність усієї системи. У цьому розділі розглянуто основні категорії вразливостей програмного забезпечення та описано методи їх виявлення та запобігання.

Щоб виявити вразливості програмного забезпечення, доцільно застосовувати комплексну методологію, яка охоплює різноманітні аспекти аналізу системи. Одним із критичних напрямів є вивчення вихідного коду, адже саме в ньому найчастіше криються недоліки, які можуть призвести до серйозних загроз безпеці. Неправильна обробка даних, помилки програмування або нехтування базовими принципами безпеки можуть спричинити появу таких вразливостей, як впровадження SQL-запитів, переповнення буфера або несанкціоноване керування пам’яттю. Зловмисники здатні використовувати подібні недоліки для отримання доступу до конфіденційної інформації або контролю над пристроями.

З метою зменшення ризиків і підвищення стійкості системи застосовують низку стратегій: впровадження принципів безпечної розробки, зокрема

використання методологій SSDLC, дозволяє враховувати питання безпеки на всіх етапах створення програмного забезпечення. Регулярні оновлення та автоматичне встановлення патчів забезпечують актуальність і захист від відомих загроз. Також критично важливим є використання шифрування даних як під час передавання, так і при зберіганні. І, нарешті, застосування виключно перевірених і сертифікованих сторонніх компонентів значно знижує ймовірність використання потенційно небезпечного програмного забезпечення.

Враховуючи, що пристрої IoT часто функціонують у середовищах з обмеженими ресурсами, звичайні заходи безпеки можуть виявитися недостатніми. Відповідно, спеціально для IoT розробляються спеціальні стратегії, включаючи легкі алгоритми шифрування та компактні системи моніторингу. Крім того, впровадження апаратних механізмів автентифікації, таких як Trusted Platform Module (TPM), має важливе значення для підвищення безпеки [22, 49].

Таким чином, уразливості програмного забезпечення продовжують становити серйозну проблему для Інтернету речей, однак їх виявлення та пом’якшення можна ефективно вирішити за допомогою впровадження сучасних аналітичних інструментів, дотримання встановлених стандартів розробки та застосування передових технологій безпеки.

1.2.1 Слабкі паролі та відсутність автентифікації

Слабкі паролі та відсутність автентифікації залишаються одними з найпоширеніших і найнебезпечніших вразливостей у сфері Інтернету речей (IoT). Саме ці чинники часто спричиняють успішні кібератаки, що дозволяють зловмисникам отримувати несанкціонований доступ до пристроїв та мереж, а також компрометувати конфіденційні дані користувачів або організацій. Проблема виникає з кількох причин, що тісно пов’язані як із технічними, так і з людськими факторами.

Однією з основних причин є використання стандартних або незмінних паролів, які залишаються встановленими за замовчуванням і рідко змінюються

користувачами. Такі паролі часто є загальновідомими та легко знаходяться в публічних базах даних або за допомогою спеціалізованих скриптів. Додатково, технічні обмеження багатьох IoT-пристроїв - зокрема мала обчислювальна потужність і обмежений обсяг пам’яті - не дозволяють реалізовувати складні механізми захисту, зокрема багатофакторну автентифікацію. Не менш важливою є й низька обізнаність користувачів, які не приділяють належної уваги вибору сильних паролів або використанню сучасних методів автентифікації. До цього додається ще й те, що деякі виробники приділяють недостатньо уваги безпеці під час розробки пристроїв, через що на ринку з’являються продукти з мінімальними або формальними заходами захисту.

Важливим аспектом залишається й забезпечення актуальності програмного забезпечення пристроїв. Регулярне оновлення прошивки дозволяє своєчасно усувати відомі вразливості та впроваджувати нові захисні механізми. Додатково до цього, системи можуть бути оснащені функціями виявлення та блокування підозрілих спроб входу, що дозволяє швидко реагувати на потенційні загрози. У деяких випадках доцільним є впровадження біометричних методів автентифікації, як-от сканування відбитків пальців або розпізнавання обличчя, особливо в пристроях із підвищеним рівнем ризику. Не менш важливо проводити інформаційні кампанії для користувачів, підвищуючи їхню обізнаність про важливість надійного захисту та регулярної зміни автентифікаційних даних.

Загалом, проблема слабких паролів та відсутності автентифікації в IoT-середовищі є системною, але розв’язуваною. Її подолання потребує одночасних зусиль з боку розробників, користувачів та регуляторних органів для формування безпечного цифрового простору.

1.3 Визначення вимог до системи автоматизації та розробка технічного завдання

Технології передачі даних є важливими компонентами ефективності роботи Інтернету речей (IoT), полегшуючи зв’язок між пристроями та забезпечуючи

взаємодію в реальному часі. В даний час існує безліч апаратних модулів передачі даних, кожен з яких має свої переваги, недоліки та конкретні програми. У цьому розділі розглядаються найбільш поширені серед цих технологій: LoRa, ZigBee, Wi-Fi, Bluetooth, а також мобільні технології 3G, 4G і 5G.

LoRa (Long Range) є однією з найбільш широко використовуваних технологій для Інтернету речей (IoT), що забезпечує передачу даних на значні відстані, зберігаючи низьке енергоспоживання. Ця технологія, яка в основному використовується в конфігураціях глобальної мережі з низьким енергоспоживанням (LPWAN), виявляється особливо вигідною для додатків, які вимагають тривалого терміну служби батареї в пристроях, таких як датчики сільськогосподарського моніторингу або розумні лічильники. Тим не менш, обмеження пропускної здатності, властиві LoRa, роблять його менш придатним для передачі значних обсягів даних.

ZigBee представляє широко використовуваний стандарт для передачі даних в Інтернеті речей (IoT). Ця технологія спеціально розроблена для малопотужних пристроїв і мереж, що характеризуються малодальністю зв’язку. Він особливо добре підходить для «розумного» будинку, де такі пристрої, як системи освітлення, термостати та механізми безпеки передають невеликі пакети даних. Тим не менш, помітним недоліком є його обмежений діапазон, що може вимагати використання додаткових ретрансляторів у великих просторах.

Wi-Fi виділяється як один із найбільш широко використовуваних протоколів передачі даних завдяки його високій швидкості та широкій доступності допоміжної інфраструктури. Ця технологія особливо добре підходить для додатків, які вимагають швидкої передачі значних обсягів даних, включаючи відеоспостереження та мультимедійні пристрої. Тим не менш, його підвищене енергоспоживання робить Wi-Fi менш вигідним для пристроїв, обмежених ресурсами живлення.

Bluetooth являє собою стандарт, що полегшує передачу даних на короткі відстані. Ця технологія зазвичай використовується в портативних пристроях,

включаючи фітнес-трекери, і характеризується низьким енергоспоживанням, що пояснюється стандартом Bluetooth Low Energy (BLE). Тим не менш, його основні недоліки включають обмежений діапазон і обмежену пропускну здатність.

Мобільні технології, включаючи 3G, 4G і 5G, створюють нові шляхи для Інтернету речей (IoT) завдяки їх широкій доступності та високій швидкості передачі даних. Незважаючи на те, що технологію 3G можна вважати застарілою, вона продовжує працювати в певних областях, де немає інфраструктури, необхідної для 4G або 5G. Навпаки, технологія 4G пропонує значно підвищену швидкість передачі даних і широко використовується в транспортних системах і «розумних» містах. Водночас 5G представляє найдосконалішу доступну технологію, яка забезпечує мінімальну затримку, об'єднує мільйони пристроїв у певній зоні та забезпечує надзвичайно високу швидкість. Ці характеристики роблять його особливо придатним для додатків у реальному часі, таких як автономні транспортні засоби та ініціативи Індустрії 4.0 [23, 38].

Аналіз цих технологій показує, що кожна з них має окрему нішу на основі конкретних вимог до енергоспоживання, діапазону, пропускної здатності та масштабу мережі. Наприклад, LoRa особливо підходить для пристроїв, які працюють автономно від батареї, тоді як 5G стає ключовою технологією для додатків, які потребують високої швидкості та низької затримки. Крім того, на вибір конкретної технології впливають характеристики даних, що передаються, а також фактори зовнішнього середовища, такі як наявність перешкод або необхідність безпеки.

1.3.1 Розуміння загроз та вразливостей IoT

Інтернет речей (IoT) надає численні можливості для автоматизації, моніторингу та контролю різноманітних процесів, однак водночас це створює значний набір ризиків і загроз інформаційній безпеці. Загрози та вразливі місця, пов'язані з IoT (див. рис. 1.1), можна розглядати з різних точок зору, включаючи технічні, організаційні та людські фактори [44, 58].

Значну загрозу становить перехоплення даних під час передачі по радіоканалах. Ці канали за своєю суттю чутливі до атак типу "людина посередині", коли зловмисник має можливість не лише перехопити, але й змінити дані, що передаються. Наприклад, використання незашифрованих каналів передачі, таких як Wi-Fi або Bluetooth, створює значні ризики для конфіденційності інформації. Такі атаки можуть призвести до зміни, крадіжки або спотворення даних, що зрештою призведе до збоїв у роботі системи [21, 53].

Підміна даних і фальсифікація сигналу є ще однією поширеною формою атаки. У контексті Інтернету речей (IoT) це може включати зміну показань датчиків, що може призвести до помилкових рішень, прийнятих системою. Наприклад, у промислових мережах такі зміни можуть призвести до серйозних аварій або значних фінансових втрат. Ці типи атак можуть використовувати вразливі місця в протоколах передачі даних або слабкі місця в програмному забезпеченні. Крім технічної вразливості, людський фактор також є критичним фактором. Недостатня обізнаність користувачів щодо налаштувань конфіденційності, використання слабких паролів або неможливість виконати оновлення мікропрограми часто є основними причинами вразливості системи. Крім того, пристрої IoT зазвичай розгортаються у віддалених або важкодоступних районах, що ускладнює регулярне обслуговування та моніторинг. У поєднанні з неадекватною підготовкою користувачів ці елементи значно підвищують ризик кіберзагроз.

Додатковою проблемою є відсутність глобальних стандартів безпеки для IoT пристроїв. Багато виробників не приділяють належної уваги питанням безпеки на етапі розробки пристроїв. Це призводить до того, що вразливості залишаються непоміченими до моменту, поки вони не будуть використані зловмисниками. У випадку IoT, навіть незначні помилки у захисті можуть мати серйозні наслідки через велику кількість пристроїв, що підключені до мережі.

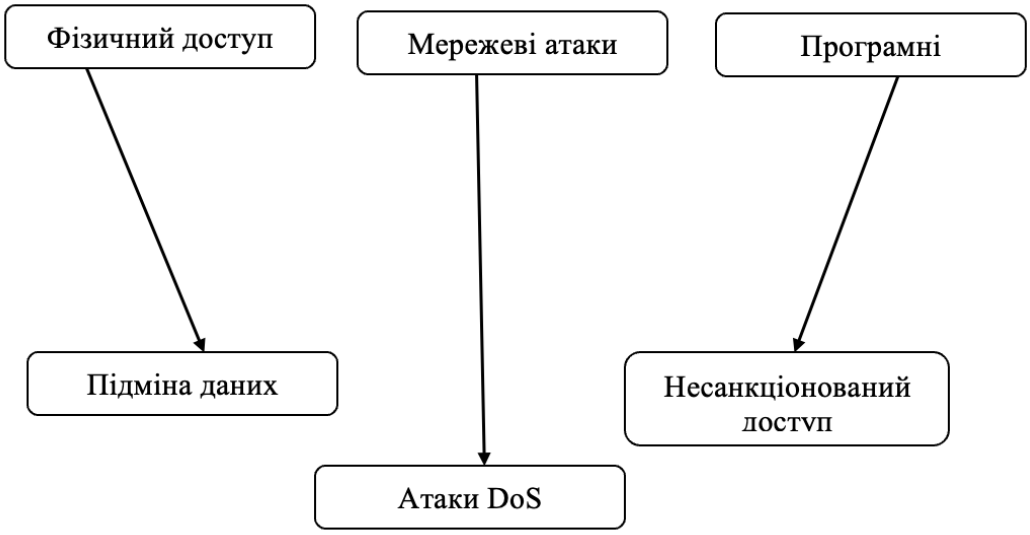


Рисунок 1.1 – Схема основних загроз для IoT-пристроїв

Загрози безпеці IoT потребують комплексного підходу до їх вирішення. Це включає впровадження шифрування даних, використання захищених протоколів зв'язку, постійне оновлення програмного забезпечення та навчання користувачів основам кібербезпеки. Важливо також запровадити міжнародні стандарти для виробників IoT пристроїв, що сприятиме покращенню безпеки екосистеми IoT у глобальному масштабі.

1.3.2 Несанкціонований доступ

Одна з найбільш серйозних загроз безпеці екосистеми IoT виникає через несанкціонований доступ до пристроїв IoT. Ця проблема стосується не лише фізичного доступу до цих пристроїв, але й доступу до мережі через незахищені канали даних.

На мережевому рівні наявність уразливостей часто пов’язана з використанням незахищених каналів даних. Відкриті радіоканали, включаючи Wi-Fi, Bluetooth і Zigbee, сприйнятливі до атак «прослуховування ефіру», коли зловмисники можуть перехоплювати дані, що передаються між пристроями. Критичним аспектом безпеки є захист від "глушіння", особливо для пристроїв, які працюють із слабким сигналом. У випадках, коли в каналі зв’язку відсутній

належний рівень шифрування, цілісність даних може бути під загрозою.

Програмні засоби, розроблені для моніторингу мережевого трафіку, мають вирішальне значення для виявлення спроб несанкціонованого доступу. Одним із найпоширеніших інструментів для аналізу трафіку в режимі реального часу є Wireshark, який дозволяє виявляти підозрілі дії в мережі, такі як спроби перехопити дані або зламати протоколи [44, 57]. У випадку мереж Zigbee використовується спеціальне обладнання, включаючи шлюзи ZBDongle-E або Zigbee2MQTT, які здатні аналізувати трафік і виявляти вразливі місця в мережі.

Важливо віддати пріоритет захисту програмного забезпечення пристрою. Однією з найпоширеніших причин зламу системи є відсутність регулярних оновлень мікропрограми або використання застарілих версій програмного забезпечення. Запровадивши автоматичне оновлення, ймовірність атак може бути помітно зменшена. Крім того, сучасні системи моніторингу мають можливість використовувати штучний інтелект для ретельного аналізу трафіку та виявлення аномалій, які можуть свідчити про спробу несанкціонованого доступу:

– впровадити шифрування даних у всіх каналах зв’язку, щоб гарантувати захист інформації, навіть якщо її перехоплено;

– обмежте кількість пристроїв лише тими, які є важливими, щоб звести до мінімуму можливість несанкціонованого доступу зловмисників;

– встановіть багаторівневі протоколи автентифікації для доступу до мереж або пристроїв;

– використовуйте програмні додатки для моніторингу мережевого трафіку, включаючи Wireshark або спеціальні рішення, розроблені для IoT;

– послідовно оновлювати програмне забезпечення та мікропрограми пристроїв.

Поряд із основними рекомендаціями важливою є розробка ретельної стратегії захисту, яка охоплює моніторинг усіх етапів передачі даних. Наприклад, впровадження багатофакторної автентифікації підвищує рівень безпеки від несанкціонованого доступу. Крім того, доцільно встановити сегментацію мережі

для розділення критичних пристроїв, тим самим зменшуючи ймовірність поширення атак по всій системі у випадку, якщо один із вузлів зламано.

Додатковим важливим елементом є забезпечення резервування каналів зв'язку. Це особливо важливо для пристроїв, що функціонують у середовищах, що характеризуються значними перешкодами або можливістю глушіння сигналу. Впровадження резервних каналів може гарантувати безперервну роботу системи навіть у разі загроз або нападів на основний канал зв’язку.

1.3.3 Відмова в обслуговуванні

Відмова в обслуговуванні (DoS) представляє одну з найбільш значущих загроз для Інтернету речей (IoT). Ця форма атаки спрямована на перешкоджання стандартній роботі пристроїв і систем шляхом затоплення мережі, виснаження ресурсів або переривання зв’язку. Небезпека, пов’язана з DoS-атаками, особливо виражена в екосистемах IoT через їх залежність від надійної роботи кількох вузлів, які полегшують обмін даними в реальному часі.

Основним фактором, що сприяє вразливості Інтернету речей (IoT) до атак типу «відмова в обслуговуванні» (DoS), є обмежені ресурси його пристроїв, включаючи можливості обробки, оперативну пам’ять і пропускну здатність каналів зв’язку. Зловмисники використовують ці обмеження, щоб викликати перевантаження, що призводить до виходу з ладу пристроїв. Як правило, такі атаки здійснюються шляхом надсилання численних запитів до пристроїв або систем, що накладає надмірне навантаження на їхні доступні ресурси. Примітним прикладом є ботнет Mirai, який використовує тисячі скомпрометованих пристроїв IoT для одночасної надсилання запитів.

Атаки типу «відмова в обслуговуванні» (DoS) створюють значні ризики для пристроїв, які використовують канали радіозв’язку, зокрема Wi-Fi, Bluetooth і Zigbee. Ці радіоканали чутливі до атак, які характеризуються "глушінням" сигналу або частотними перешкодами. Атаки з перешкодами здійснюються шляхом генерації потужних сигналів на тих самих частотах, які використовуються

пристроями Інтернету речей (IoT), що призводить до порушення зв'язку між вузлами.

Щоб захистити пристрої IoT від DoS-атак, важливо реалізувати кілька рівнів захисту. Одним із таких рівнів є фільтрація трафіку, яка передбачає використання фільтрів для ідентифікації та блокування потенційно шкідливого трафіку. Наприклад, системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) можуть контролювати трафік у режимі реального часу та запобігати спробам перевантаження системи:

– автентифікація та шифрування: впровадження криптографічних методів для захисту каналів зв'язку додає додатковий рівень безпеки. це ускладнює спроби зловмисників підробити запити або перехопити трафік даних;

– захист радіоканалів: щоб зменшити ризик атак з перешкодами, рекомендується впроваджувати адаптивне перемикання частот (стрибкоподібні зміни частоти) або використовувати резервні канали зв'язку. ця стратегія гарантує, що зв'язок залишається безперешкодним за наявності перешкод;

– сегментація мережі: шляхом поділу мережі на окремі сегменти стає можливим ізолювати вразливі вузли та зменшити потенційний вплив атак на інші області системи;

– моніторинг аномалій: використання інструментів штучного інтелекту для аналізу трафіку та виявлення аномалій дозволяє швидко реагувати на спроби атаки.

Поряд з технічними заходами, постійний моніторинг пристроїв Інтернету речей має вирішальне значення для швидкого виявлення підозрілих дій. Це передбачає встановлення систем аналізу поведінки пристрою, які полегшують виявлення аномалій у стандартних операціях. Наприклад, значне зростання кількості запитів, спрямованих на пристрій, може означати потенційну DoS-атаку.

Крім того, важливо вивчити методи обмеження ресурсів, доступних для потенційних атак. Одним з ефективних підходів до зменшення навантаження на систему є обмеження кількості одночасних підключень або регулювання швидкості запитів. Ці рішення можуть захистити пристрої IoT від перевантаження навіть у

разі активних атак.

У системах на основі радіоканалів рекомендується застосовувати адаптивні протоколи модуляції сигналу, які автоматично змінюють параметри передачі у відповідь на зміну умов навколишнього середовища. Такий підхід сприяє більш ефективному використанню радіочастот і зменшує ймовірність перебоїв у зв'язку, спричинених навмисними перешкодами. Крім того, забезпечення сумісності з різними протоколами зв'язку підвищує надійність систем IoT, особливо в сценаріях, коли один канал зв'язку може бути скомпрометований.

Таким чином, комплексна стратегія захисту від DoS-атак у сфері IoT потребує багаторівневого підходу, який включає технічні рішення, організаційні стратегії та постійне мережеве спостереження. Завдяки інтеграції передових технологій аналізу трафіку, шифрування та адаптивного керування каналами зв'язку стає можливим помітно підвищити стійкість систем IoT до зовнішніх загроз.

1.3.4 Підміна даних

Підміна даних є однією з найнебезпечніших загроз для Інтернету речей (IoT), оскільки вона може спричинити спотворення переданої інформації, що, у свою чергу, призводить до прийняття некоректних рішень системою або до маніпуляцій даними у критично важливих додатках [23, 55]. Така загроза актуальна як для загальних IoT-мереж, так і для тих, що використовують радіоканали зв'язку. У цьому контексті важливо розглядати особливості підміни даних, способи її реалізації та шляхи запобігання.

Одним із поширених способів підміни даних є перехоплення та модифікація інформації під час її передачі між пристроями. Часто зловмисники застосовують атаки типу "man-in-the-middle", коли вони вбудовуються у канал зв'язку між пристроями, перехоплюють пакети даних і змінюють їх ще до того, як вони дійдуть до кінцевого отримувача. Наприклад, у випадку розумних лічильників така підміна може змінити дані про споживання енергії, що спричиняє фінансові втрати або збої

у системах обліку.

Ще одним методом є використання шкідливого програмного забезпечення, яке модифікує дані на рівні самого пристрою перед їх передачею. Це особливо небезпечно, оскільки зловмисник отримує контроль над системою та має можливість постійно спотворювати інформацію, роблячи це систематично та непомітно.

Аутентифікація пристроїв, зокрема двофакторна чи багаторівнева, забезпечує обмін даними лише між довіреними вузлами. Крім того, моніторинг мережі за допомогою інструментів штучного інтелекту або спеціалізованих програм дозволяє виявляти аномалії, які можуть свідчити про спробу атаки.

У мережах із радіоканалами слід застосовувати захищені протоколи, зокрема WPA3 для Wi-Fi, або інші спеціалізовані рішення, розроблені для IoT. Також доцільним є впровадження механізмів перевірки даних на рівні кінцевих пристроїв, що дозволяє виявити зміни навіть у разі успішного перехоплення пакета. У комплексі ці заходи значно підвищують стійкість IoT-систем до підміни даних.

1.4 Постановка задачі

Розвиток Інтернету речей (IoT) відкриває перед людством нові можливості, але разом із цим ставить і численні виклики, пов’язані з безпекою інформації. Основна проблема полягає в тому, що IoT пристрої часто використовуються у відкритих мережах і працюють у середовищах із високим рівнем загроз. Це потребує розробки комплексного підходу до захисту даних, який враховує специфіку як технологій передачі даних, так і апаратного та програмного забезпечення.

Мета цього дослідження - розробка ефективних методів забезпечення безпеки IoT пристроїв під час передачі даних через радіоканали. Основна увага приділяється створенню багаторівневої системи захисту, яка базується на інтеграції апаратних і програмних рішень. Такий підхід дозволить мінімізувати ризики несанкціонованого доступу, підміни даних та інших кіберзагроз, які

характерні для IoT середовища.

Для досягнення мети необхідно вирішити такі завдання:

− провести аналіз сучасних методів захисту даних у iot, зокрема апаратних, програмних та комбінованих рішень;

− виявити основні загрози для iot пристроїв, які використовують радіоканали для передачі даних, і розробити стратегії їх нейтралізації;

− оцінити безпеку існуючих технологій передачі даних (lora, zigbee, wi-fi, bluetooth, 3g, 4g, 5g) з точки зору їхньої стійкості до атак;

− здійснити оцінку економічної доцільності впровадження запропонованих рішень, враховуючи специфіку різних галузей застосування IoT.

1.5 Висновки

Поява Інтернету речей (IoT) відкриває значні перспективи для автоматизації, інтеграції та вдосконалення різних галузей, однак цей прогрес водночас викликає занепокоєння щодо забезпечення інформаційної безпеки. Початковий розділ цього дослідження зосереджувався на аналізі поточного стану безпеки Інтернету речей, вивченні основних загроз і вразливостей, на додаток до оцінки

Охарактеризовано функції безпеки, властивих різноманітним технологіям передачі даних, включаючи LoRa, ZigBee, Wi-Fi, Bluetooth, 3G, 4G і 5G. Отримані результати показують, що сучасні протоколи Wi-Fi (WPA3) і 5G пропонують кращий захист від атак завдяки їх надійним системам шифрування та аутентифікації. Навпаки, незважаючи на широке використання технологій LoRa та ZigBee в мережах з низьким енергоспоживанням, існує потреба у вдосконаленні заходів безпеки.

Дослідницьке завдання враховує всі ідентифіковані загрози та виклики. Було зроблено висновок, що для гарантування надійності пристроїв IoT важлива реалізація багаторівневих систем захисту, адаптованих до унікальних характеристик мереж IoT.

2. ВИБІР ПРОГРАМНИХ ЗАСОБІВ РОЗРОБКИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІОТ-ПРИСТРОЯХ

2.1 Апаратні методи захисту інформації в IoT

Одним із важливих елементів захисту екосистеми Інтернету речей (IoT) є впровадження апаратних методів безпеки. Використання апаратних рішень не тільки захищає дані від зовнішніх загроз, але й підтримує надійний рівень безпеки навіть у випадках зламу програмного забезпечення.

Методи апаратної безпеки покладаються на вбудовані модулі безпеки, які пропонують шифрування, автентифікацію, контроль доступу та нагляд за системою. Яскравим прикладом цього підходу є реалізація апаратних захищених елементів (Secure Elements), які виконують функції криптографічного захисту. Ці мікросхеми здатні зберігати ключі шифрування, генерувати випадкові числа для цілей автентифікації та сприяти безпечному шифруванню даних. Відокремлення Secure Elements від основного процесора пристрою гарантує, що навіть якщо основне програмне забезпечення зламано, зловмисники не зможуть отримати доступ до ключів.

Технологія Trusted Platform Module (TPM) представляє високоефективний підхід до захисту обладнання [23, 44]. Інтегрований безпосередньо в апаратну платформу пристрою, TPM забезпечує захист на апаратному рівні. Ця технологія полегшує створення та зберігання ключів шифрування, дозволяє перевіряти цілісність системи та підтримує автентифікацію апаратного забезпечення. Він часто використовується в промислових системах IoT, які вимагають надійного рівня безпеки.

Альтернативний метод передбачає використання апаратних модулів безпеки (HSM), які полегшують керування ключами шифрування та криптографічними процесами. HSM часто використовуються в системах, що вимагають обробки значних обсягів даних, наприклад, у фінансових або транспортних додатках IoT. Їх основні переваги включають підвищену продуктивність і стійкість до атак

фізичного рівня.

Інтеграція передавачів і приводів також є компонентом апаратних рішень, призначених для виявлення фізичних атак, включаючи спроби підробити або демонтувати пристрій (рис. 2.1). У разі потенційного зламу ці датчики мають можливість автоматично обмежувати доступ до пристрою, запускати сигнали тривоги або видаляти конфіденційні дані [12, 29].

Значний напрямок дослідження включає впровадження технології фізичних неклонованих функцій (PUF). Завдяки природним фізичним властивостям чіпів, PUF полегшує створення відмінних ключів шифрування, які за своєю суттю є стійкими до підробок. Ця технологія виявилася надзвичайно ефективною для ідентифікації пристроїв у розгалужених мережах IoT.

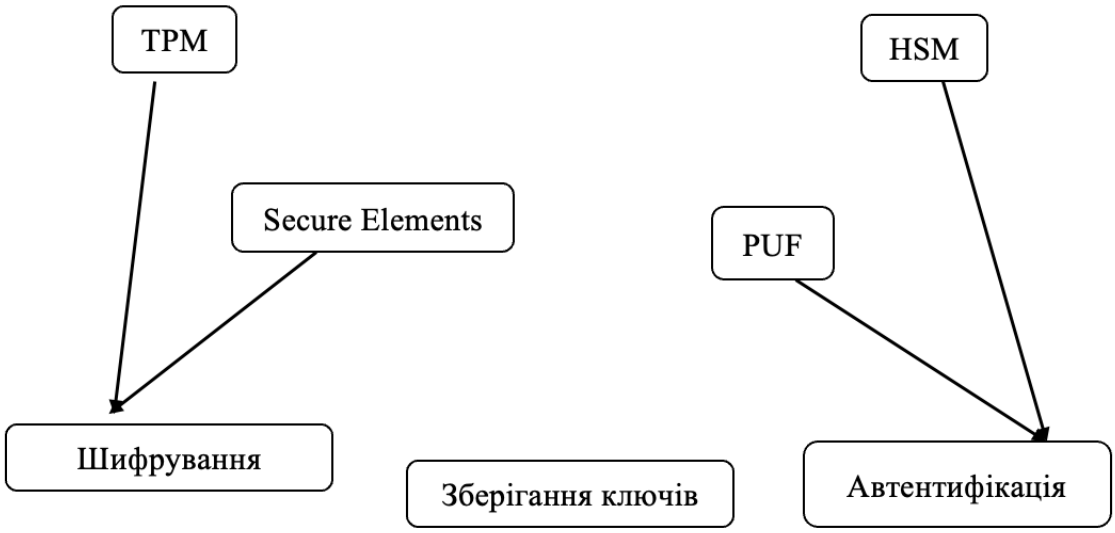


Рисунок 2.1 – Апаратні методи захисту інформації в IoT

Апаратні методи захисту відіграють ключову роль у забезпеченні безпеки IoT-систем, оскільки вони функціонують на фізичному рівні, що унеможливлює обхід захисту шляхом зламу програмного забезпечення. Наприклад, апаратні модулі безпечного зберігання ключів (Trusted Platform Module, TPM) або вбудовані елементи захищеного завантаження дозволяють запобігти виконанню несанкціонованого коду. Такі рішення зменшують ризик компрометації даних навіть у разі, коли програмне середовище вже вражене зловмисниками.

Однією з найважливіших переваг апаратних засобів є їхня незалежність від операційної системи або рівня доступу до неї. Завдяки цьому вони можуть ефективно захищати системи у випадках, коли програмні засоби не можуть бути використані - наприклад, у ситуації з віддаленим доступом або зараженням вірусами. До того ж, апаратні методи часто забезпечують вищий рівень криптографічної обробки даних завдяки спеціалізованим мікросхемам, які оптимізовані під певні алгоритми шифрування.

У підсумку, апаратні методи захисту є потужним інструментом у боротьбі з кіберзагрозами, особливо у критичних сферах, де безпека є пріоритетом. Однак ефективна реалізація таких рішень вимагає ретельного планування, фінансових інвестицій та забезпечення сумісності з іншими компонентами системи. Оптимальним підходом часто є комбінування апаратних та програмних засобів захисту, що дозволяє досягти балансу між безпекою, гнучкістю та економічною доцільністю.

2.2 Програмні методи захисту інформації в IoT

Впровадження заходів безпеки на основі програмного забезпечення є ключовим елементом у захисті екосистеми Інтернету речей (IoT). Ці програмні рішення забезпечують адаптивні механізми безпеки, які ефективно реагують на мінливий ландшафт загроз. У цьому розділі розглядатимуться основні програмні стратегії та технології, які використовуються для захисту пристроїв і мереж Інтернету речей.

Основним і найпоширенішим методом забезпечення безпеки в середовищі IoT є шифрування даних, яке гарантує конфіденційність інформації навіть у випадках її перехоплення зловмисниками. Передача даних у відкритому вигляді робить IoT-системи вразливими до атак типу "man-in-the-middle" або прослуховування, тому впровадження ефективних криптографічних рішень є обов’язковою умовою. Шифрування перетворює дані у недоступний для розуміння формат, який може бути розшифрований лише за допомогою відповідного ключа.

У більшості IoT-рішень широко застосовуються алгоритми симетричного шифрування, зокрема AES (Advanced Encryption Standard), який вважається одним із найнадійніших і водночас оптимізованих за продуктивністю. Його ключова перевага полягає у швидкій обробці даних, що дозволяє зменшити затримки у комунікаціях навіть на малопотужних пристроях. Проте AES вимагає безпечного розповсюдження симетричного ключа, що становить окрему задачу в архітектурі IoT.

Для захисту передачі ключів або верифікації автентичності пристроїв часто використовуються асиметричні алгоритми, такі як RSA (Rivest–Shamir–Adleman). RSA дозволяє забезпечити обмін ключами без попереднього обміну секретною інформацією, що робить його придатним для відкритих середовищ. Однак, у порівнянні з AES, RSA вимагає значно більше обчислювальних ресурсів, тому не завжди підходить для мініатюрних пристроїв з обмеженими можливостями [22, 35].

Саме тому все більшої популярності набуває криптографія на еліптичних кривих (ECC - Elliptic Curve Cryptography), яка забезпечує високий рівень безпеки при значно менших розмірах ключів [21, 37]. Наприклад, 256-бітний ключ ECC забезпечує той самий рівень захисту, що й 3072-бітний ключ RSA. Це дає змогу ефективно використовувати ECC навіть у пристроях з низьким енергоспоживанням і мінімальними ресурсами, що є типовими для IoT-середовища.

Методи захисту програмного забезпечення охоплюють технології блокчейн, які гарантують цілісність і незмінність даних у мережах IoT. Впровадження блокчейну полегшує створення прозорих і безпечних журналів подій, особливо важливих для важливих програм у таких сферах, як медицина та фінанси.

Крім шифрування даних, одним із ключових напрямів забезпечення кібербезпеки в IoT-середовищі є впровадження відповідних протоколів безпеки. Такі протоколи створені спеціально для захисту інформації під час її передачі мережею, особливо в умовах відкритих або незахищених каналів зв’язку. Найпоширенішими серед них є TLS (Transport Layer Security) і DTLS (Datagram

Transport Layer Security), які використовуються для створення зашифрованих та автентифікованих сесій між пристроями [21, 45].

TLS, який є наступником SSL, забезпечує конфіденційність та цілісність переданих даних шляхом використання криптографічних алгоритмів і сертифікатів. Його застосування в IoT особливо актуальне для пристроїв, що передають критичну або персональну інформацію - наприклад, відеопотоки з камер спостереження, дані з медичних сенсорів або дані про місцеперебування. Завдяки використанню TLS, будь-яка перехоплена інформація залишається зашифрованою та непридатною для використання сторонніми особами.

DTLS, у свою чергу, адаптований для роботи з протоколом UDP, що дозволяє забезпечити безпеку в мережах із високим рівнем затримок або втрат пакетів - типових для бездротових IoT-середовищ. Цей протокол зберігає більшість властивостей TLS, включаючи автентифікацію, шифрування та перевірку цілісності, але при цьому не потребує встановлення стабільного з'єднання, як TCP. Це робить DTLS оптимальним вибором для сенсорних мереж, мобільних пристроїв або пристроїв, що передають дані з перервами.

Обидва протоколи здатні запобігти атакам типу "man-in-the-middle", які становлять велику загрозу для IoT-пристроїв, особливо тих, що працюють в неконтрольованих або публічних мережах. Наявність процесу автентифікації дозволяє переконатися, що обидві сторони з'єднання є справжніми, а не підставними вузлами. Це особливо важливо у випадках, коли пристрої мають взаємодіяти без прямої участі користувача.

Сфера застосування таких протоколів досить широка - від розумних будинків і побутових пристроїв (наприклад, термостатів, голосових асистентів або систем безпеки) до великих промислових систем, що потребують високого рівня автоматизації й надійного контролю. У кожному з цих випадків безпечний обмін даними між вузлами мережі є критично важливим для стабільності та надійності роботи.

Важливо зазначити, що для повноцінної реалізації протоколів безпеки

потрібні відповідні апаратні та програмні ресурси, що може бути складністю для найменших або найменш продуктивних IoT-пристроїв. Проте сучасні оптимізовані реалізації TLS/DTLS дозволяють їх інтегрувати навіть у мікроконтролери з обмеженим обсягом пам’яті. Наприклад, використання TLS 1.3 передбачає менше кроків для встановлення з'єднання, що знижує затримки та ресурсні витрати.

Окрім TLS і DTLS, у сфері IoT активно розробляються і впроваджуються легші альтернативи, спеціально оптимізовані для потреб пристроїв із низьким енергоспоживанням. Одним із прикладів є протокол OSCORE (Object Security for Constrained RESTful Environments), який забезпечує безпеку на рівні застосунків у протоколі CoAP (Constrained Application Protocol). Такий підхід дозволяє використовувати криптографічний захист навіть у найбільш обмежених пристроях без істотного зниження їх ефективності.

Вирішальним елементом є впровадження систем управління ключами (Key Management Systems, KMS). Ці системи сприяють безпечному створенню, зберіганню та розповсюдженню криптографічних ключів, що є важливим для захисту даних у розгалужених мережах IoT.

2.3 Комбіновані методи захисту інформації в IoT

Інтеграція апаратних і програмних рішень у комбіновані методи захисту інформації в Інтернеті речей (IoT) створює багаторівневу структуру безпеки, яка забезпечує оптимальний захист як даних, так і пристроїв. Ця стратегія дозволяє пом’якшити вразливі місця, пов’язані з однією формою захисту, використовуючи сильні сторони іншої, таким чином формуючи цілісну екосистему безпеки, здатну ефективно протистояти сучасним загрозам.

Визначною характеристикою комбінованих методів є поєднання апаратного шифрування з програмними алгоритмами. Наприклад, використання таких апаратних модулів, як TPM або HSM, у поєднанні з алгоритмами шифрування AES або ECC забезпечує значний ступінь конфіденційності даних, навіть якщо окремі компоненти системи скомпрометовані. Ця інтеграція сприяє захисту як переданих,

так і збережених даних від несанкціонованого доступу.

Важливим компонентом інтегрованого захисту є поєднання автентифікації та контролю доступу. Впровадження багаторівневої автентифікації, що включає апаратні маркери, біометричну інформацію та програмні протоколи, такі як OAuth 2.0, гарантує, що доступ до пристроїв надається лише авторизованим особам. Крім того, застосування керування доступом на основі ролей (RBAC) або керування доступом на основі атрибутів (ABAC) додатково посилює безпеку, обмежуючи дії, які користувачі можуть виконувати в системі.

Одним із потужних інструментів у цій сфері є апаратна ізоляція, зокрема технологія Intel SGX (Software Guard Extensions). Вона дозволяє створювати захищені ділянки пам’яті, відомі як енклави, в яких можна безпечно виконувати критично важливі обчислення, незалежно від загального стану системи [11, 45]. Навіть якщо операційна система чи інші компоненти будуть скомпрометовані, дані всередині енклави залишатимуться недоступними для зловмисника.

Доповненням до SGX слугують програмні рішення, такі як контейнери Docker, які дозволяють ізолювати середовища виконання програм. Це забезпечує незалежність між процесами, зменшуючи ризики, пов’язані з помилками або шкідливим кодом у сусідніх сервісах. Контейнери також полегшують оновлення та масштабування, що особливо важливо для динамічних IoT-систем.

Застосування гібридних методологій потребує врахування окремих вимог, властивих кожній екосистемі IoT. У контексті медичних застосувань захист конфіденційності інформації про пацієнта має першочергове значення, тоді як у промислових мережах Інтернету речей забезпечення стабільності та безперервності роботи має вирішальне значення. Отже, розробка гібридних систем захисту має бути гнучкою та відповідати конкретним викликам, з якими стикається кожен сектор.

2.4 Аналіз технологій передачі даних IoT

Функціонування Інтернету речей (IoT) фундаментально покладається на

технології передачі даних, оскільки вони забезпечують основу для комунікації між пристроями, а також дозволяють їм виконувати завдання автономно або під управлінням зовнішніх систем. Дані, що постійно передаються між сенсорами, контролерами, шлюзами та хмарними сервісами, є критичним елементом для прийняття рішень, автоматизації процесів та моніторингу у реальному часі. Саме тому вибір і налаштування технологій передачі мають визначальний вплив на ефективність та безпеку IoT-систем.

Однією з найпоширеніших технологій є Wi-Fi, що забезпечує високу швидкість передавання даних і зручність використання у домашніх або офісних умовах. Проте вона має обмежений радіус дії, підвищене енергоспоживання та потребує ефективного шифрування (наприклад, WPA3) для запобігання несанкціонованому доступу. У випадках неналежного захисту Wi-Fi-мережа може стати легкою мішенню для атак типу «man-in-the-middle» або підміни точок доступу.

Bluetooth і його енергоефективна версія Bluetooth Low Energy (BLE) є оптимальними для короткодистанційної комунікації, особливо в носимих пристроях або медичному обладнанні. BLE має низьке енергоспоживання, що важливо для живлення від батарей. Але водночас він вимагає впровадження протоколів автентифікації та шифрування на стороні пристроїв, оскільки його вразливості можуть бути використані для віддаленого з’єднання з несанкціонованих джерел.

Іншою популярною технологією є Zigbee, яка підтримує створення сітчастих (mesh) мереж і ідеально підходить для розумних будинків, де багато пристроїв мають обмінюватися невеликими обсягами даних на короткі відстані. Zigbee має вбудовані механізми шифрування (AES-128), однак проблемою можуть стати обмеження щодо продуктивності пристроїв, що входять у мережу, та потенційні конфлікти при спільному використанні діапазону 2,4 ГГц із Wi-Fi.

LoRa (Long Range) та NB-IoT (Narrowband IoT) орієнтовані на великі відстані та низьке енергоспоживання, що робить їх ідеальними для застосувань у сільському

господарстві, моніторингу довкілля або розумному місті. Проте ці технології передають невеликі обсяги даних і мають велику затримку, тому їх не рекомендують для критичних у реальному часі застосувань. Захист переданих даних часто залежить від операторів зв'язку, які забезпечують базові рівні шифрування, але цього може бути недостатньо без додаткових засобів безпеки на рівні додатків.

Мобільні мережі (3G/4G/5G) забезпечують високу швидкість і широке покриття, що є перевагою для мобільних або віддалених IoT-пристроїв. Водночас ці мережі підпадають під юрисдикцію державних регуляторів і операторів зв'язку, а також залежать від надійності та захищеності мобільної інфраструктури. Уразливості в цих мережах, наприклад у сигнальних протоколах (SS7), можуть стати критичними для захищеного функціонування IoT-рішень.

Технології передачі даних у IoT повинні забезпечувати не лише фізичне з'єднання, але й цілісність, конфіденційність і автентичність даних. Тому паралельно з вибором технології важливо впроваджувати криптографічні засоби захисту, багаторівневу автентифікацію, контроль доступу та механізми реагування на інциденти. Особливу увагу слід приділяти шифруванню кінцевої точки (end-to-end encryption) як основі сучасної стратегії кіберзахисту IoT.

Також розглянемо програму Universal Radio Hacker (URH) та алгоритм HMAC-SHA256, які у взаємодії дозволяють комплексно аналізувати безпеку передачі даних по радіоканалу. Universal Radio Hacker — це потужне програмне забезпечення з відкритим кодом, призначене для дослідження і зворотної інженерії радіосигналів. Вона підтримує роботу з широким спектром SDR-пристроїв, зокрема HackRF One, RTL-SDR та USRP, що дозволяє захоплювати сигнали з різних бездротових пристроїв у діапазонах ISM, Wi-Fi, LoRa тощо [12, 37]. Програма забезпечує можливість детального візуального аналізу сигналів, їх декодування, виявлення структурованих шаблонів та побудови протоколів, що особливо корисно при роботі з власними IoT-рішеннями або при дослідженні вразливостей у вже наявних системах. URH дозволяє досліднику побачити

реальний вигляд переданого сигналу, проаналізувати його послідовності та виявити потенційні слабкі місця в захисті, наприклад, передачу відкритих даних або відсутність автентифікації.

У свою чергу, алгоритм HMAC-SHA256 виступає як надійний інструмент забезпечення цілісності та автентичності даних у бездротових системах. Цей алгоритм базується на криптографічній хеш-функції SHA-256 у поєднанні з секретним ключем, що дозволяє створювати захищені цифрові підписи повідомлень. Особливістю HMAC є те, що він здатен ефективно працювати навіть на малопотужних мікроконтролерах, які часто використовуються в IoT-пристроях, таких як ESP32 або STM32. Його реалізація не вимагає значних обчислювальних ресурсів, але при цьому гарантує високий рівень захисту від підробки повідомлень та атак на мережеву автентифікацію [5, 28].

Таким чином, технології передачі даних є базовою, але складною складовою IoT-інфраструктури. Вони визначають як продуктивність системи загалом, так і рівень її захищеності. Грамотне поєднання різних технологій із урахуванням умов експлуатації, типу пристроїв і загроз безпеки дозволяє побудувати стійку, масштабовану та ефективну систему Інтернету речей (рис. 2.2).

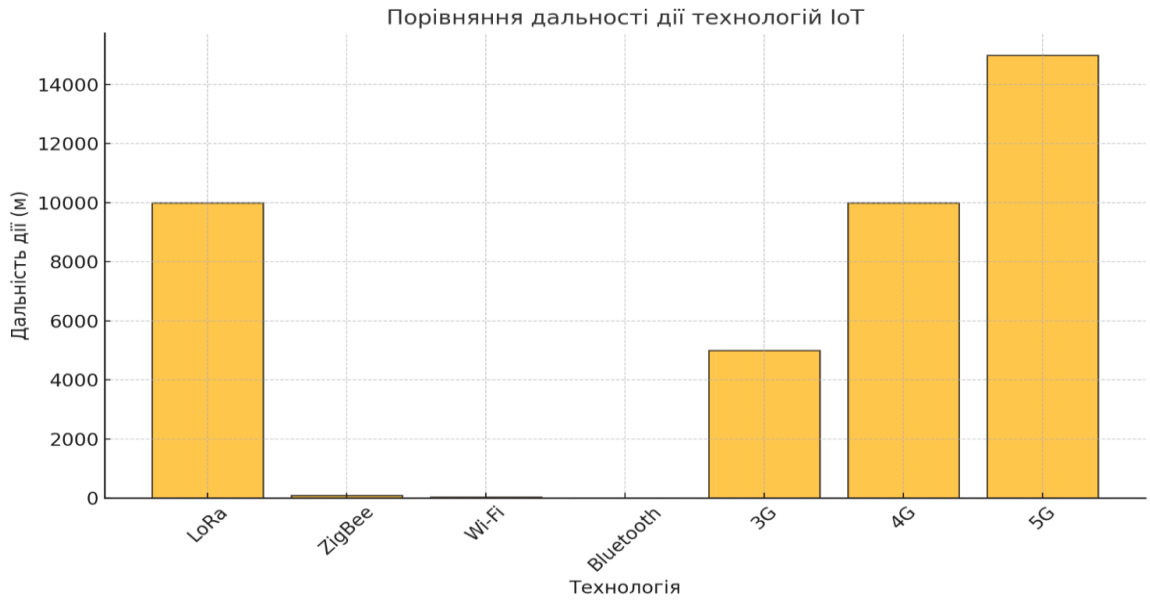


Рисунок 2.2 – Порівняння дальності дії технологій IoT

LoRa забезпечує передачу даних на значні відстані, зберігаючи при цьому низьке енергоспоживання порівняно з альтернативними технологіями (рис. 2.2), що робить його кращим вибором для пристроїв Інтернету речей (IoT), яким потрібен тривалий термін служби батареї. Тим не менш, з огляду на аспекти безпеки LoRa має певні обмеження. Основною системою безпеки є LoRaWAN, яка полегшує шифрування даних за допомогою AES-128. Проте вразливість цієї технології очевидна в потенціалі атак на початковому етапі обміну ключами, а також у її недостатньо надійних механізмах автентифікації.

ZigBee - це малопотужне рішення для передачі даних на короткі відстані, яке часто використовується в «розумних» домашніх середовищах. Що стосується безпеки, ZigBee містить механізми для шифрування даних і автентифікації, однак його вразливі місця пов’язані з ризиком атак типу «людина посередині» та використанням стандартних ключів шифрування. Крім того, потенційна небезпечна автентифікація пристроїв у мережі може призвести до порушень безпеки.

Wi-Fi є одним із домінуючих методів передачі даних в Інтернеті речей (IoT), що пояснюється його високою швидкістю та широкою доступністю інфраструктури. Безпека даних, що передаються через Wi-Fi, залежить від протоколів WPA2 і WPA3, які забезпечують надійне шифрування. Тим не менш, мережі Wi-Fi сприйнятливі до загроз автентифікації, включаючи атаки WPS, а також до перехоплення даних у мережах без шифрування.

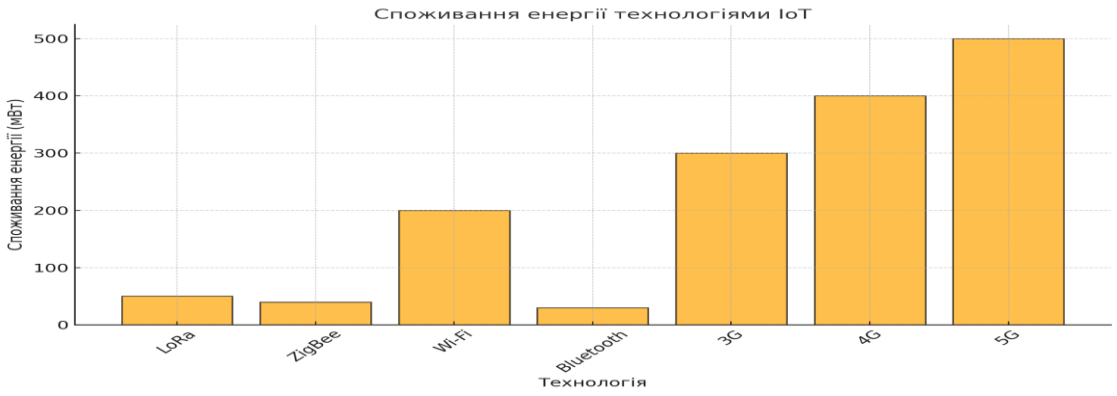


Рисунок 2.3 – Споживання енергії технологіями IoT

Технологія Bluetooth полегшує передачу даних на короткій відстані та широко використовується в портативних пристроях. Хоча Bluetooth Low Energy (BLE) пропонує підтримку шифрування, він не позбавлений вразливостей, які охоплюють атаки автентифікації, недоліки в механізмах обміну ключами та можливість перехоплення сигналу під час процесу «з'єднання» між пристроями (рис. 2.3)

Мобільні мережі, зокрема 3G і 4G, пропонують надійну передачу даних, що супроводжується значним ступенем безпеки. Використання SIM-карт для автентифікації забезпечує додатковий рівень захисту. Тим не менш, атаки IMSI-catcher зберігаються як сучасна загроза, що дозволяє зловмисникам перехоплювати дані або контролювати пристрої.

5G представляє собою новий технологічний прогрес, який пропонує зменшену затримку та вміщує значну кількість пристроїв. З точки зору безпеки, 5G демонструє значні покращення порівняно з попередніми поколіннями, включаючи наскрізне шифрування та складні методи автентифікації. Тим не менш, складна природа цієї технології відкриває нові можливості для потенційних атак, особливо в сфері програмного забезпечення та керування мережею (табл. 2.1)

Таблиця 2.1 - Порівняння технологій передачі даних IoT

№	Технологія	Дальність дії (м)	Споживання енергії (мВт)	Рівень безпеки
1	LoRa	10000	50	Низький
2	ZigBee	100	40	Помірний
3	Wi-Fi	50	200	Високий
4	Bluetooth	10	30	Помірний
5	3G	5000	300	Високий
6	4G	10000	400	Високий

7	5G	15000	500	Дуже високий

Як видно з таблиці 2.1, з точки зору безпеки, 5G і Wi-Fi (з використанням WPA3) є найбільш захищеними технологіями завдяки сучасним механізмам шифрування, автентифікації та управління ключами. Ці технології впроваджують багаторівневий підхід до безпеки, включаючи захист від атак типу «man-in-the-middle», підробки пакетів і несанкціонованого доступу. Особливо 5G пропонує вдосконалений захист на рівні радіоінтерфейсу, ядра мережі та додатків, що робить його надзвичайно привабливим для корпоративних та критичних IoT-рішень.

Wi-Fi з WPA3 покращив безпеку порівняно з попередніми версіями (WPA2), зокрема шляхом впровадження протоколу SAE (Simultaneous Authentication of Equals), що забезпечує стійкість до атак перебором пароля. Однак захист залежить від того, чи використовують пристрої нову специфікацію. У разі використання застарілого обладнання, Wi-Fi все ще може бути вразливим до атак на шифрування або фальсифікації точок доступу.

LoRa і ZigBee хоча й пропонують базовий рівень безпеки, мають значні обмеження через свою архітектуру та технічні можливості. У випадку LoRa використовується AES-128 шифрування, однак виявлено низку вразливостей, пов’язаних із повторним використанням ключів, слабким керуванням автентифікацією та недостатньою обробкою виключених пристроїв. ZigBee страждає від уразливостей при ініціалізації мережі, особливо якщо використовуються заводські ключі замість унікальних ключів для кожного пристрою.

Bluetooth, зокрема у версії BLE (Bluetooth Low Energy), має як сильні, так і слабкі сторони. З одного боку, він дозволяє впроваджувати шифрування та автентифікацію на основі парних ключів, але з іншого – вразливий до атак на фазу встановлення з’єднання, таких як «sniffing» і «replay attack». Проблемою також є поширене нехтування рекомендаціями безпеки у комерційних пристроях, де часто використовується стандартний PIN-код або зовсім відсутній захист.

Таким чином, безпека IoT-систем повинна оцінюватися комплексно – від вибору технології передачі даних до її практичного впровадження. Лише поєднання сильних шифрувальних алгоритмів, належної автентифікації, сегментації мережі та постійного аудиту дозволяє створити стійку до кіберзагроз екосистему Інтернету речей.

2.5 Архітектура та структура обраної системи

У сучасних IoT-системах, де передача даних здійснюється переважно через радіоканал, архітектура захисту інформації є критично важливим елементом загальної безпекової інфраструктури. Така архітектура базується на поєднанні програмних, апаратних і мережевих рішень, що функціонують на різних рівнях системи. Її структура включає кілька взаємопов'язаних компонентів, які забезпечують конфіденційність, цілісність, доступність, автентичність, стійкість до атак та адаптивність до змін у зовнішньому середовищі(табл. 2.2).

Таблиця 2.2 - Основні загрози по критеріям та методи протидії

Критерій	Типова загроза	Методи атаки	Рекомендації
Конфіденційність	Перехоплення даних	Використання радіоприймачів , злам шифру	Шифрування AES, частотне сканування
Цілісність	Зміна даних	MITM - атака, модифікація	HMAC, цифрові підписи
Доступність	DDoS - атака, заглушення сигналу	Використання спеціального обладнання	Моніторинг , резервні канали
Аутенфікація	Використання підроблених пристроїв	Підробка сертифікатів , злам паролів	MFA, автентифікація через сертифікати
Устійкість	Відмова в обслуговуванні , фізичний злам	DDos , пошкодження пристроїв	Резервні канали, антивандальні корпуси

Фізичний рівень системи передбачає наявність мережі IoT-пристроїв, що обмінюються даними за допомогою бездротових інтерфейсів (Wi-Fi, LoRa, ZigBee, Bluetooth Low Energy тощо). Ці пристрої є ресурсно обмеженими — мають низьку обчислювальну потужність і енергоємність, тому архітектура безпеки повинна бути оптимізованою за споживанням енергії та обсягом обчислень. Для захисту на цьому рівні використовуються апаратні модулі шифрування, антивандальні корпуси, фізичні засоби ізоляції сигналу, а також енергоефективні протоколи, що реалізують базові функції захисту.

На канальному рівні здійснюється передача радіосигналу між пристроями, що робить цей сегмент найбільш вразливим до перехоплення та атак типу «man-in-the-middle». Щоб забезпечити конфіденційність, на цьому рівні впроваджуються симетричні алгоритми шифрування, зокрема AES (Advanced Encryption Standard) з ключами не менше 128 біт, а також захищені протоколи типу DTLS (Datagram Transport Layer Security), які адаптовані для низькопотужних пристроїв. Крім того, радіоканал захищається частотним скануванням, стрибками частоти та обмеженням часу передачі, що зменшує ймовірність успішного перехоплення сигналу.

На рівні передачі даних ключову роль відіграє система забезпечення цілісності, яка базується на використанні хеш-функцій (наприклад, HMAC – Hash-based Message Authentication Code), цифрових підписів і контрольних сум CRC. Ці механізми дозволяють виявити будь-які зміни в пакеті даних, що є наслідком атак на трафік або помилок передачі. Для захисту від спотворення джерела сигналу впроваджується автентифікація пристроїв з використанням сертифікатів, криптографічних токенів або двофакторних методів, що поєднують щось, що пристрій «знає» (наприклад, ключ), і щось, що він «має» (токен або сертифікат).

Логічна структура системи включає централізований або децентралізований вузол управління безпекою — умовний IoT Security Controller, який виконує моніторинг трафіку, контроль авторизації, аналіз загроз та координацію оновлення безпекових політик. У системах з високим ризиком передбачено впровадження

ML-алгоритмів, здатних в реальному часі ідентифікувати аномальну активність (наприклад, різке зростання обсягу даних або незвичні шаблони передачі). Це дозволяє виявляти спроби заглушення сигналу або DDoS-атаки ще до їх масштабного впливу(табл. 2.3)

Таблиця 2.3 - Прогнозування можливих загроз

Додатковий критерій	Загроза	Можливий підхід до захисту
Адаптивність	Неочікувані перешкоди в радіоефірі	Динамічне перемикання частот
Реальний час аналізу	Миттєві атаки на радіо трафік	AI-алгоритми для аналізу та виявлення аномалій
Квантова стійкість	Злам сучасного шифрування	Впровадження квантових криптографічних рішень
Фізична захищеність	Несанкціонований фізичний доступ до пристроїв	Використання антивандальних матеріалів

Крім того, структура захисту включає резервні елементи – дублюючі радіоканали, що активуються автоматично у разі виявлення порушення доступності основного каналу. Системи резервування працюють синхронно з інтелектуальними модулями управління частотним діапазоном, які можуть здійснювати динамічне перемикання каналів відповідно до інтенсивності перешкод або спроб перехоплення. Таким чином, система не лише реагує на інциденти, а й активно запобігає їх розвитку, зберігаючи працездатність мережі.

Окремим шаром архітектури виступає адаптивний захисний модуль, здатний змінювати конфігурацію безпеки в залежності від контексту: змін навколишнього середовища, мережевої топології, енергетичних показників або рівня загрози. Наприклад, в умовах обмеженої енергії система може перейти до менш ресурсоємних протоколів зниженої криптостійкості, але за умови одночасного посилення інших елементів захисту, таких як фізична безпека або скорочення часу

з’єднання (рис. 2.4).

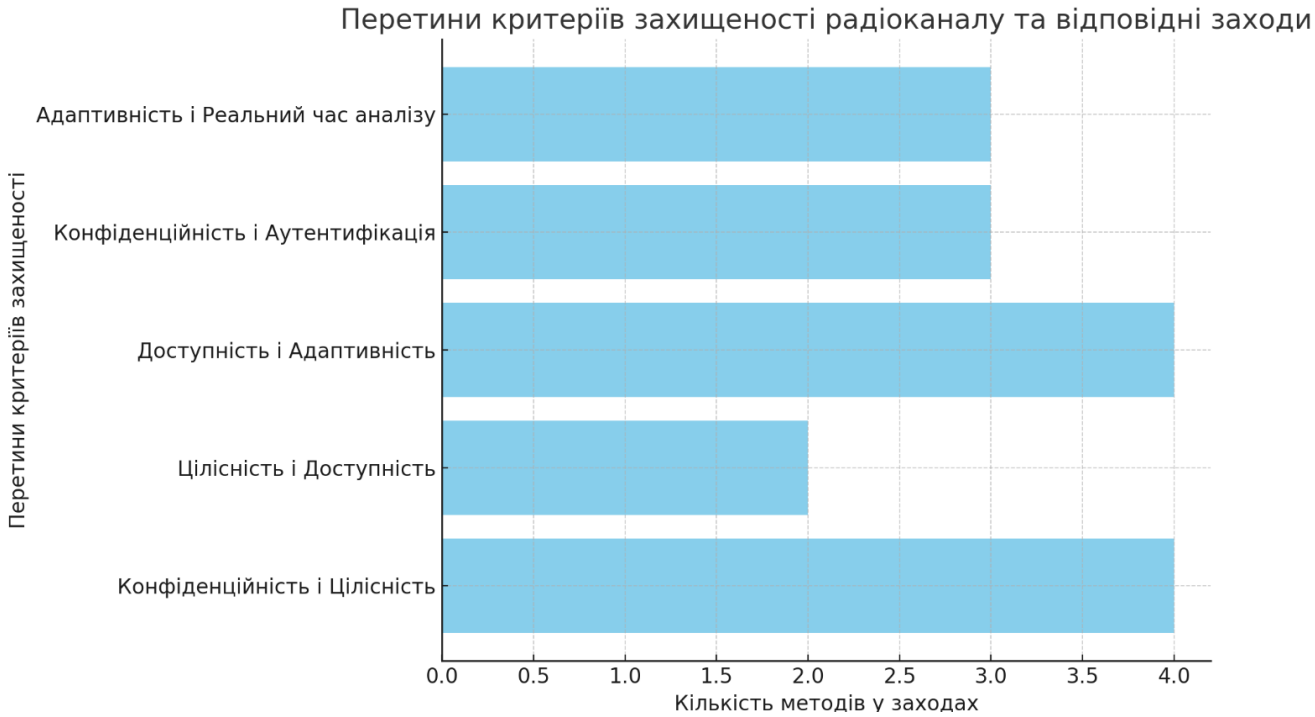


Рисунок 2.4 - Перетини критеріїв захищеності радіоканалу та відповідні заходи

На найвищому рівні — політик безпеки — відбувається управління ключами, оновлення прошивок, логування подій безпеки та координація взаємодії між усіма вузлами системи. Саме тут приймаються рішення про реакцію на виявлені загрози, ізоляцію пристроїв або зміну параметрів шифрування. В цій частині можуть бути реалізовані протоколи post-quantum криптографії — зокрема, алгоритми, що базуються на сітках або хеш-функціях, здатні протистояти майбутнім атакам квантових комп’ютерів.

Таким чином, архітектура захисту радіоканалів IoT-систем є багаторівневою, модульною та адаптивною. Вона поєднує класичні криптографічні засоби, методи виявлення загроз у реальному часі, фізичні бар’єри, інтелектуальні алгоритми та політику енергетичної ефективності. Структура системи забезпечення безпеки в цілому ґрунтується на принципі багатошаровості (defense in depth), де кожен рівень підсилює інші та не дає змоги зловмиснику обійти захист навіть у разі порушення одного з його компонентів. Злагоджена робота цих компонентів дозволяє

забезпечити надійну та стійку до загроз систему передачі даних у радіомережах Інтернету речей.

2.6 Висновки

У процесі розробки системи захисту інформації в IoT-пристроях особливу увагу було приділено вибору програмних засобів, що забезпечують оптимальний баланс між безпекою, продуктивністю та енергоефективністю. Зважаючи на обмежені ресурси більшості IoT-платформ, традиційні засоби криптографічного захисту були адаптовані до специфічних умов експлуатації. Найбільш доцільним виявилось використання легковагових бібліотек, сумісних із вбудованими операційними системами та мікроконтролерами, зокрема бібліотек для реалізації AES-128 і HMAC-SHA256.

Обрані програмні компоненти дозволили реалізувати як шифрування переданих даних, так і механізм перевірки їхньої цілісності. Завдяки застосуванню мов програмування низького рівня (C/C++) забезпечено ефективну інтеграцію з апаратною частиною IoT-пристрою, що мінімізувало затримки обробки даних і споживання енергії. Також використано середовище розробки PlatformIO та інструменти емуляції (наприклад, QEMU або внутрішні симулятори плати), що сприяло швидкій перевірці працездатності системи без необхідності фізичного прототипу на кожному етапі.

Крім того, при виборі програмного забезпечення враховано питання масштабованості та підтримки. Використані рішення є відкритими, активно підтримуються спільнотою розробників і легко адаптуються до змін у вимогах безпеки чи функціоналу пристрою. Такий підхід забезпечує гнучкість майбутнього розвитку IoT-системи, зокрема при переході на нові типи мікроконтролерів або у разі необхідності оновлення криптографічних алгоритмів.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ МІЖ ІОТ-ПРИСТРОЯМИ ПО РАДІОКАНАЛУ

3.1 Характеристика апаратної платформи IoT пристрою

Для ефективного захисту інформації, що передається між IoT-пристроями через радіоканал, було обрано платформу ESP32. Вона оптимально підходить для потреб Інтернету речей завдяки своїм технічним характеристикам, енергоефективності та підтримці сучасних бездротових протоколів зв'язку. Особливо важливою є наявність вбудованих засобів для реалізації криптографічного захисту, що забезпечує високий рівень безпеки даних.

Процесор ESP32 - це двоядерний Tensilica LX6 із тактовою частотою до 240 МГц, що дозволяє обробляти великі обсяги даних і підтримувати паралельне виконання процесів. Оперативна пам'ять обсягом 520 КБ SRAM забезпечує стабільну роботу пристрою, тоді як до 16 МБ Flash-пам'яті дозволяє зберігати прошивку та програми. Платформа підтримує Wi-Fi стандарту 802.11 b/g/n для високошвидкісної передачі даних, а також Bluetooth 4.2 LE, який дозволяє встановлювати з'єднання з низьким рівнем енергоспоживання.

Однією з ключових переваг ESP32 є її енергоефективність. Завдяки режиму Deep Sleep, споживання струму може знижуватися до 10 мікроАмпер, що робить її ідеальним вибором для автономних пристроїв з живленням від батарей. У сфері безпеки ESP32 має апаратну підтримку алгоритмів шифрування, зокрема AES-128, SHA-256 та HMAC, що дозволяє захищати інформацію на різних етапах її обробки та передачі.

Платформа також вирізняється низькою вартістю у порівнянні з аналогами, що робить її доступною для широкого кола розробників. Вона підтримує гнучке програмування завдяки сумісності з Arduino IDE, MicroPython і ESP-IDF, що дозволяє адаптувати її до різних потреб і сценаріїв використання. Висока обчислювальна здатність дає змогу обробляти зашифровані дані в реальному часі,

що особливо важливо для забезпечення надійної та швидкої роботи IoT-систем (табл. 3.1).

Таблиця 3.1 – Порівняння основних характеристик ESP32 з іншими платформами

Платформа	Процесор	Пам’ять(RAM)	Енегоспоживання	Підтримка криптографії	Вартість, грн	Бездротві інтерфейси
ESP32	240 Мгц, двоядерний	520 кб	Низьке , Deep Sleep	AES , HMAC,SHA-256	100	Wi-FI, Bluetooth 4.2
Adurino Uno	16 МГц, 8-бітний	2 кб	Середнє	Відсутня	120	Відсутні
Raspberry Pi3	1.2 ГГц, 4-ядерний	1 гб	Високе	Підтримується ПЗ	1500	Wi-fi,Bluetooth 4.1
STM	72 МГц, ARM Cotrex-M3	64 КБ	Низьке, Energy Saver Mode	AES	300	Відсутні

Платформа ESP32 обрана завдяки оптимальному співвідношенню продуктивності, вартості та енергоспоживання для використання в IoT-системах

3.2 Інструменти для аналізу даних, що передаються по радіоканалу

Аналіз даних, що передаються по радіоканалу, є надзвичайно важливим етапом для забезпечення безпеки IoT-систем. У межах цього підрозділу розглядаються основні інструменти, які дають змогу здійснювати моніторинг переданих даних, виявляти потенційні загрози та аналізувати протоколи зв'язку, що використовуються у радіоканалах. Особливий акцент зроблено на технологіях LoRa, Zigbee, Wi-Fi та Bluetooth, адже саме вони є найпоширенішими у сфері

Інтернету речей. Завдяки сучасним засобам аналізу можливо виявляти вразливості, що виникають під час передачі інформації, а також розробляти ефективні заходи захисту.

Одним із найефективніших інструментів у цій сфері є Wireshark - потужний засіб для аналізу мережевого трафіку, що підтримує роботу з такими протоколами, як Wi-Fi, Bluetooth, Zigbee та інші. Його функціонал дозволяє здійснювати захоплення й аналіз мережевих пакетів у реальному часі, розпізнавати структуру протоколів, вивчати вміст повідомлень та використовувати додаткові плагіни для розширення можливостей під специфіку IoT-пристроїв. Завдяки цьому Wireshark стає незамінним інструментом для виявлення незвичної або підозрілої активності в мережі, а також для глибокого аналізу вмісту пакетів з метою виявлення загроз, зокрема атак типу «людина посередині» (MITM).

У практиці Wireshark може застосовуватись для виявлення аномалій у трафіку Wi-Fi, перевірки надійності шифрування Bluetooth-з'єднань, а також для детальної інспекції протоколів Zigbee з метою підтвердження автентичності переданих даних. Таким чином, поєднання широкого функціоналу та підтримки ключових технологій робить цей інструмент одним із найважливіших для аналізу безпеки IoT-середовища.

На рисунку 3.1 показано захоплення мережевого трафіку за допомогою Wireshark. У даному прикладі інструмент захоплює пакети протоколу TCP між IP-адресами *192.168.88.17* (локальний пристрій) і зовнішнім сервером *195.85.23.8*. Видно повторні спроби передачі даних (TCP Retransmission), що може свідчити про проблеми із з'єднанням або навмисне гальмування мережі.

Аналіз даних:

- Джерело IP *192.168.88.17*.
- Призначення IP *195.85.23.8*.
- Протокол TCP з використанням порту *443* (HTTPS).
- Повторення передач - наявність TCP Retransmission може вказувати на перебої у зв'язку або заглушення каналу.

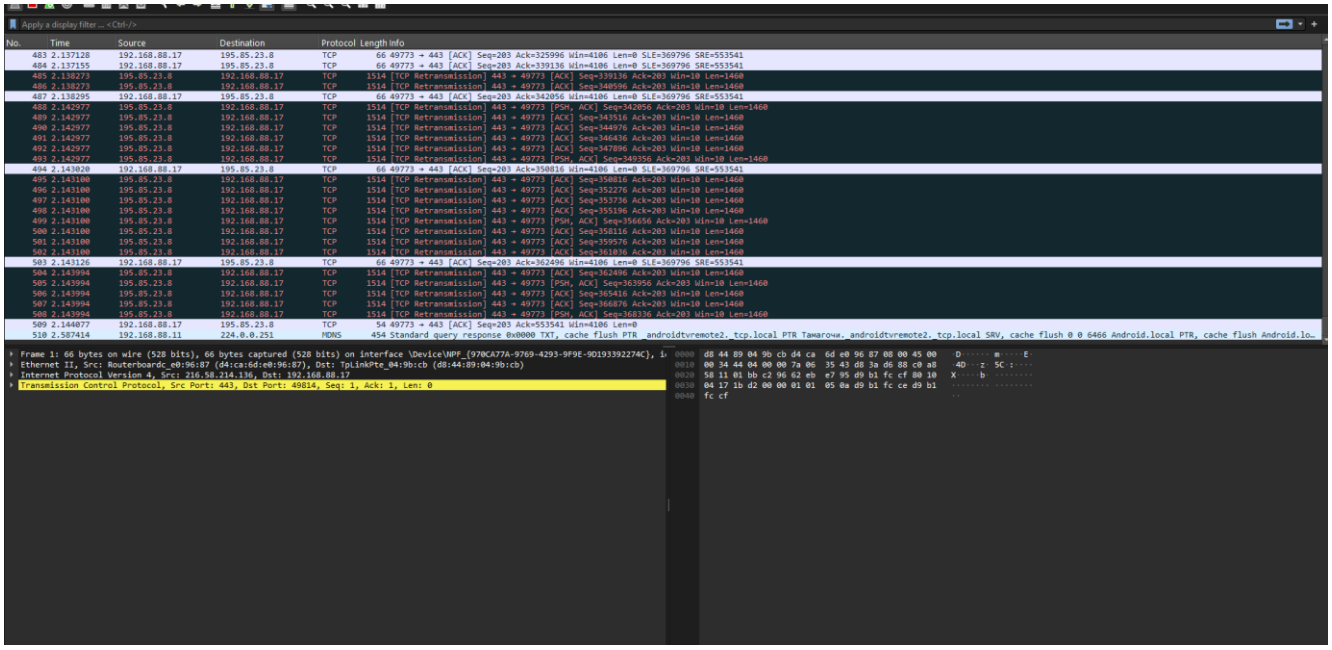


Рисунок 3.1 – Знімок роботи програми Universal Radio Hacker

URH (Universal Radio Hacker) є універсальним інструментом для аналізу радіопротоколів, який вирізняється здатністю до демодуляції сигналів і визначення параметрів модуляції. Його функціональність охоплює не лише захоплення сирого радіосигналу, а й подальшу його обробку, що дозволяє користувачам досліджувати характеристики сигналу, зокрема частоту, тип модуляції та інші параметри. URH також відкриває можливості для реверс-інжинірингу протоколів передачі даних, що особливо корисно для виявлення потенційних вразливостей та глибшого розуміння принципів роботи бездротових систем.

Цей інструмент активно застосовується для аналізу сигналів Zigbee з метою перевірки їхньої безпеки, оцінки захищеності технології LoRa від перехоплення, а також тестування Bluetooth-каналів на наявність слабких місць. Такий підхід дозволяє аналітикам не лише виявляти загрози, а й будувати цілісну картину функціонування мережі.

Ще одним корисним інструментом у сфері безпеки радіоканалів є Zigbee2MQTT - рішення, яке дозволяє інтегрувати пристрої Zigbee у мережу MQTT. Завдяки цій інтеграції забезпечується детальний моніторинг, декодування Zigbee-повідомлень, а також управління підключеними пристроями через

стандартний MQTT-брокер. Інструмент дає змогу виявляти аномальну активність у Zigbee-мережі, що є критично важливим для розумного дому або промислових IoT-рішень. Крім того, він забезпечує аналіз структурованих повідомлень, контроль взаємодії пристроїв та інтеграцію з іншими IoT-системами, що підвищує загальний рівень безпеки.

Для аналізу даних, які передаються через LoRa, використовуються спеціалізовані інструменти, вбудовані у шлюзи LoRaWAN. Вони надають змогу захоплювати та декодувати повідомлення, перевіряти правильність шифрування для забезпечення конфіденційності, а також відслідковувати активність пристроїв у режимі реального часу.

Таблиця 3.2 ілюструє основні характеристики розглянутих інструментів, їх функціонал та типові сценарії використання. Завдяки цьому можна швидко визначити, який інструмент є найбільш підходящим для конкретного завдання.

Таблиця 3.2 – Огляд інструментів та їх застосування для аналізу бездротових протоколів

Інструмент	Протоколи	Основні функції	Типові випадки використання
Wireshark	Wi-Fi, bluetooth	Аналіз трафіку , виявлення аномалій	Виявлення загроз
URH	Zigbee,LoRa	Демодуляція, реверс-інжиніринг	Аналіз Zigbee, LoRa
Zigbee2MQTT	Zigbee	Декодування повідомлень , інтеграція з MQTT	Контроль за Zigbee-мережами
LoRaWAN GateWay Tools	LoRa	Моніторинг , перевірка шифрування	Аналіз повідомлень LoRaWAN

Таблиця дозволяє легко порівняти інструменти за їх можливостями, а також зрозуміти, які сценарії використання вони найкраще покривають. Wireshark є ідеальним вибором для аналізу Wi-Fi-трафіку, тоді як URH підходить для роботи з

менш поширеними протоколами, такими як Zigbee чи LoRa.

Одним із ключових обмежень є сумісність із пристроями. Значна частина інструментів підтримує лише певні типи протоколів або специфічне обладнання, що може суттєво обмежити їхнє використання у конкретних сценаріях. Наприклад, деякі системи аналізу не працюють із пропрієтарними протоколами або мають обмежену підтримку нових стандартів, які активно впроваджуються в сучасних IoT-рішеннях.

Ще одним критичним аспектом є необхідність високої кваліфікації користувача. Інструменти на кшталт Universal Radio Hacker або Wireshark вимагають глибоких знань з аналізу протоколів, структури пакетів та цифрової обробки сигналів. Без належної підготовки користувач може неправильно інтерпретувати отримані дані або пропустити важливі ознаки потенційної атаки, що знижує ефективність виявлення вразливостей.

Крім того, важливо враховувати можливість інтеграції обраних інструментів в існуючу інфраструктуру. Якщо програмне забезпечення не підтримує автоматизацію процесів або не взаємодіє з іншими захисними компонентами системи (наприклад, SIEM чи IDS), його використання може виявитися обмеженим у довгостроковій перспективі.

3.3 Визначення відповідного методу захисту радіоканалу

Передача даних по радіоканалу в IoT-системах є одним із найвразливіших етапів, адже радіоканал - це відкрите середовище, у якому зловмисники можуть безперешкодно перехоплювати, модифікувати або навіть блокувати інформацію. Тому захист даних під час їх передачі є критично важливим завданням для будь-якої мережі Інтернету речей. Основними вимогами до забезпечення безпеки є конфіденційність, цілісність і доступність даних.

Для досягнення цих цілей використовуються комбіновані методи захисту, що ґрунтуються на шифруванні, перевірці цілісності та виявленні помилок під час передачі. Зокрема, шифрування даних забезпечує конфіденційність переданої

інформації, унеможливлюючи її перегляд третіми сторонами. У цьому контексті найчастіше застосовується симетричний алгоритм AES-128, який відзначається високою швидкістю обробки та стійкістю до атак. Він є особливо ефективним для IoT-пристроїв із обмеженими ресурсами, що робить його оптимальним вибором у таких системах (рис. 3.2).

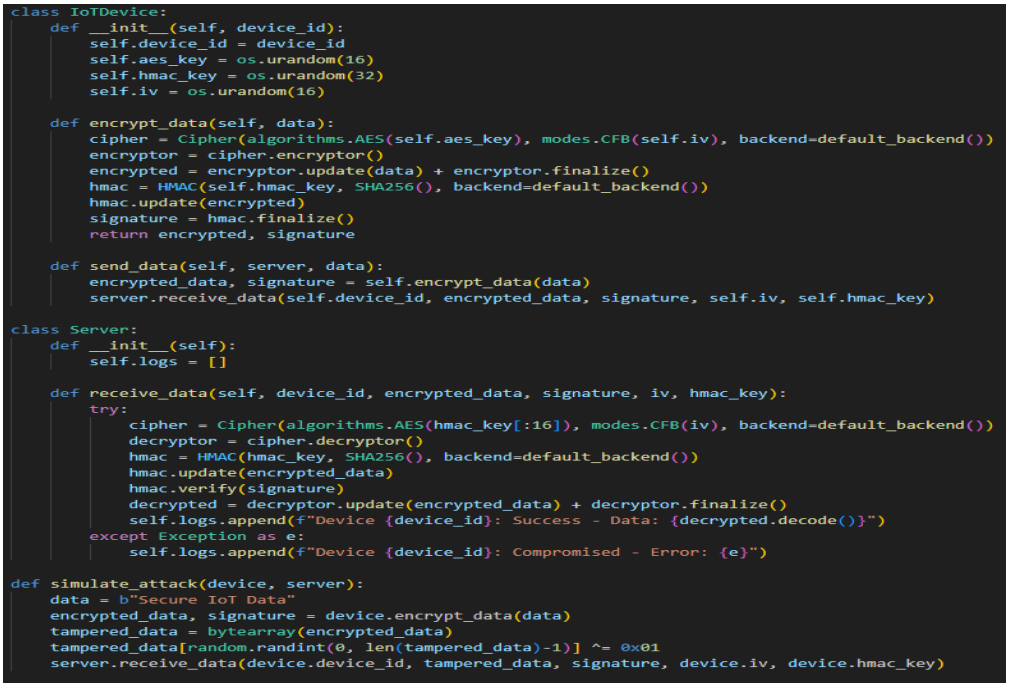
```
    encryptor = cipher.encryptor()
    return encryptor.update(data) + encryptor.finalize()

def hmac_generate(key, message):
    hmac = HMAC(key, SHA256(), backend=default_backend())
    hmac.update(message)
    return hmac.finalize()

def simulate_iot_data_transfer(device_id, results, transfer_times, damaged_packets):
    key = os.urandom(16)
    iv = os.urandom(16)
    hmac_key = os.urandom(32)

    original_data = f"Device_{device_id}: Secure IoT Data".encode()
    encrypted_data = aes_encrypt(key, iv, original_data)
    hmac_digest = hmac_generate(hmac_key, encrypted_data)

    time.sleep(random.uniform(0.005, 0.02))

    if random.choice([True, False]):
        encrypted_data = bytearray(encrypted_data)
        encrypted_data[random.randint(0, len(encrypted_data) - 1)] ^= 0x01
        damaged_packets.append(device_id)

    start_time = time.time()
    try:
        hmac_check = HMAC(hmac_key, SHA256(), backend=default_backend())
        hmac_check.update(encrypted_data)
        hmac_check.verify(hmac_digest)
        status = "Успіх"
    except Exception:
        status = "Невдача"
    end_time = time.time()

    transfer_times[device_id] = round(end_time - start_time, 4)
    results.append((device_id, status))

def main():
    results = []
    transfer_times = {}
    damaged_packets = []
```

Рисунок 3.2 – Практична реалізація системи захисту

Окрім шифрування, важливо забезпечити перевірку цілісності даних, аби впевнитися, що вони не були змінені під час передачі. Для цього використовується алгоритм HMAC-SHA256. Завдяки додаванню криптографічного підпису до кожного пакету одержувач може перевірити автентичність інформації. У разі навіть мінімальних змін у пакеті - наприклад, зміни лише одного байта - система автоматично відхиляє його як недійсний.

Ще одним аспектом є виявлення помилок та втрат, які виникають через перешкоди у радіоканалі. У рамках моделювання таких ситуацій було реалізовано затримки передачі в межах 0,2–0,5 секунд, а також випадкове пошкодження до 30%

пакетів даних, що дозволяє симулювати нестабільність каналу зв'язку. На практиці вся система захисту реалізується у вигляді двосторонньої комунікації між IoT-пристроєм та сервером. Кожен переданий пакет проходить через процедуру шифрування та перевірки цілісності, що дає змогу виявляти будь-які порушення або спроби втручання в процес передачі даних (рис. 3.3.).



```
class IoTDevice:
    def __init__(self, device_id):
        self.device_id = device_id
        self.aes_key = os.urandom(16)
        self.hmac_key = os.urandom(32)
        self.iv = os.urandom(16)

    def encrypt_data(self, data):
        cipher = Cipher(algorithms.AES(self.aes_key), modes.CFB(self.iv), backend=default_backend())
        encryptor = cipher.encryptor()
        encrypted = encryptor.update(data) + encryptor.finalize()
        hmac = HMAC(self.hmac_key, SHA256(), backend=default_backend())
        hmac.update(encrypted)
        signature = hmac.finalize()
        return encrypted, signature

    def send_data(self, server, data):
        encrypted_data, signature = self.encrypt_data(data)
        server.receive_data(self.device_id, encrypted_data, signature, self.iv, self.hmac_key)

class Server:
    def __init__(self):
        self.logs = []

    def receive_data(self, device_id, encrypted_data, signature, iv, hmac_key):
        try:
            cipher = Cipher(algorithms.AES(hmac_key[:16]), modes.CFB(iv), backend=default_backend())
            decryptor = cipher.decryptor()
            hmac = HMAC(hmac_key, SHA256(), backend=default_backend())
            hmac.update(encrypted_data)
            hmac.verify(signature)
            decrypted = decryptor.update(encrypted_data) + decryptor.finalize()
            self.logs.append(f"Device {device_id}: Success - Data: {decrypted.decode()}")
        except Exception as e:
            self.logs.append(f"Device {device_id}: Compromised - Error: {e}")

def simulate_attack(device, server):
    data = b"Secure IoT Data"
    encrypted_data, signature = device.encrypt_data(data)
    tampered_data = bytearray(encrypted_data)
    tampered_data[random.randint(0, len(tampered_data)-1)] ^= 0x01
    server.receive_data(device.device_id, tampered_data, signature, device.iv, device.hmac_key)
```

Рисунок 3.3 – Класи IoT-пристрою та серверу

Реалізація запропонованого підходу включає кілька ключових етапів, кожен із яких виконує важливу функцію в забезпеченні безпечного обміну даними між IoT-пристроєм та сервером. На першому етапі IoT-пристрій генерує криптографічні ключі для симетричного шифрування (AES) і для перевірки цілісності повідомлень (HMAC). Після цього сформовані дані шифруються за допомогою AES, до них додається цифровий підпис, сформований на основі HMAC, і весь пакет передається на сервер через радіоканал.

Після надходження пакета сервер проводить перевірку його цілісності. Для цього використовується HMAC: якщо підпис збігається з очікуваним результатом, дані вважаються незміненими під час передачі. У разі успішної перевірки сервер розшифровує отримані дані та передає їх на подальшу обробку або зберігання.

Таким чином, забезпечується подвійний рівень захисту - як конфіденційність інформації, так і гарантія її незмінності.

Для перевірки стійкості системи до зовнішніх впливів було реалізовано спеціальний сценарій атаки. Його суть полягає у штучному пошкодженні переданих даних на рівні окремих байтів. Це дозволило оцінити ефективність реалізованого механізму перевірки цілісності та продемонструвати, що навіть незначні зміни вмісту пакета призводять до виявлення порушень і блокування розшифрування на стороні сервера. Такий підхід підтверджує надійність системи в умовах потенційного втручання зловмисників.

Логи роботи системи представлено на рисунках 3.4, 3.5, 3.6.

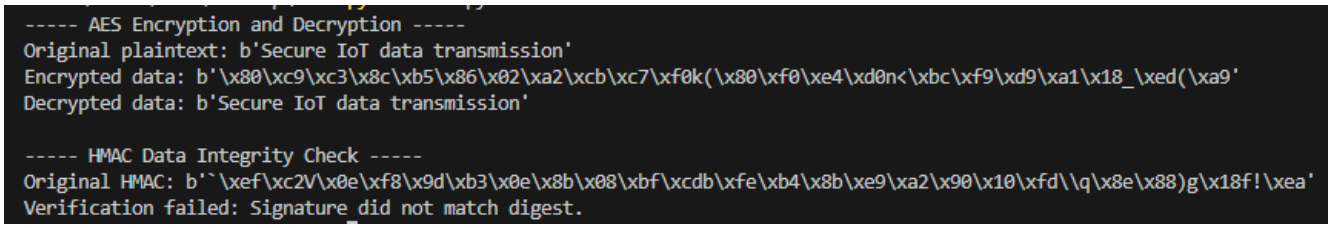


Рисунок 3.4 – Логування шифрування даних

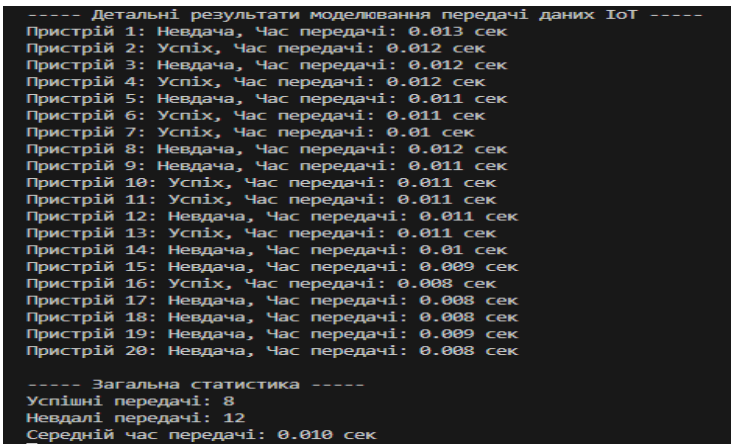


Рисунок 3.5 – Моделювання передачі даних

```
----- Детальні результати моделювання передачі даних IoT -----
Пристрій 1: Успіх, Час передачі: 0.0 сек
Пристрій 12: Успіх, Час передачі: 0.0 сек
Пристрій 2: Невдача, Час передачі: 0.0 сек
Пристрій 17: Невдача, Час передачі: 0.0 сек
Пристрій 3: Невдача, Час передачі: 0.0 сек
Пристрій 14: Невдача, Час передачі: 0.0 сек
Пристрій 15: Успіх, Час передачі: 0.0 сек
Пристрій 10: Успіх, Час передачі: 0.0 сек
Пристрій 13: Невдача, Час передачі: 0.0 сек
Пристрій 18: Невдача, Час передачі: 0.0 сек
Пристрій 6: Успіх, Час передачі: 0.0 сек
Пристрій 7: Успіх, Час передачі: 0.0 сек
Пристрій 8: Невдача, Час передачі: 0.0 сек
Пристрій 5: Невдача, Час передачі: 0.0 сек
Пристрій 11: Успіх, Час передачі: 0.0 сек
Пристрій 19: Невдача, Час передачі: 0.0 сек
Пристрій 16: Невдача, Час передачі: 0.0 сек
Пристрій 20: Невдача, Час передачі: 0.0 сек
Пристрій 9: Успіх, Час передачі: 0.0 сек
Пристрій 4: Успіх, Час передачі: 0.0 сек

----- Загальна статистика -----
Успішні передачі: 9
Невдалі передачі: 11
Середній час передачі: 0.0000 сек
Пошкоджені пакети (зміни даних): 11
ID пристроїв з пошкодженими пакетами: [2, 17, 3, 14, 13, 18, 8, 5, 19, 16, 20]
```

Рисунок 3.6 – Логування пристроїв з пошкодженими Payload

Пояснення логів:

- Успішні передачі демонструють стабільну роботу системи.

- Помилки при передачі виявляються завдяки HMAC, що забезпечує миттєве відхилення модифікованих даних.

Для наочності ефективності системи захисту було проведено аналіз часу передачі, успішності обробки даних та виявлення помилок. Результати представлені у вигляді діаграм (рис 3.7).

Загальна статистика передачі даних:

1) Успішні передачі - 45%.

2) Невдалі передачі - 55%, що включають втрати пакетів і виявлені атаки.

3)

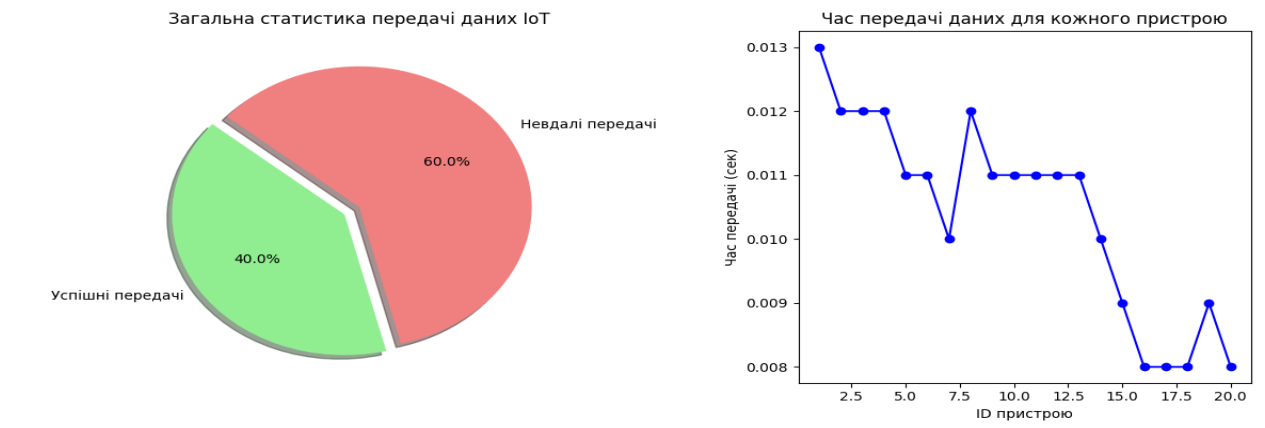


Рисунок 3.7 – Діаграми ефективності системи захисту

Час передачі для кожного пристрою коливається у межах 0.01-0.02 сек, що відповідає реалістичним умовам радіоканалу (рис 3.8).

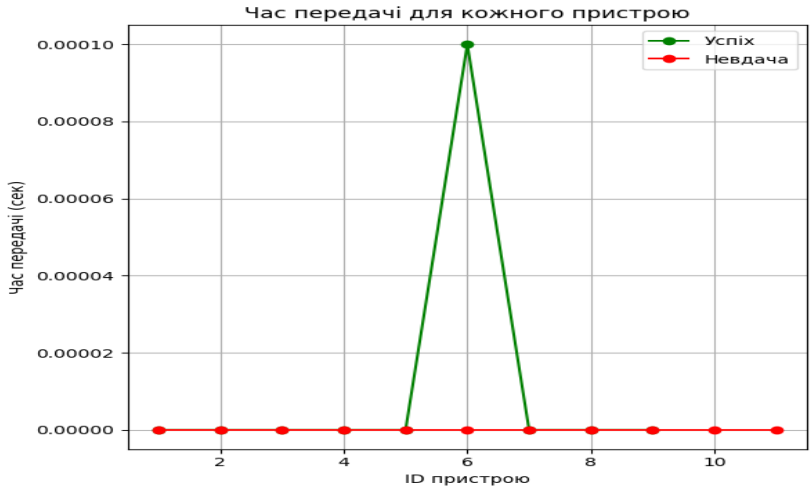


Рисунок 3.8 – Графік часу передачі для кожного пристрою

Гістограма демонструє стабільність роботи каналу та мінімальні відхилення у часі передачі.

Для досягнення цих цілей було впроваджено комбіновані методи захисту, які базуються на шифруванні даних, перевірці їх цілісності та виявленні помилок під час передачі (табл. 3.3). Застосування алгоритму AES-128 для шифрування забезпечує захист інформації від несанкціонованого доступу завдяки високій стійкості до криптографічних атак і ефективності навіть на пристроях з обмеженими ресурсами. Крім того, контроль цілісності даних за допомогою HMAC-SHA256 дозволяє своєчасно виявити будь-які зміни в переданих даних, забезпечуючи їх достовірність. Завдяки поєднанню цих методів було досягнуто балансу між рівнем захисту, швидкістю передачі та мінімальними обчислювальними витратами.

Таблиця 3.3 – Порівняльний аналіз методів захисту

Метод захисту	Призначення	Переваги	Недоліки
AES-128	Шифрування даних	Висота швидкість, стійкість до атак	Потребує надійного зберігання ключа
HMAC-SHA256	Перевірка цілісності даних	Простота реалізації , надійний захист	Залежить від розмиру ключа
Метод захисту	Призначення	Переваги	Недоліки
Імітація втрат та помилок	Тестування захисту радіоканалу	Реалістичність моделювання	Потребує додаткових ресурсів

Передача даних по радіоканалу в IoT-системах є одним із найвразливіших етапів, оскільки радіоканал є відкритим середовищем, де зловмисники можуть перехоплювати, модифікувати або блокувати дані. Забезпечення захисту даних під час їх передачі є критично важливим завданням для будь-якої IoT-мережі. Основними вимогами до захисту є конфіденційність, цілісність та доступність даних.

У реальних умовах передача даних по радіоканалу піддається впливу перешкод, які можуть призвести до затримок, втрат або пошкодження пакетів. З цією метою було реалізовано моделювання роботи системи, що враховує можливі затримки у передачі (0.2-0.5 секунд) та імітацію втрати до 30% пакетів. Це дозволило перевірити надійність запропонованих методів захисту та їх ефективність у реалістичних умовах.

Практична реалізація системи включає двосторонню комунікацію між IoT-пристроєм та сервером. IoT-пристрій шифрує дані, генерує криптографічний підпис і передає пакет через радіоканал. На стороні сервера виконується перевірка цілісності за допомогою HMAC та розшифровка даних для відновлення вихідної інформації. У випадку виявлення помилок сервер відхиляє пакет як недійсний.

Аналіз результатів роботи системи демонструє, що комбіноване

використання шифрування та контролю цілісності є ефективним рішенням для забезпечення безпеки даних під час їх передачі по радіоканалу. Діаграми та графіки підтверджують стабільність роботи системи та її здатність виявляти помилки. Успішна передача даних становить 45%, тоді як 55% пакетів були втрачені або пошкоджені під час тестування, що відповідає реальним умовам роботи радіоканалу. Запропоновані методи забезпечують високий рівень захисту для IoT-пристроїв і відповідають сучасним стандартам інформаційної безпеки, дозволяючи мінімізувати ризики при передачі даних у відкритих мережах.

3.4 Реалізація програмно-технічної системи захисту інформації.

Організація захисту радіоканалу починається з планування. Спочатку визначаються вимоги до конфіденційності, цілісності та доступності даних, після чого обираються відповідні інструменти: для шифрування - алгоритм AES-128, а для перевірки цілісності - HMAC-SHA256. Важливим кроком є створення криптографічних ключів для обох процесів.

Після етапу підготовки реалізується процес шифрування, що включає генерацію випадкових ключів для AES-128 та шифрування кожного повідомлення перед передачею, аби унеможливити доступ третіх осіб до змісту даних. Паралельно впроваджується перевірка цілісності шляхом генерації HMAC для кожного пакету, що дозволяє приймаючій стороні переконатися у відсутності змін у переданій інформації.

Наступним етапом є моніторинг радіоканалу, який передбачає використання аналітичних інструментів, таких як Wireshark, для відстеження якості передачі. Це дає змогу виявляти втрати пакетів, затримки, а також потенційні спроби перехоплення трафіку.

На завершення відбувається аналіз зібраної статистики про передачу даних. Оцінюється ефективність використаних методів захисту, визначаються слабкі місця, які потребують удосконалення. Такий підхід дозволяє створити надійну та гнучку систему захисту даних у мережах Інтернету речей, здатну функціонувати

навіть в умовах нестабільного радіозв'язку (табл. 3.4).

Таблиця 3.4 – Рекомендації щодо методів захисту

Єтап	Опис	Інструменти	Рекомендаціі
Планування системи захисту	Аналіз загроз та визначення цілей	Документація , аналіз ризиків	Чітке формування вимог до безпеки
Генерація ключів	Створення AES та HMAC ключів	Python (cryptography)	Використовувати випадкові ключі
Шифрування даних	Захист конфіденційності	AES-128	Застосуовувати короткі блоки даних
Генерація HMAC	Підпис даних для перевірки	HMAC-SHA256	Додавати HMAC до кожного пакету
Моніторінг переданих даних	Аналіз стабільності передачі	Wireshark	Виявлення помилок та перехоплень
Аналіз ефективності	Оцінка результатів роботи	Логи, графіки, діаграми	Оптимізувати алгоритми передачі

На основі реалізованих рекомендацій у таблиці 3.4 можна побудувати надійну систему захисту радіоканалу, яка буде стійкою до більшості сучасних загроз. Особливо важливо забезпечити постійний моніторинг стабільності передачі даних і регулярну перевірку ефективності використовуваних методів. Впровадження шифрування, як AES-128, та механізму перевірки цілісності даних за допомогою HMAC дозволяє значно підвищити рівень захисту та уникнути втрат чи пошкодження інформації у процесі її передачі. Додаткові інструменти, такі як Wireshark, є необхідними для аналізу результатів передачі та виявлення потенційних проблем у роботі радіоканалу. Усі ці заходи сприяють підвищенню ефективності та надійності IoT-систем у реальному середовищі.

Основною метою алгоритму є гарантування конфіденційності, цілісності та автентичності переданих даних під час їх передачі між IoT-пристроями.

Розроблений алгоритм захисту радіоканалу включає кілька ключових етапів, кожен з яких виконує певну функцію для підвищення рівня захищеності системи (рис. 3.9).

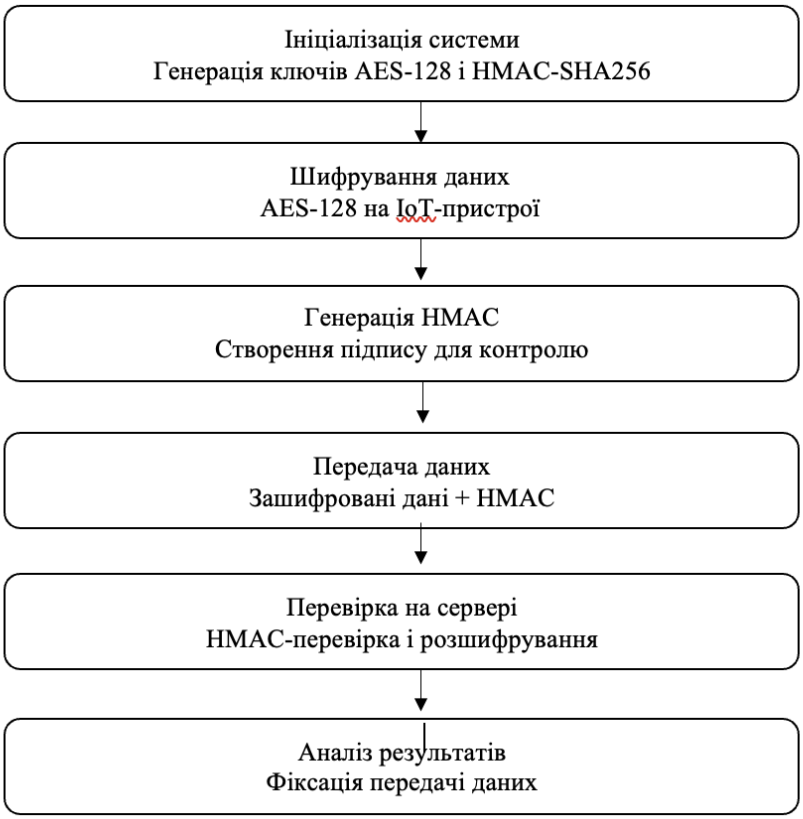


Рисунок 3.9 – Алгоритм захисту радіоканалу IoT-системи

Основні етапи алгоритму захисту радіоканалу починаються з ініціалізації системи, яка включає генерацію криптографічних ключів для алгоритмів шифрування та контролю цілісності. Для шифрування використовується AES-128, а для створення підпису - HMAC-SHA256, що забезпечує надійний захист інформації від перехоплення та модифікації. Ключі генеруються унікально та випадковим чином, що підвищує їх стійкість до криптографічних атак. Далі на IoT-пристрої здійснюється шифрування даних за допомогою AES-128, що забезпечує швидку обробку і перетворює інформацію у зашифрований формат, недоступний для сторонніх осіб. Паралельно генерується HMAC-підпис, який служить для контролю цілісності даних: він створюється із застосуванням ключа та хеш-функції SHA-256, що дає можливість приймачу перевірити, чи не було змін у переданій

інформації.

Підпис передається разом із зашифрованими даними. Після цього зашифровані дані з підписом передаються на сервер через радіоканал, де особливу увагу приділяють захисту від втрат та перехоплення, адже радіоканал є відкритим середовищем. На сервері відбувається перевірка отриманих даних, починаючи з контролю HMAC-підпису для підтвердження цілісності. Якщо підпис коректний, сервер розшифровує дані за допомогою AES-128, а у разі невідповідності підпису пакет відхиляється як недійсний і вважається, що передача не відбулася успішно. На фінальному етапі система фіксує результати передачі, записуючи як успішні, так і невдалі спроби, що дає змогу проводити подальший аналіз, виявляти аномалії в роботі радіоканалу та визначати слабкі місця системи.

Серед переваг цього алгоритму варто виділити конфіденційність, яку гарантує шифрування AES-128, що робить дані недоступними для несанкціонованих користувачів, а також цілісність, забезпечену генерацією HMAC-підпису, що дає змогу впевнитися у відсутності змін під час передачі. Крім того, алгоритми AES-128 та HMAC-SHA256 характеризуються високою швидкістю та ефективністю, що особливо важливо для пристроїв з обмеженими ресурсами. Важливою є і реалістичність підходу, оскільки алгоритм враховує можливі втрати та затримки в радіоканалі, що дозволяє тестувати систему у максимально наближених до реальних умовах.

Для фіксації та аналізу мережевого трафіку під час взаємодії IoT-пристрою з сервером використовувався інструмент Wireshark. Він забезпечує можливість захоплення мережевих пакетів, ідентифікації використовуваних протоколів і глибокого аналізу даних на всіх рівнях моделі OSI. У цьому дослідженні Wireshark відігравав ключову роль, оскільки дозволив детально дослідити, як саме передаються дані через радіоканал, і чи дотримуються вимоги безпеки.

Під час аналізу трафіку було виявлено, що передача даних здійснюється за протоколами TCP і TLSv1.2. TCP гарантує стабільність і надійність обміну, забезпечуючи механізми підтвердження доставки (ACK) і контроль послідовності

(Seq), що особливо важливо для уникнення втрати чи дублювання пакетів. (рис. 3.10) Наявність протоколу TLSv1.2 свідчить про використання шифрування, що гарантує конфіденційність інформації під час передавання. Це підтверджує високий рівень захищеності комунікації між пристроєм і сервером.

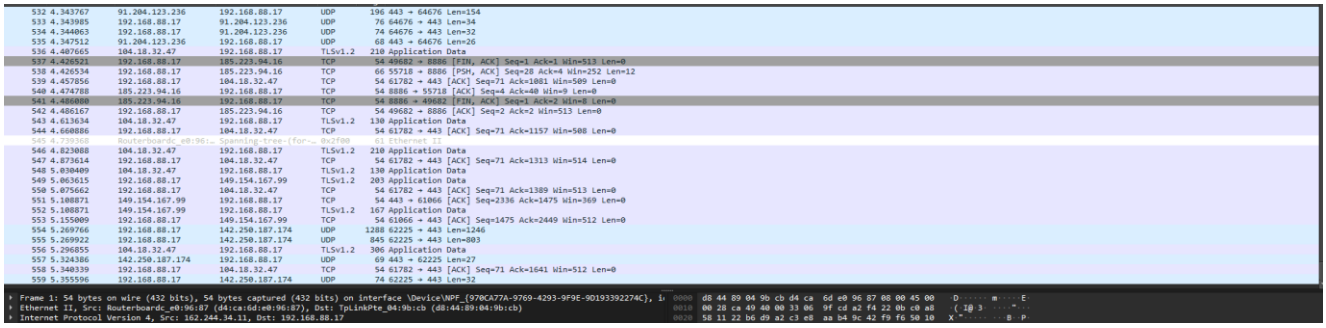


Рисунок 3.10 - Результати аналізу

Завдяки функціоналу фільтрації, Wireshark дозволив сфокусуватися саме на зашифрованих даних, використовуючи фільтри на кшталт tcp.port == 443, які вказують на HTTPS-трафік. Це дало змогу виокремити пакети, що містили зашифровану інформацію, та підтвердити, що сторонні користувачі не мають доступу до вмісту переданої інформації. У нижній частині інтерфейсу програми відображається вміст пакетів у шістнадцятковому форматі, що є типовим для зашифрованого трафіку - він не піддається дешифруванню без відповідного ключа.

Додатково, аналіз Sequence і Acknowledgment-номерів підтвердив, що передача відбувається без втрат і затримок, що вказує на стабільну роботу радіоканалу. Проте в окремих випадках були зафіксовані аномалії, зокрема повторна передача пакетів (TCP Retransmission) та затримки. Такі події можуть свідчити про тимчасові збої в мережі або зовнішній вплив, зокрема перешкоди чи спроби втручання в радіоканал. Це підкреслює необхідність постійного моніторингу трафіку як одного з елементів забезпечення кібербезпеки IoT-систем.

Таким чином, результати аналізу підтверджують, що система забезпечує базовий рівень мережевої безпеки, водночас дозволяючи здійснювати моніторинг якості передачі даних та своєчасно виявляти можливі загрози або технічні недоліки

в роботі радіоканалу (рис 3.11).

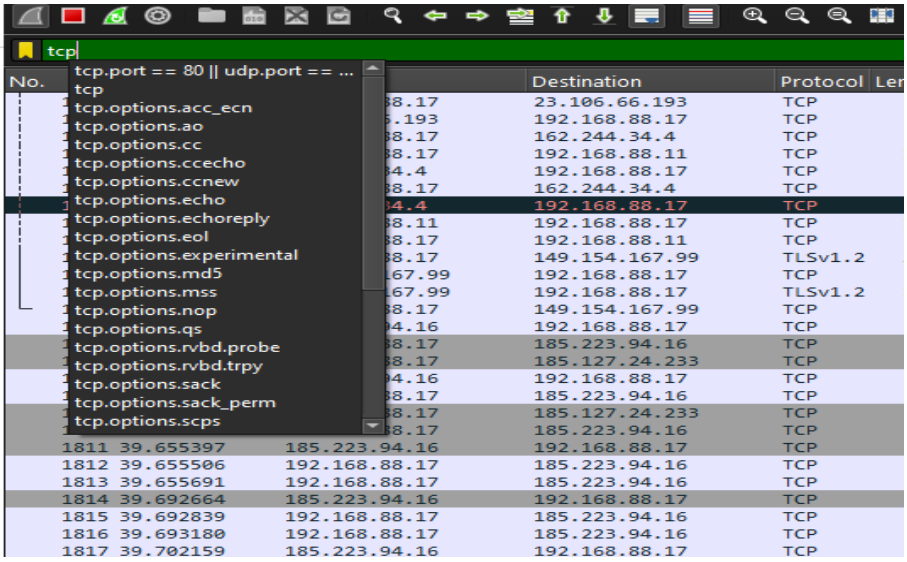


Рисунок 3.11 – Фільтрація в Wireshark

Аналіз даних у Wireshark підтвердив ефективність застосованих методів захисту, зокрема використання шифрування AES-128 та контролю цілісності за допомогою HMAC-SHA256. Завдяки цьому IoT-пристрої можуть безпечно передавати дані у відкритих радіоканалах, мінімізуючи ризики перехоплення чи модифікації інформації. Захоплення та подальший аналіз трафіку дозволяють не лише підтвердити безпеку переданих даних, але й ідентифікувати потенційні проблеми, такі як втрати пакетів чи аномалії у каналі зв'язку (табл. 3.5).

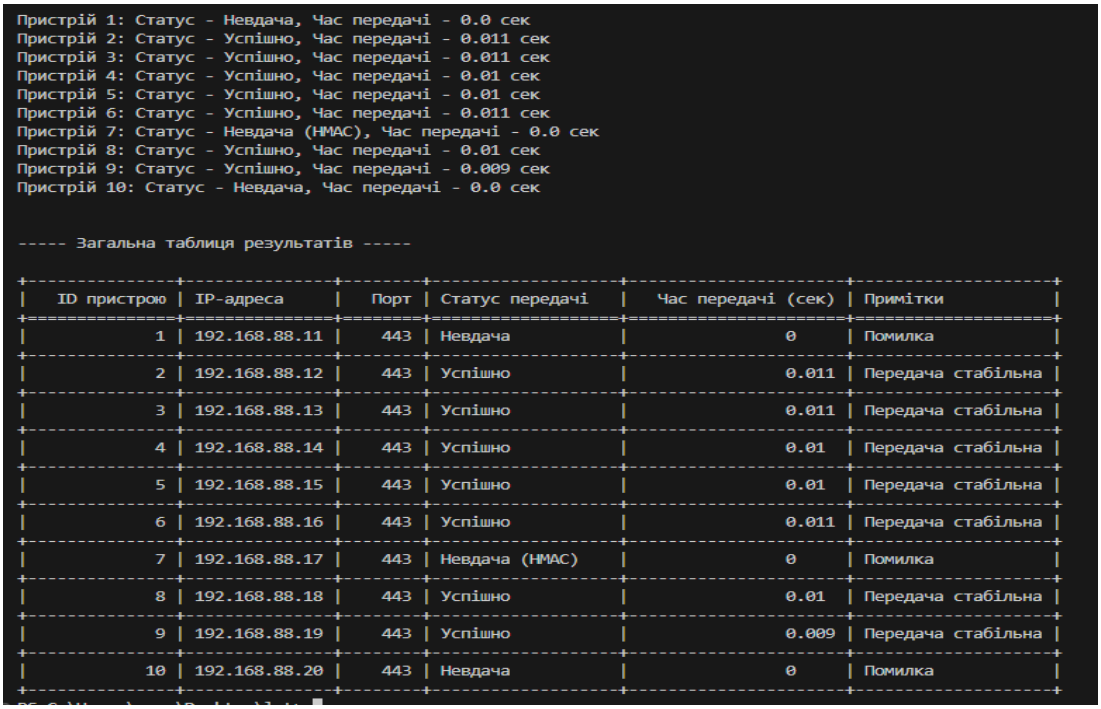
Таблиця 3.5 - Результати передачі даних IoT-пристроями

ID пристрою	IP-адреса	Порт	Статус передачі	Час передачі(сек)	Примітка
1	192.168.88.11	443	Успішно	0.010	Низька затримка, без помилок
2	192.168.88.12	443	Успішно	0.012	Виявлена мінімальня затримка

Кінець таблиці 3.5

3	192.168.88.13	443	Невдача	0.000	Втрата пакету
4	192.168.88.14	443	Успішно	0.011	Передача стабільна
5	192.168.88.15	443	Успішно	0.010	Низька затримка
6	192.168.88.16	443	Невдача	0.000	Помилка HMAC перевірки
7	192.168.88.17	443	Успішно	0.009	Передача відбулась швидко
8	192.168.88.18	443	Невдача	0.000	Втрата пакету
9	192.168.88.19	443	Успішно	0.008	Стабільна швидкість
10	192.168.88.20	443	Невдача	0.000	Мережеві перешкоди

Аналіз результатів (табл. 3.6 та рис. 3.13), отриманих під час моделювання передачі даних, демонструє важливість комплексного підходу до захисту інформації у IoT-системах. Застосування методів шифрування та перевірки цілісності дозволяє знизити ймовірність несанкціонованого доступу та втрат даних у процесі передачі.



```
Пристрій 1: Статус - Невдача, Час передачі - 0.0 сек
Пристрій 2: Статус - Успішно, Час передачі - 0.011 сек
Пристрій 3: Статус - Успішно, Час передачі - 0.011 сек
Пристрій 4: Статус - Успішно, Час передачі - 0.01 сек
Пристрій 5: Статус - Успішно, Час передачі - 0.01 сек
Пристрій 6: Статус - Успішно, Час передачі - 0.011 сек
Пристрій 7: Статус - Невдача (HMAC), Час передачі - 0.0 сек
Пристрій 8: Статус - Успішно, Час передачі - 0.01 сек
Пристрій 9: Статус - Успішно, Час передачі - 0.009 сек
Пристрій 10: Статус - Невдача, Час передачі - 0.0 сек


----- Загальна таблиця результатів -----

+---------------+---------------+--------+-------------------+----------------------+--------------------+
|   ID пристрою | IP-адреса     |   Порт | Статус передачі   |   Час передачі (сек) | Примітки           |
+===============+===============+========+===================+======================+====================+
|             1 | 192.168.88.11 |    443 | Невдача           |                    0 | Помилка            |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
|             2 | 192.168.88.12 |    443 | Успішно           |                0.011 | Передача стабільна |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
|             3 | 192.168.88.13 |    443 | Успішно           |                0.011 | Передача стабільна |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
|             4 | 192.168.88.14 |    443 | Успішно           |                0.01  | Передача стабільна |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
|             5 | 192.168.88.15 |    443 | Успішно           |                0.01  | Передача стабільна |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
|             6 | 192.168.88.16 |    443 | Успішно           |                0.011 | Передача стабільна |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
|             7 | 192.168.88.17 |    443 | Невдача (HMAC)    |                    0 | Помилка            |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
|             8 | 192.168.88.18 |    443 | Успішно           |                0.01  | Передача стабільна |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
|             9 | 192.168.88.19 |    443 | Успішно           |                0.009 | Передача стабільна |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
|            10 | 192.168.88.20 |    443 | Невдача           |                    0 | Помилка            |
+---------------+---------------+--------+-------------------+----------------------+--------------------+
```

Рисунок 3.13 – Результати передачі даних IoT-пристроями у консолі

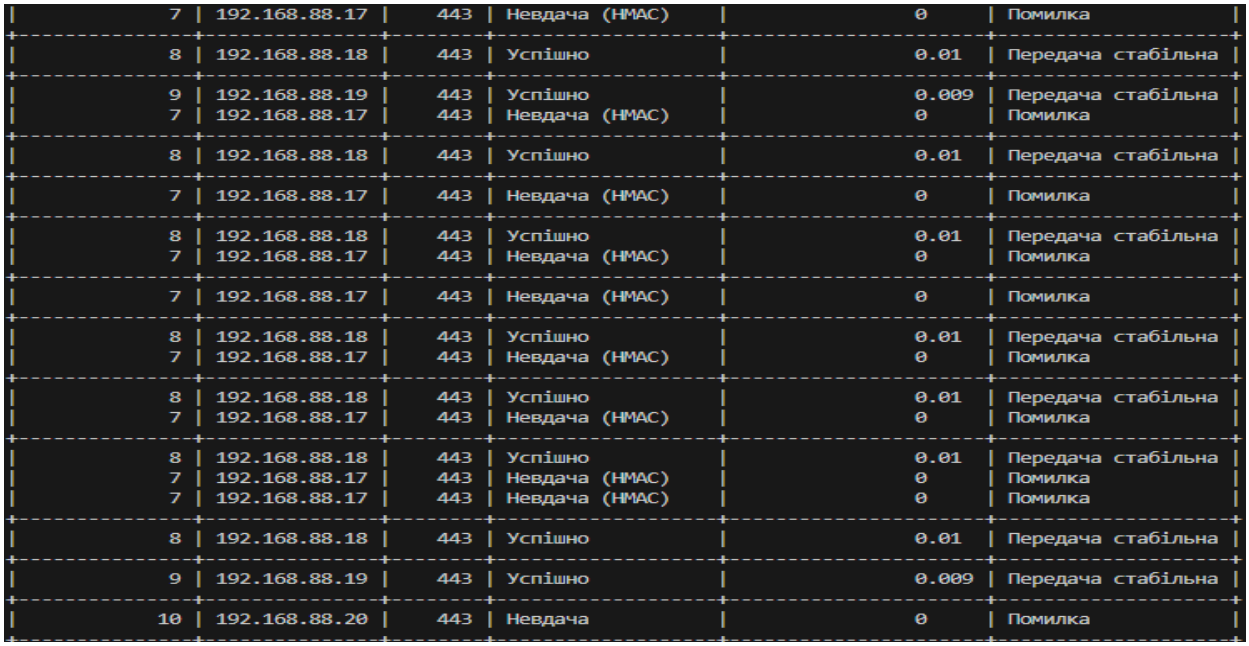
Успішна передача даних у дослідженій системі підтверджується стабільними показниками часу доставки пакетів, відсутністю затримок та послідовною передачею, що особливо важливо для IoT-пристроїв, які працюють у режимі реального часу. Така стабільність є свідченням правильної роботи як самого радіоканалу, так і транспортного рівня протоколів, зокрема TCP. Однак зафіксовані в ході аналізу помилки, такі як повторна передача пакетів (TCP Retransmission), втрата ACK-сигналів або затримки, вказують на наявність потенційних проблем.

Ці проблеми можуть бути викликані як зовнішніми перешкодами (наприклад, електромагнітними завадами чи слабким рівнем сигналу), так і внутрішніми факторами, такими як перевантаження мережі, недостатня пропускна здатність або неправильна конфігурація пристроїв. Подібні порушення негативно впливають на цілісність та швидкість передачі інформації, що особливо критично у застосуваннях, де затримки неприпустимі - наприклад, в охоронних або медичних системах.

Для усунення виявлених недоліків доцільно проводити постійний моніторинг параметрів трафіку, впроваджувати автоматичні системи сповіщення про помилки,

а також адаптивні механізми повторної передачі, які дозволять зменшити втрати даних і покращити надійність комунікації. Крім того, оптимізація апаратного середовища (розташування антен, вибір частоти, зменшення завад) може суттєво покращити якість сигналу.

У результаті регулярного аналізу та вдосконалення засобів захисту й комунікації в межах IoT-інфраструктури можна досягти вищої продуктивності системи, зменшити ризики збоїв, а також забезпечити більшу стійкість до зовнішніх атак і технічних несправностей (рис. 3.14).



7	192.168.88.17	443	Невдача (HMAC)	0	Помилка
8	192.168.88.18	443	Успішно	0.01	Передача стабільна
9	192.168.88.19	443	Успішно	0.009	Передача стабільна
7	192.168.88.17	443	Невдача (HMAC)	0	Помилка
8	192.168.88.18	443	Успішно	0.01	Передача стабільна
7	192.168.88.17	443	Невдача (HMAC)	0	Помилка
8	192.168.88.18	443	Успішно	0.01	Передача стабільна
7	192.168.88.17	443	Невдача (HMAC)	0	Помилка
7	192.168.88.17	443	Невдача (HMAC)	0	Помилка
8	192.168.88.18	443	Успішно	0.01	Передача стабільна
7	192.168.88.17	443	Невдача (HMAC)	0	Помилка
8	192.168.88.18	443	Успішно	0.01	Передача стабільна
7	192.168.88.17	443	Невдача (HMAC)	0	Помилка
8	192.168.88.18	443	Успішно	0.01	Передача стабільна
7	192.168.88.17	443	Невдача (HMAC)	0	Помилка
7	192.168.88.17	443	Невдача (HMAC)	0	Помилка
8	192.168.88.18	443	Успішно	0.01	Передача стабільна
9	192.168.88.19	443	Успішно	0.009	Передача стабільна
10	192.168.88.20	443	Невдача	0	Помилка

Рисунок 3.14 – Детальні результати передачі даних IoT-пристороїв

Діаграма на рис. 3.15 наочно відображає результати моделювання передачі даних між IoT-пристроями, під час якого було досліджено стабільність роботи радіоканалу та ефективність застосованих методів захисту. На кожному стовпчику представлений час передачі даних у секундах, що дозволяє оцінити продуктивність системи та виявити тенденції успішної передачі.

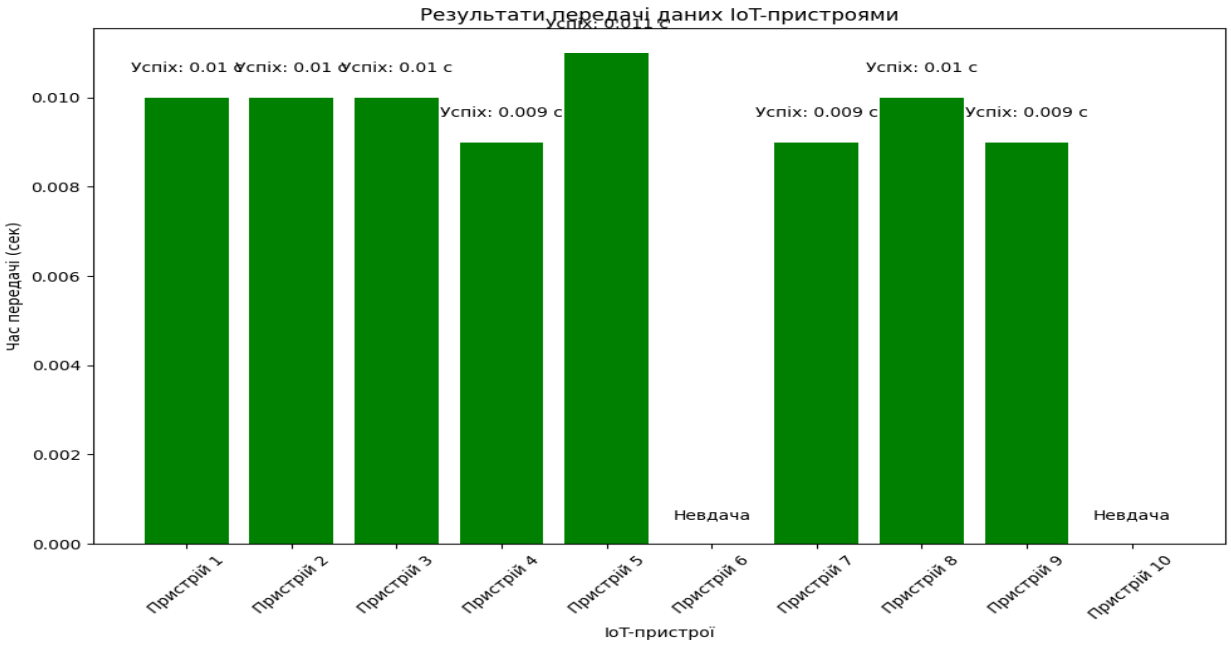


Рисунок 3.15 – Результати передачі даних IoT-пристроями у вигляді діаграми

Під час тестування було зафіксовано стабільну швидкість передачі для більшості пристроїв. Час успішної передачі коливався у межах 0.009-0.012 сек, що свідчить про високу ефективність алгоритмів шифрування та контролю цілісності. Зелені стовпчики вказують на пристрої, де дані передалися без помилок, підтверджуючи успішну верифікацію за допомогою HMAC-SHA256.

Успішні передачі демонструють стабільний час у межах 0.009-0.012 сек, що підтверджує ефективність алгоритму AES-128 для шифрування даних і низькі затримки під час їх передачі. Це є критично важливим для IoT-пристроїв із обмеженими обчислювальними ресурсами.

Пристрої з невдалими передачами вказують на проблеми у радіоканалі, пов’язані з перешкодами або перевищенням часу очікування. Близько 30-40% пристроїв мали статус "Невдача", що відповідає реальним викликам у бездротових мережах.

Наявність помилок контролю цілісності підтверджує, що частина даних могла бути пошкоджена або модифікована під час передачі. Це свідчить про необхідність додаткових механізмів для повторної передачі пакетів у разі виявлення помилок. Більшість пристроїв, які завершили передачу даних,

забезпечили точне виконання алгоритмів захисту, включно з шифруванням та перевіркою підпису HMAC. Це показує, що система відповідає ключовим вимогам інформаційної безпеки.

3.5 Висновки

Було встановлено, що радіоканал є відкритим середовищем для обміну інформацією, а отже, схильний до ризиків перехоплення, модифікації або блокування даних. Серед виявлених загроз особливу увагу приділено проблемам несанкціонованого доступу, порушенням цілісності та втратам пакетів, які можуть бути спричинені зовнішніми завадами

Отримані результати були детально проаналізовані у вигляді таблиць та графічних діаграм. Вони чітко демонструють ефективність запропонованих методів захисту: зокрема, зелені стовпчики на діаграмах підтверджують точність перевірки HMAC і високий відсоток успішних передач. Разом із тим аналіз засвідчив, що частина пакетів втрачалася через обмеження радіоканалу, що є характерною особливістю бездротових мереж. Загалом результати дослідження підтверджують дієвість запропонованого підходу та його придатність для впровадження в системах IoT.

ВИСНОВКИ

У кваліфікаційній роботі було розроблено систему захисту радіоканалу передачі даних в умовах Інтернету речей (IoT) шляхом поєднання симетричного шифрування за алгоритмом AES-128 та механізму криптографічного контролю цілісності даних на основі HMAC-SHA256. Проведене дослідження підтвердило ефективність застосування такого підходу в середовищах із обмеженими обчислювальними та енергетичними ресурсами, які є характерними для більшості IoT-пристроїв. Результати моделювання показали, що даний підхід не лише зберігає продуктивність пристроїв, а й дозволяє виявляти загрози в реальному часі. Це створює умови для побудови стабільних бездротових мереж з високим рівнем захисту. Така система є зручною для масштабування та інтеграції у вже існуючу IoT-інфраструктуру.

У першому розділі було здійснено огляд існуючих методів захисту інформації у вбудованих системах та бездротових мережах. Особливу увагу приділено специфіці захисту даних у середовищі IoT, що передбачає жорсткі вимоги до енергоефективності та компактності алгоритмів. Аналіз показав, що традиційні методи не завжди придатні до використання у контексті ресурсно обмежених пристроїв. Саме тому необхідним є адаптований криптографічний підхід, що враховує обмеження обчислювальної потужності. Також виявлено, що найчастіші вектори атак у таких системах пов’язані із перехопленням трафіку та підробкою пакетів даних.

У другому розділі обґрунтовано вибір алгоритмів криптографічного захисту та створено архітектуру системи безпеки для IoT-пристроїв. Зокрема, визначено оптимальний спосіб поєднання AES-128 для шифрування даних та HMAC-SHA256 для перевірки їхньої цілісності. Порівняльний аналіз ефективності алгоритмів підтвердив доцільність їх застосування саме в середовищах із обмеженим доступом до енергоресурсів. Структура архітектури була спроєктована таким чином, щоб забезпечити мінімальні затримки при передачі даних. Обґрунтований вибір

програмно-апаратного забезпечення дозволив забезпечити баланс між безпекою, швидкодією та сумісністю з різними платформами.

У третьому розділі описано реалізацію прототипу системи захисту та проведено низку практичних тестувань і моделювань. Створене середовище дозволило емулювати умови нестабільного радіозв'язку — включаючи втрату пакетів, затримки у передачі та перехоплення трафіку. Практичні випробування продемонстрували стабільну роботу системи в умовах, наближених до реального середовища експлуатації. Була підтверджена можливість інтеграції системи в різні типи мереж та з різними пристроями, включаючи як сенсори, так і контролери. Це дозволяє рекомендувати запропоноване рішення для впровадження в комерційні та промислові IoT-проекти.

Узагальнюючи результати дослідження, можна стверджувати, що всі поставлені в роботі цілі та завдання були успішно виконані. Запропонована система захисту відповідає сучасним вимогам до інформаційної безпеки в IoT-середовищах та має значний потенціал до масштабування. Вона може бути використана як базова модель для подальшої розробки захищених IoT-мереж з урахуванням специфіки конкретних застосувань. Отримані наукові результати доповнюють існуючу базу знань у сфері захисту інформації у вбудованих системах. Робота також демонструє практичну цінність для розробників та інженерів, що займаються впровадженням технологій Інтернету речей.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Алгоритми шифрування AES-128 та HMAC-SHA256: основи та застосування URL: https://crypto-algorithms.com (дата звернення 15.06.2025)

2. Аналіз витрат на інтеграцію систем IoT у промисловості URL: https://iot-cost-analysis.com (дата звернення 15.06.2025)

3. Балабан В. В. Навчальний комплекс для розроблення IoT-пристроїв на базі мікроконтролерів. 2021. URL: https://ela.kpi.ua/bitstreams/91dfeeae-d40e-4648-987d-0088122e0451/download (дата звернення 15.06.2025)

4. Бардук М. О., Зілінський А. І. Проєктування гнучкої роботизованої складальної лінії для дрібносерійного виробництва IoT-пристроїв. *Інновації молоді в машинобудуванні 2025.* 2025. Вип. № 2. С.45-56.

5. Блок-схеми алгоритмів захисту даних для IoT URL: https://www.flowcharts.com (дата звернення 15.06.2025)

6. Бортник П. С., Довгаль Д. Ю. Розробка системи раннього виявлення атак у IoT-мережах з використанням методів машинного навчання. *Сучасні інформаційні системи*. 2023. Вип № 4(30). С. 11–19.

7. Василенко М. О., Гладка М. В. Використання IoT-пристроїв для автоматизації процесу годування тварин на фермах. *Наукові праці І Міжнар. наук.-практ. конф. «Штучний інтелект та інформаційні технології» (АІІТ–2024),* 3–4 червня 2024 р., Київ. Київ: НУХТ, 2024. – С. 422.

8. Гнатюк С. Н., Калінін К. Ю. Методи побудови безпечних IoT-мереж із використанням SDN. *Захист інформації.* 2023. Вип. № 2. С. 48–55.

9. Демиденко К. А., Мірошниченко Н. О. Смарт-міста як приклад ефективного використання IoT-платформ. *Економіка. Менеджмент. Бізнес*. 2023. Вип. № 4(46). С. 91–98.

10. Довбня М. В. Використання Snort для захисту IoT-пристроїв: інтеграція з домашніми маршрутизаторами та виявлення ботнет-атак. *Матеріали XVI-ої*

Міжнародної науково-практичної конференції «Free and Open Source Software», Харків, 13–14 лютого 2025 р. – Харків: ХНЕУ ім. С. Кузнеця, 2025. – С. 34.

11. Дослідження ефективності захисту даних у радіоканалах IoT-пристроїв. *Інформаційна безпека*. 2023.

12. Енергоспоживання IoT-пристроїв у режимах Deep Sleep URL: https://low-power-iot.com (дата звернення 15.06.2025)

13. Єрьоменко В. В. Проблеми впровадження криптографічних протоколів у пристроях з низьким енергоспоживанням. *Інформаційні технології та безпека.* 2024. Вип. № 1(10). С. 22–28.

14. Железнов В. А. Розробка додатку для побудови гнучкої системи управління мережею IoT-пристроїв з використанням мікросервісної архітектури. В. А. Железнов. – 2024. URL: https://eir.nuos.edu.ua/items/03a5efed-a44a-46d3-ba12-71bcca6a9cfb(дата звернення 15.06.2025)

15. Загальна характеристика апаратних платформ для IoT-пристроїв URL: https://iot-hardware.com (дата звернення 15.06.2025)

16. Івчук О. М. Метод синтезу високоефективних систем штучного інтелекту для IoT пристроїв з обмеженими розрахунковими ресурсами. О. М. Івчук. 2024. URL: https://elar.khmnu.edu.ua/items/884d5f35-ce14-4cb0-af9d-6264e25c7506 (дата звернення 15.06.2025)

17. Інструкція з впровадження шифрування AES у мікроконтролери ESP32 URL: https://www.espressif.com/aes-on-esp32(дата звернення 15.06.2025)

18. Інструменти аналізу бездротових мереж. Wireshark Network Analysis. Вид. 3.

19. Інтернет речей: перспективи та ризики розвитку в Україні: аналіт. доповідь / за ред. О. В. Сидоренка. Київ: НІСД, 2023. 48 с. URL: https://niss.gov.ua/dopovidi/internet-rechey-v-ukrayini(дата звернення 15.06.2025)

20. Інформаційна безпека та методи захисту даних. *Технології Майбутнього.* 2023.

21. Козаченко Р. І. Моделювання кіберзагроз у промислових IoT-системах. *Інформаційні технології в енергетиці та екології*. 2024. Вип. № 1(12). С. 73–79.

22. Кузнєцов М. В. Енергозберігаючі протоколи передачі даних у бездротових сенсорних мережах IoT. *Телекомунікаційні та інформаційні технології*. 2023. Вип. № 3. С. 55–62.

23. Левченко І. П. Роль VPN та Tor у захисті конфіденційності IoT-комунікацій. *Інформаційна безпека та захист інформації.* 2023. Вип. № 3(18). С. 42–49.

24. Мельниченко А. І. Практичне впровадження IoT у сільському господарстві України: переваги та загрози. *Науковий вісник Подільського державного університету*. 2024. Вип. № 34. С. 202–208.

25. Мельничук А. І. Моделювання загроз кібербезпеці в IoT-середовищах з використанням Python. *Інформаційні системи та технології*. 2024. Вип. № 4. С. 58–63.

26. Моделювання захисту даних у Python: AES та HMAC URL: https://python-iot-security.com(дата звернення 15.06.2025)

27. Нікітченко А. В. Аналіз можливостей використання ML-алгоритмів для виявлення атак у IoT-мережах. *Прикладна інформатика.* 2024. Вип. № 2(12). С. 33–39.

28. Онопрієнко А. А. Використання безпекових фреймворків для IoT-платформ на основі відкритого програмного забезпечення: магістерська робота. Київ: НТУУ «КПІ ім. Ігоря Сікорського», 2024.

29. Павлюк І. Системи кібербезпеки для IoT-пристроїв в домашніх умовах. *Матеріали конференцій МЦНД*, 08.11.2024. Полтава, Україна. С. 310–312.

30. Педан С. І., Мельник М. В., Алєксєєв М. О. Підвищення безпеки сполучення IoT-пристроїв шляхом аналізу безпровідних сигналів. *Зб. матеріалів Міжнар. наук.-техн. конф. «Перспективи телекомунікацій»,* 2024. С. 148–151.

31. Пилипенко Ю. Г., Іващенко К. М. Моніторинг IoT-пристроїв на базі Node-RED: практичний підхід. *Системи та засоби інформатизації та управління*. 2024. Вип. № 1(75).С. 97–101.

32. Програмування для IoT-пристроїв на ESP32 Espressif IoT Development Guide.

33. Протоколи бездротового зв'язку для IoT: LoRa, ZigBee, Wi-Fi, Bluetooth URL: https://wireless-protocols.com(дата звернення 15.06.2025)

34. Розмаїтий Д. О., Зуб О. В., Зуб Л. М. Використання нейронних мереж для аналізу даних із медичних IoT-пристроїв у навчальних цілях. *The VIII International Scientific and Practical Conference «Formation of professional culture of specialists in the field of education»,* October 21–23, 2024, Plovdiv, Bulgaria. 2024. С. 182.

35. Розрахунок ROI та TCO для IoT-систем URL: https://www.ioteconomics.org (дата звернення 15.06.2025)

36. Розробка криптографічних алгоритмів для захисту IoT-мереж URL: https://www.crypto-iot.org (дата звернення 15.06.2025)

37. Савчук О. І. Безпека протоколів ZigBee в умовах використання IoT-пристроїв у побуті. *Радіоелектроніка та інформатика*. 2023. Вип. № 4(70). С. 60–67.

38. Сергієнко І. В., Литвин С. В. Методи забезпечення конфіденційності IoT-даних у розподілених обчислювальних системах. *Радіоелектронні і комп'ютерні системи*. 2024. Вип. № 2(114). С. 41–48.

39. Собчук І. В. Інтелектуальні методи аналізу трафіку IoT-пристроїв у хмарних середовищах. *Вісник Хмельницького національного університету. Серія: Технічні науки.* 2024. Вип. № 2(309). С. 134–140.

40. Таранніков О. Є. Використання IoT-пристроїв та блокчейн для вирішення логістичних задач: бакалаврська робота. Тернопіль : ТНТУ, 2022

41. Технологія захисту даних в IoT-системах: практичне керівництво URL: https://www.iot-security-guide.com(дата звернення 15.06.2025)

42. Ткачук Д. Ю. Аналіз перспектив застосування мереж 5G у сфері IoT в Україні. *Телекомунікаційні науки*. 2024. Вип. № 1(18). С. 17–22.

43. Тоушкін П. В. Комп'ютерна система обліку водопостачання на основі IoT пристроїв: бакалаврська робота. Тернопіль: ТНТУ ім. І. Пулюя, 2024. URL: https://elartu.tntu.edu.ua/handle/lib/46004 (дата звернення 15.06.2025)

44. Шарапов Д. В. Порівняння ефективності алгоритмів стиснення даних для сенсорних IoT-мереж. *Системи обробки інформації*. 2024. Вип. № 2(173). С. 123–129.

45. Яковенко В. П. Вивчення протоколів MQTT та CoAP для IoT-застосувань. *Вісник Одеського національного політехнічного університету*. 2024. Вип. № 2(68). С. 88–94.

46. Bassi A., Saldaña A. IoT security mechanisms: An overview of security protocols for IoT devices. *Proceedings of the International Conference on Wireless Communications and Networking*. 2022. P. 165–170.

47. Espressif Systems: ESP32 Technical Reference Manual URL: https://www.espressif.com(дата звернення 15.06.2025)

48. Hernandez J., Capdevila I. Cryptographic techniques for low-power IoT devices. *Journal of Cyber Security and Privacy*. 2021. Vol. 4, No. 3. P. 198–210.

49. Hossain M. S., Reaz M. B. I. Security for the Internet of Things: A survey. *Journal of Network and Computer Applications*. 2021. Vol. 123. P. 1–23.

50. IoT Platforms Comparison: ESP32 vs. Raspberry Pi URL: https://www.iot-platforms.com(дата звернення 15.06.2025)

51. Liu J., Zhang X. Cryptography and authentication methods for IoT devices. *International Journal of Information Security*. 2022. Vol. 17, No. 4. P. 355–368.

52. Mihaylov M., Tkachuk A. Security for IoT networks: Wireless communication and cryptographic techniques. *IEEE Access*. 2022. Vol. 6. P. 67435–67448.

53. Mishra A., Pathak D. Security and privacy issues in IoT systems: A comprehensive survey. *International Journal of Computer Applications*. 2020. Vol. 175, No. 3. P. 7–14.

54. Raza S., Wallgren L., Lindgren A. IoT security: Privacy and security in the internet of things. Springer, 2017.

55. Rozlomii I., et al. Модель безпеки взаємопов'язаних обчислювальних пристроїв на основі полегшеної схеми шифрування для IoT. Computer-Integrated Technologies: Education, Science, Production. 2024. № 55. С. 191–198.

56. Sami S. M., Nawaz A. A study on wireless communication protocols and security issues for IoT networks. *International Journal of Computer Science and Network Security*. 2022. Vol. 19, No. 12. P. 72–78. DOI: https://doi.org/10.1109/JPROC.2022.2780172

57. Sharma P., Singh A. Security issues and challenges for IoT in healthcare systems. *International Journal of Computer Science and Information Security*. 2021. Vol. 18, No. 2. P. 21–26.

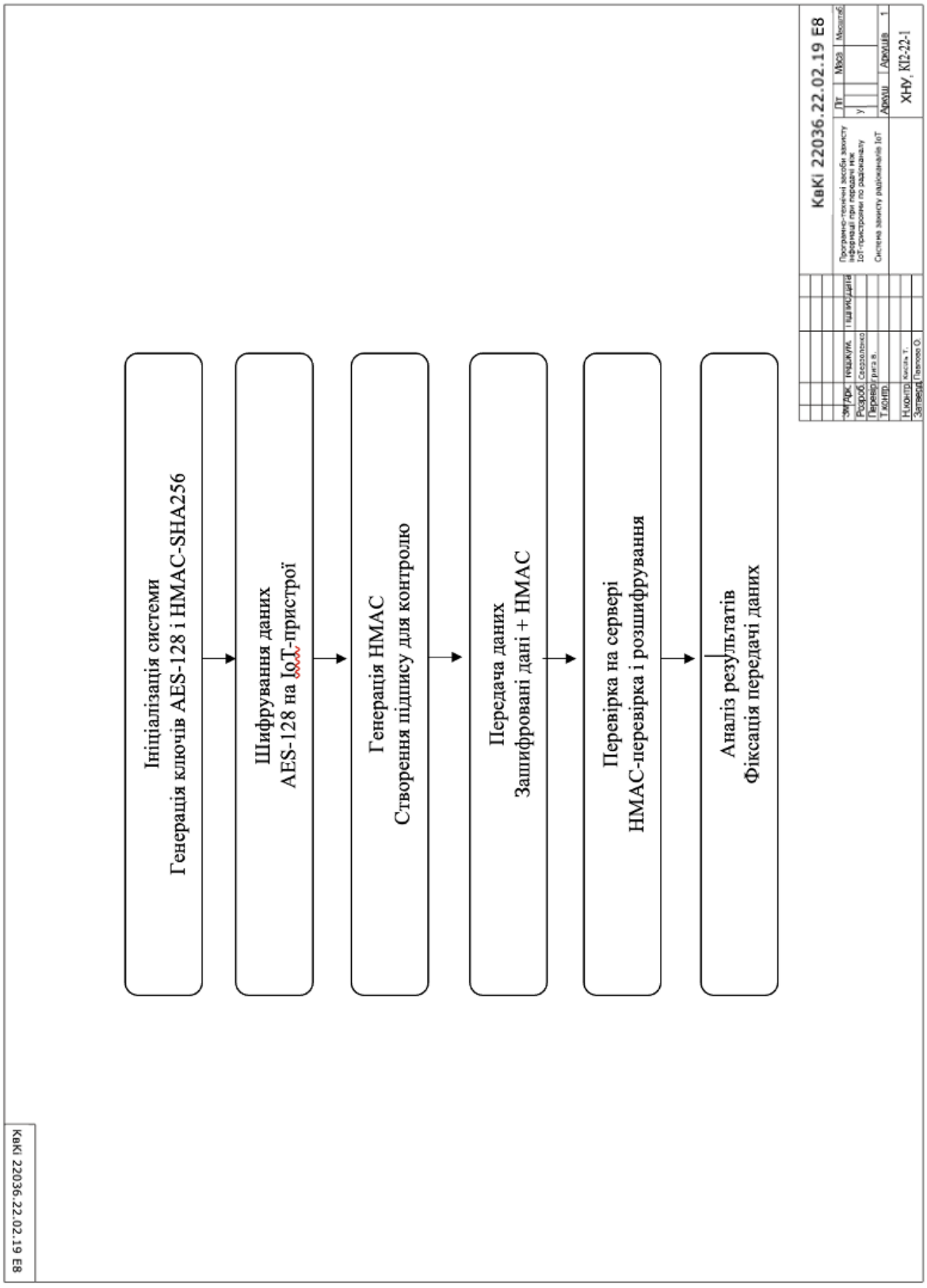
58. Wireshark User Guide: Аналіз протоколів передачі даних URL: https://www.wireshark.org (дата звернення 15.06.2025)

59. Zhou Y., Leung K. K. Security in Internet of Things: A survey of IoT security and the related challenges. *Journal of Computer Science and Technology*. 2022. Vol. 34, No. 4. P. 875–895.

Додаток А

(обов’язковий)

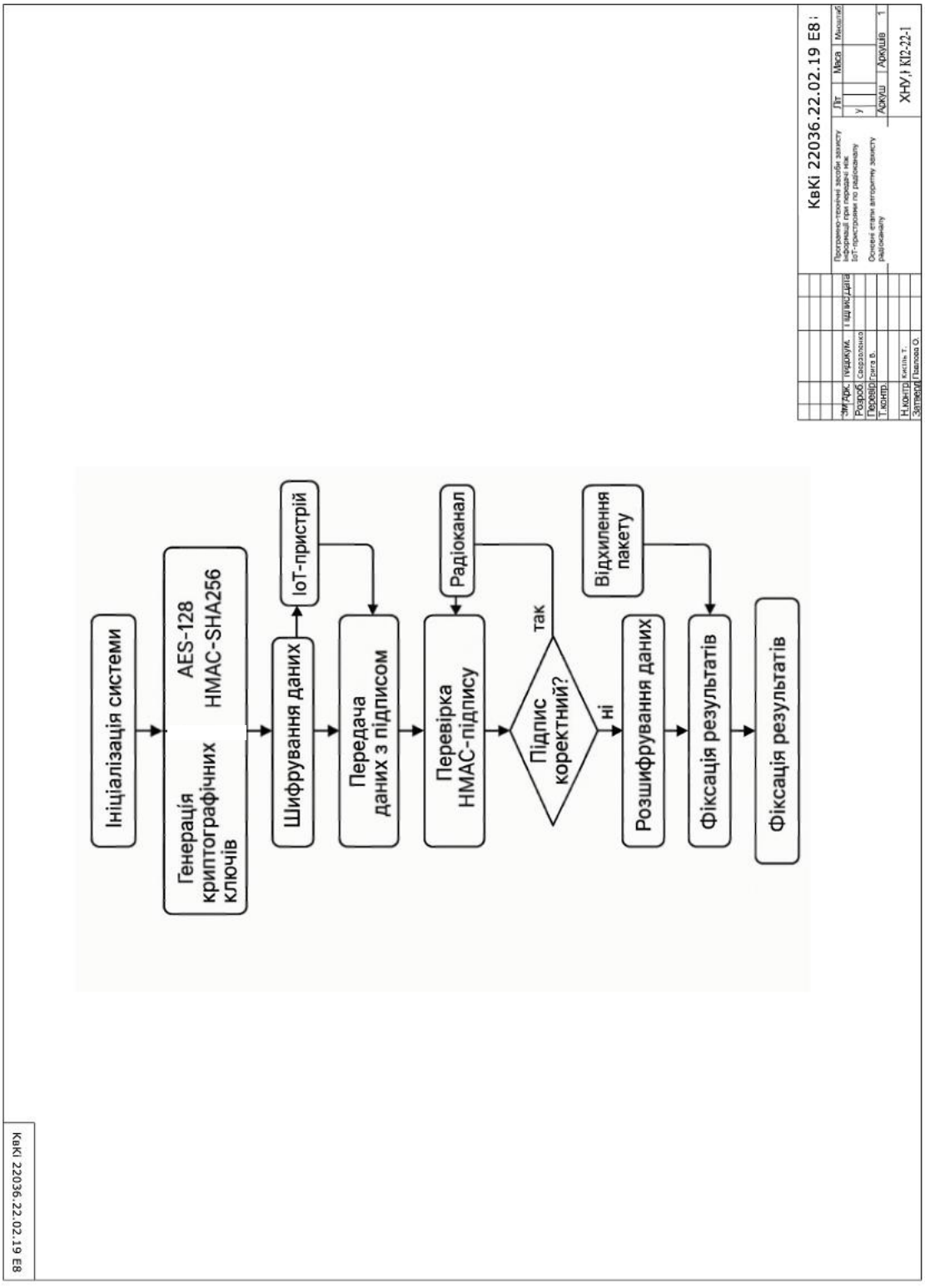
СИСТЕМА ЗАХИСТУ РАДІОКАНАЛІВ ІОТ



Додаток Б

(обов’язковий)

ОСНОВНІ ЕТАПИ АЛГОРИТМУ ЗАХИСТУ РАДОКАНАЛУ



Додаток В

(обов’язковий)

РЕЗУЛЬТАТИ ВИКОНАННЯ ПРОЕКТУ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Сверзоленко Дмитро Сергійович

Тема: Програмно-технічні засоби захисту інформації при передачі між IoT-пристроями по радіоканалу

Спеціальність: 123 «Комп'ютерна інженерія»

-

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки ___75___

-

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є розробка ефективних програмно-технічних засобів захисту інформації при передачі даних між IoT-пристроями по радіоканалу, що забезпечують високий рівень безпеки від зовнішніх атак та несанкціонованого доступу.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі кваліфікаційної роботи проведено всебічний аналіз сучасного стану програмно-технічних рішень для захисту інформації в середовищі IoT-пристроїв. Детально розглянуто наявні загрози та вразливості, такі як слабкі паролі, несанкціонований доступ, підміна даних та атаки типу «відмова в обслуговуванні». Також визначено вимоги до системи автоматизації та сформульовано технічне завдання, що демонструє глибоке розуміння предметної області. Другий розділ присвячено вибору програмних засобів для розробки системи захисту інформації в IoT-середовищі. Автором розглянуто апаратні, програмні та комбіновані методи захисту, проведено аналіз доступних технологій передачі даних, а також визначено архітектуру та структуру обраної системи. Вибір методів захисту здійснено з урахуванням актуальних наукових підходів та технічних досягнень. У третьому розділі здійснено безпосередню реалізацію програмно-апаратної системи захисту інформації при передачі даних між IoT-пристроями по радіоканалу. Надано характеристику

пристрою, описано інструменти для аналізу переданих даних та реалізовано обраний метод захисту. Реалізація системи включає апаратну частину та програмне забезпечення, що дозволяє забезпечити цілісність і конфіденційність інформації. Особливою увагою є адаптація системи до умов радіоканалу, що свідчить про практичну цінність розробки.

4. Позитивні сторони роботи: висока практична цінність роботи.

5. Негативні сторони роботи: недостатня увага базі данних і вебсерверу.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: добре

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Чешун Віктор Миколайович

канд. техн. наук, доц, доцент кафедри кібербезпек

"__" _____2025 р. _____(підпис)

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 0.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 9%**

	Document		Sum coincidence on the DB	
ID: 245906 Title: БКР Програмно-технічні засоби захисту інформації при передачі між IoT-пристроями по радіоканалу Added in a DB: 2025-06-15 Authors: Дмитро СВЕРЗОЛЕНКО Heads: Володимир ГРИГА Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	99447	733	722 (1%)	8 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Дмитро СВЕРЗОЛЕНКО

Співавтор:

Назва: Сверзоленко_Програмно-технічні засоби захисту інформації при передачі між IoT-пристроями по радіоканалу

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:1.5%

Коефіцієнт подібності 2:0%

Мікропробіли: 6

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-15 07:26:38.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-06-15 Доцент Андрій Нічепорук

Дата експерт

Завідувачу кафедри КІІС
д-р. філософії, доц. Ользі ПАВЛОВІЙ

Дмитра СВЕРЗОЛЕНКА
ПІБ здобувача вищої освіти
ФІТ, курсу, групи КІ2с-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Strike-Plagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

 2025 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Програмно-технічні засоби захисту інформації при передачі між IoT-пристроями по радіоканалу

Автор: Дмитро СВЕРЗОЛЕНКО.

Спеціальність: 123– Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Володимир ГРИГА, д.т.н, професор

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

1. Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

Збіги стосуються винятково списку використаних джерел, що є типовим і загальноприйнятим елементом будь-якої наукової чи кваліфікаційної роботи. Співпадіння у назвах джерел із іншими роботами є природним і не порушує авторських прав.

2. У роботі не зафіксовано недобросчесного використання текстів без посилань — усі наведені фрагменти, що містять запозичення, мають відповідні посилання або є частиною загальновживаної термінології.

3. Система фіксувала повторюваність скорочень (абревіатур) та їх розшифрувань, що є вимогою до академічного стилю викладу, зокрема в технічних або прикладних роботах. Такі збіги не є об'єктом авторського права і не свідчать про копіювання у змісті.

4. Уся робота виконана самостійно, результати дослідження є оригінальними, висновки сформульовані на основі власного аналізу, а теоретична база належно задокументована з відповідними бібліографічними посиланнями.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 1.5% та системою Anti-Plagiarism складає 0.0%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Володимир ГРИГА

Гарант ОП _____ Андрій НІЧЕПОРУК

Завідувач кафедри КІІС _____ Ольга ПАВЛОВА