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

КВАЛІФІКАЦІЙНА РОБОТА

Кіберфізична системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу

Рівень вищої освіти *другий (магістерський)*

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

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

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

Шифр КвРКІ 240256.24.01.24 ПЗ

Виконав здобувач II курсу, група КІ2м-24-2 _____ Денис ТКАЧЕНКО
Підпис Ініціали, прізвище

Керівник д. техн. наук, професор _____ Василь ЯЦКІВ
Науковий ступінь, учене звання Підпис Ініціали, прізвище

Нормоконтролер д. техн. наук, професор _____ Сергій ЛИСЕНКО
Науковий ступінь, учене звання Підпис Ініціали, прізвище

До захисту допускаю:
завідувач кафедри КІІС _____ Ольга ПАВЛОВА
«1» травня 2026 р. Підпис Ініціали, прізвище
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Рівень вищої освіти другий (магістерський)

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІС
_____ Ольга ПАВЛОВА

"12" 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ткаченку Денису Дмитровичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу
Керівник проекту (роботи) Яцків Василь Васильович, д.т.н., проф.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 12.01.2026 р. № 6

2. Термін подання здобувачем роботи на кафедру 19.05.2026 р.

3. Вихідні дані до роботи Завдання на кваліфікаційну роботу

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

Кіберфізична система виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу та постановка задачі щодо її розроблення і вдосконалення

Обґрунтування вибору моделей і методів аналізу параметрів радіоканалу для виявлення та локалізації прихованих Wi-Fi камер у приміщеннях

Реалізація, експериментальна перевірка та оцінювання ефективності кіберфізичної системи виявлення і локалізації прихованих Wi-Fi камер у приміщеннях

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

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийня

7. Дата видачі завдання «12» 01 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	12.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	12.01.2026	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	20.01.2026	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	01.02.2026	виконано
5	Робота над науковою статтею	01.03.2026	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.03.2026	виконано
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	01.04.2026	виконано
8	Оформлення пояснювальної записки згідно вимог	18.04.2026	виконано
9	Попередній захист ДРМ	29.04.2026	виконано
10	Захист ДРМ на засіданні ЕК	20.05.2026	

Здобувач _____ Денис ТКАЧЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Василь ЯЦКІВ
Підпис Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Кіберфізична системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу

Автор роботи: Ткаченко Денис Дмитрович.

Керівник роботи: Яцків Василь Васильович.

Пояснювальна записка: 78 с., 19 рис., 13 табл., 3 дод., 81 джерело.

КІБЕРФІЗИЧНА СИСТЕМА, WI-FI КАМЕРА, ПРИХОВАНЕ ВІДЕОСПОСТЕРЕЖЕННЯ, РАДІОКАНАЛ, CSI, RSSI, ЛОКАЛІЗАЦІЯ, ДИФРАКЦІЯ

Об’єктом дослідження є процес виявлення та локалізації прихованих Wi-Fi камер у приміщеннях із використанням параметрів бездротового радіоканалу.

Предметом дослідження є моделі, методи, алгоритми та програмно-апаратні засоби кіберфізичної системи, що забезпечують виявлення підозрілих Wi-Fi пристроїв і визначення напрямку на приховану камеру на основі аналізу параметрів радіоканалу.

Метою кваліфікаційної роботи магістра є розроблення архітектури та програмно-апаратних компонентів кіберфізичної системи виявлення і локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу, зокрема CSI/RSSI-характеристик та ефектів контрольованої дифракції електромагнітного сигналу.

Для розв’язання поставлених задач використовувалися методи аналізу бездротових мереж, методи цифрової обробки сигналів, методи статистичного аналізу параметрів радіоканалу, методи пасивного моніторингу Wi-Fi трафіку, методи моделювання кіберфізичних систем, методи аналізу CSI/RSSI-параметрів, а також методи експериментальної перевірки ефективності програмно-апаратних засобів.

Наукова новизна отриманих результатів:

– набув подальшого розвитку метод виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу, який, на відміну від традиційних підходів, поєднує пасивне спостереження за Wi-Fi трафіком із оцінюванням змін характеристик бездротового сигналу для визначення напрямку на джерело випромінювання;

– набув подальшого розвитку підхід до побудови кіберфізичних систем захисту приватності, що поєднує апаратний збір радіоданих, аналіз трафіку та алгоритми локалізації прихованих пристроїв.

На основі проведених досліджень розроблена архітектура і компоненти програмного забезпечення кіберфізичної системи виявлення та локалізації прихованих Wi-Fi камер, що включають модулі сканування бездротового середовища, фільтрації підозрілих пристроїв, збору параметрів радіоканалу, обробки CSI/RSSI-даних, визначення азимутального напрямку на джерело сигналу та формування результатів для користувача.

Практична значимість отриманих результатів полягає у можливості використання запропонованої системи для підвищення рівня приватності та безпеки в житлових, офісних, готельних і тимчасово орендованих приміщеннях. Розроблені алгоритми та програмно-апаратна архітектура можуть бути використані як основа для створення переносного засобу виявлення прихованих Wi-Fi камер без потреби у дорогому спеціалізованому обладнанні або попередньому навчанні системи для конкретного приміщення.

У першому розділі проведено обґрунтування актуальності теми, проаналізовано сучасний стан задачі виявлення прихованих Wi-Fi камер, розглянуто існуючі підходи до пошуку та локалізації прихованих пристроїв відеоспостереження, визначено їх переваги й недоліки, а також сформульовано постановку задачі дослідження.

У другому розділі обґрунтовано вибір теоретичних та експериментальних методів дослідження, описано моделі аналізу параметрів радіоканалу, розглянуто використання CSI/RSSI-характеристик для виявлення змін у бездротовому

середовищі, а також сформовано математичні й структурні основи побудови кіберфізичної системи.

У третьому розділі розроблено алгоритмічне забезпечення та архітектуру програмно-апаратної системи, визначено функціональні й нефункціональні вимоги, описано структуру програмних модулів, логіку взаємодії апаратних компонентів і послідовність роботи системи під час виявлення та локалізації прихованої Wi-Fi камери.

У четвертому розділі наведено опис реалізації програмно-апаратних компонентів системи, розглянуто особливості роботи розробленого програмного забезпечення, проведено експериментальну перевірку, проаналізовано результати досліджень, оцінено достовірність, ефективність, практичну цінність запропонованого рішення та визначено напрями його подальшого вдосконалення.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

ОС – операційна система

ІТ – інформаційні технології

Wi-Fi – технологія бездротової передачі даних стандарту IEEE 802.11

CSI – інформація про стан каналу, що відображає параметри поширення Wi-Fi сигналу

RSSI – індикатор рівня прийнятого сигналу

MAC – апаратна адреса мережевого пристрою

IoT – Інтернет речей, сукупність підключених до мережі пристроїв

GPIO – універсальний інтерфейс введення/виведення для підключення апаратних модулів

LOS – пряма видимість між передавачем і приймачем

NLOS – відсутність прямої видимості між передавачем і приймачем

FFZ – перша зона Френеля, область поширення основної енергії радіосигналу

DIFFLOC – метод локалізації прихованих Wi-Fi камер на основі електромагнітної дифракції

ВСТУП

У сучасних умовах розвитку бездротових технологій проблема захисту приватності людини у житлових, офісних, готельних і тимчасово орендованих приміщеннях набуває особливої актуальності. Мініатюрні Wi-Fi камери та IoT-пристрої можуть бути приховані у побутових предметах, адаптерах живлення, датчиках або елементах декору. Завдяки підключенню до бездротової мережі такі пристрої здатні непомітно передавати відеопотік у реальному часі, що створює загрозу несанкціонованого спостереження.

Традиційні способи пошуку прихованих камер ґрунтуються на візуальному огляді, виявленні відблисків лінзи, тепловому контролі або аналізі електромагнітного випромінювання. Проте вони часто потребують дорогого обладнання, досвіду оператора та ретельної перевірки кожного предмета. Тому перспективним є використання параметрів Wi-Fi радіоканалу, зокрема CSI та RSSI, які відображають зміни середовища поширення сигналу.

Актуальність роботи полягає в розробленні кіберфізичної системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу, що дозволяє підвищити ефективність пошуку прихованих пристроїв відеоспостереження без використання дорогого спеціалізованого обладнання.

Метою кваліфікаційної роботи магістра є розроблення моделей, алгоритмів та програмно-апаратної архітектури кіберфізичної системи виявлення і локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу.

Поставлена мета досягається розв’язанням таких основних завдань:

– проаналізувати сучасний стан проблеми виявлення та локалізації прихованих Wi-Fi камер у приміщеннях;

– дослідити існуючі методи пошуку прихованих камер, визначити їх переваги та обмеження;

– обґрунтувати доцільність використання CSI/RSSI-параметрів радіоканалу для аналізу бездротового середовища;

– розробити модель, алгоритми та архітектуру кіберфізичної системи виявлення і локалізації прихованих Wi-Fi камер;

– провести експериментальну перевірку запропонованих рішень та оцінити ефективність системи.

Об’єктом дослідження є процес виявлення та локалізації прихованих Wi-Fi камер у приміщеннях за параметрами бездротового радіоканалу.

Предметом дослідження є моделі, методи, алгоритми та програмно-апаратні засоби визначення підозрілих Wi-Fi пристроїв і напряму на приховану камеру.

Наукова новизна отриманих результатів:

– набув подальшого розвитку метод виявлення та локалізації прихованих Wi-Fi камер, який поєднує пасивний моніторинг Wi-Fi трафіку з аналізом змін характеристик радіосигналу;

– набув подальшого розвитку підхід до побудови кіберфізичних систем захисту приватності, що поєднує апаратний збір радіоданих, аналіз трафіку та алгоритми локалізації прихованих пристроїв.

На основі проведених досліджень розроблено архітектуру кіберфізичної системи, що включає модулі сканування бездротового середовища, аналізу трафіку, збору CSI/RSSI-параметрів, визначення азимуту та подання результатів користувачу.

Практична значимість отриманих результатів полягає у можливості створення переносного засобу пошуку прихованих Wi-Fi камер у житлових, офісних, готельних та інших приміщеннях.

Для розв’язання поставлених задач використовувалися методи аналізу бездротових мереж, цифрової обробки сигналів, статистичного аналізу, моделювання кіберфізичних систем та експериментального оцінювання.

За темою кваліфікаційної роботи опубліковано одну публікацію [81] тези у 17-й Міжнародній студентській науковотехнічній конференції «Перспективні мережеві та комп’ютерні технології» – ПЕРСИК 2026 (м. Харків, 23 квіт. 2026). Харків, 2026.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Обґрунтування актуальності та аналіз стану задачі

Проблема прихованого відеоспостереження в приміщеннях набуває системного характеру через мініатюризацію камер, масове поширення Wi-Fi інфраструктури та здешевлення апаратних платформ для потокової передачі відео. У сучасних дослідженнях DIFFLOC ця проблема розглядається не лише як задача виявлення пристрою, а як задача його просторової локалізації за змінами радіоканалу [1]. Сучасна прихована камера може бути виконана у формі зарядного пристрою, годинника, датчика, декоративного елемента або мініатюрного автономного модуля. Наявність відкритих експериментальних матеріалів і наборів даних до DIFFLOC підтверджує, що такі сценарії вже аналізуються як практична задача безпеки приміщень [2].

Своєчасне виявлення прихованої камери є важливим не тільки з правової, а й з інженерної точки зору, оскільки користувач часто не має доступу до точки доступу, пароля адміністратора або технічної інформації про пристрій. Подальший розвиток підходу DiffLoc показує необхідність підвищення стійкості локалізації у складних реальних умовах [3]. На рисунку 1.1 зображено приклад такої Wi-Fi камери, а саме - Mini A9 IP Wi-Fi.

Рисунок 1.1 - Приклад мініатюрної Wi-Fi камери [82]

Традиційні засоби пошуку, зокрема ручний огляд, використання ліхтарів, оптичних детекторів, тепловізорів або індикаторів випромінювання, залежать від досвіду оператора та не завжди дають просторову оцінку положення камери. Метод LocCams [4] демонструє, що для локалізації прихованих бездротових камер перспективним є використання звичайних комерційних пристроїв і параметрів Wi-Fi каналу.

Окрема складність полягає в тому, що користувачеві зазвичай потрібно не просто встановити факт наявності камери, а визначити напрямок пошуку в кімнаті. У роботі CamLoPA запропоновано розглядати просторове положення прихованої камери через аналіз шляху поширення сигналу [5], що безпосередньо відповідає задачам цього дослідження.

Стан наукових досліджень показує, що приховані Wi-Fi камери можуть бути локалізовані без розкриття їхнього програмного забезпечення, якщо правильно використати закономірності радіопоширення. Матеріали конференції ACM SenSys щодо Hidden WiFi Camera Localization підкреслюють значення фізично інтерпретованих методів замість суто емпіричного пошуку [6].

Актуальність роботи посилюється тим, що приховані пристрої Інтернету речей можуть бути різними за виробником, форм-фактором, режимом живлення та мережевою поведінкою. Система Lumos [7] показує, що для ідентифікації й локалізації прихованих IoT-пристроїв потрібне поєднання радіоаналізу та практичного сценарію перевірки приміщення. Приховані сенсори та камери створюють загрозу не тільки приватності, а й інформаційній безпеці організацій, переговорних кімнат і тимчасово орендованих просторів. Дослідження SNOOPDOG [8] доводить, що нелегальні бездротові сенсори можуть бути виявлені, ідентифіковані та локалізовані на основі аналізу бездротового середовища .

Порівняно з ручним оглядом приміщення, радіоканальний підхід дозволяє зменшити кількість об’єктів, які потрібно перевірити фізично. MotionCompass показує, що зміни мережевого трафіку, спричинені рухом у полі зору камери, можуть бути використані для виявлення підозрілих пристроїв [9].

Отже, актуальність дослідження визначається суперечністю між потребою у швидкій, недорогій і відтворюваній локалізації прихованих Wi-Fi камер та обмеженнями традиційних засобів пошуку. Сучасні роботи з аналізу прихованих бездротових камер підтверджують, що ця задача залишається відкритою для подальшого інженерного вдосконалення.

Таблиця 1.1 - Обґрунтування актуальності теми дослідження кіберфізичної системи виявлення та локалізації прихованих Wi-Fi камер

№	Компонент актуальності	Прояв у предметній області	Практичний наслідок
1.	Соціальна значущість	Ризик порушення приватності у житлі, готелях, офісах і переговорних	Потреба у швидкій перевірці приміщення
2.	Технічна новизна	CSI та керована дифракція замість дорогих сенсорів	Недорогий переносний прототип
3.	Прикладна цінність	Оцінка напряму на камеру, а не лише факту виявлення	Скорочення часу ручного пошуку

1.2 Проблема, мета та задачі дослідження

Основна проблема дослідження полягає у створенні системи, яка здатна виявляти та локалізувати приховану Wi-Fi камеру без доступу до її облікового запису, мобільного застосунку або мережевої інфраструктури. Праці з аналізу бездротових прихованих камер [11] підкреслюють, що пасивне спостереження за трафіком може бути використане як початковий етап такої перевірки.

Метою роботи є розроблення архітектури кіберфізичної системи, яка поєднує пасивний аналіз параметрів радіоканалу, виділення підозрілих пристроїв і азимутальну локалізацію джерела Wi-Fi сигналу. Трафікові підходи до пошуку прихованих камер показують, що відеопередавання залишає характерні статистичні ознаки у бездротовому середовищі [12]. Для досягнення мети необхідно розв’язати задачу попереднього виявлення пристроїв, які можуть бути прихованими камерами, за розміром, кількістю і напрямом передавання пакетів. Метод стимулювання та зондування трафіку доводить, що реакція відеопотоку на зміну сцени може бути використана для підтвердження підозрілого пристрою [13].

Наступною задачею є перехід від виявлення до локалізації, тобто визначення напряму, у якому потрібно шукати прихований об’єктив або корпус пристрою. Роботи з локалізації прихованих Wi-Fi камер показують, що одних лише мережевих ознак недостатньо для повного вирішення просторової задачі [14]. Окремою задачею є формування вимог до системи, яка має працювати у житлових кімнатах, офісах, готельних номерах, гуртожитках та коворкінгах без складної підготовки середовища. Дослідження Hidden Webcams [15] демонструє доцільність використання подібності спостережень і непрямих ознак для пошуку прихованих камер.

У межах роботи також потрібно обґрунтувати, чому саме параметри фізичного шару Wi-Fi можуть бути використані як джерело інформації про положення камери. Підхід SpyDir [16] підтверджує, що напрямок на шпигунський пристрій може бути оцінений за радіосигнальними характеристиками без прямого фізичного контакту з пристроєм.

Важливою задачею є забезпечення легкості прототипу, щоб система могла бути використана не тільки в лабораторії, а й у звичайному приміщенні. Сучасні легкі методи виявлення та локалізації прихованих камер орієнтуються саме на зменшення складності апаратури та дій користувача [17]. Додатково необхідно врахувати роботу системи у реальному часі, оскільки користувачеві потрібна швидка відповідь про можливий напрямок пошуку. Система Wireless Spy Camera

Spotter [18] показує практичну цінність поєднання аналізу трафіку та трасування Wi-Fi сигналу в реальному часі.

Для перевірки запропонованого підходу потрібно визначити критерії ефективності: точність азимуту, час перевірки, кількість помилкових спрацювань, стійкість до багатопроменевості та зручність використання. У роботах із виявлення прихованих камер за мережевим трафіком саме ці параметри розглядаються як практично важливі для кінцевої системи [19].

Таким чином, задачі дослідження охоплюють аналіз предметної області, порівняння методів, вибір фізичної основи, побудову архітектури, формування алгоритму виявлення, локалізації та оцінювання результатів. Реальні дослідження активності смарт-камер за зашифрованим Wi-Fi трафіком [20] підтверджують, що навіть без доступу до вмісту пакетів можна отримати корисні ознаки поведінки камери.

1.3 Порівняльний аналіз переваг та недоліків існуючих рішень

Існуючі методи локалізації бездротових пристроїв можна поділити на оптичні, теплові, електромагнітні, мережево-трафікові та методи фізичного шару Wi-Fi. Узагальнені огляди з бездротової внутрішньої локалізації показують, що точність методу значною мірою залежить від типу вимірюваного параметра та умов середовища [21].

Оптичні методи мають перевагу прямого виявлення об’єктива, але вони вимагають послідовного огляду поверхонь, правильного кута підсвічування та часто не працюють для камер, захованих за напівпрозорими або декоративними елементами. На відміну від цього, Wi-Fi sensing використовує не візуальний образ, а зміну канального стану, що робить підхід корисним у прихованих сценаріях [22]. Теплові та електромагнітні методи можуть працювати незалежно від мережевого протоколу, однак часто потребують дорогого обладнання та чутливі до сторонніх джерел тепла або випромінювання. Огляди CSI-локалізації [23] підкреслюють, що

Wi-Fi сигнали можуть забезпечити додатковий рівень аналізу без спеціалізованих тепловізійних систем.

Методи RSSI простіші у реалізації, але вони дають лише інтегральну оцінку сили сигналу, яка сильно залежить від відбиттів, положення антен і перешкод. У сучасних дослідженнях CSI [24] розглядається як інформативніший параметр, оскільки він містить амплітудно-фазову інформацію по піднесучих.

Суттєвим недоліком багатьох підходів є низька узагальнюваність: система, налаштована в одному приміщенні, може працювати гірше в іншому через зміну меблів, стін, відбиттів і положення людей. Огляди Wi-Fi sensing generalizability показують, що ця проблема є однією з ключових для практичного впровадження систем на основі CSI [25]. Використання CSI стало можливим завдяки появі інструментів, які дозволяють отримувати низькорівневу інформацію з комерційних Wi-Fi адаптерів. Перші практичні інструменти для збору 802.11n CSI заклали основу для багатьох подальших досліджень у сфері Wi-Fi sensing [26].

Суттєвий внесок у розвиток цієї тематики зробили платформи, які дають змогу отримувати CSI з сучасніших чипсетів без дорогого лабораторного обладнання. Платформа Free Your CSI показала, що сучасні Wi-Fi чипи можуть бути використані як вимірювальна база для експериментів із радіоканалом [27].

Для практичної реалізації прототипу важливим є доступ до прошивки та можливість модифікації роботи бездротового інтерфейсу. Проєкт Nexmon [28] надає засоби патчування прошивок Broadcom/Cypress, що є важливим для експериментів із низькорівневими параметрами Wi-Fi. Окрему роль у запропонованій архітектурі відіграє nexmon_csi, [29] який дозволяє отримувати оцінки канального стану на Raspberry Pi та сумісних пристроях. Саме цей інструмент робить можливим побудову недорогого прототипу без використання спеціалізованого SDR-обладнання.

Порівняння наявних рішень показує, що найперспективнішим для цієї роботи є поєднання трафікового виявлення і CSI-локалізації (табл. 1.2). Дослідження збору CSI на Wi-Fi точках доступу підтверджують, що такі дані можуть збиратися у практичних умовах для задач sensing та локалізації [30].

Таблиця 1.2 - Порівняльна характеристика методів виявлення та локалізації прихованих камер

№	Метод	Вартість	Навчання	Вимоги до простору	Особливість
1.	Оптичні методи	Середня/висока	Ні	Низькі	Пошук відблисків і лінз
2.	Теплові методи	Висока	Ні	Низькі	Потребують тепловізора
3.	RSSI	Низька	Ні	Середні	Груба оцінка сили сигналу
4.	LocCams	Низька	Так	Низькі	Потрібні CSI-відбитки
5.	CamLoPA	Низька	Ні	Середні	Залежність від траєкторії руху
6.	DIFFLOC	Низька	Ні	Низькі	Керована дифракція

1.4 Концепція побудови кіберфізичної системи

Запропонована система розглядається як кіберфізична, оскільки вона поєднує фізичну дію на радіоканал і цифрову обробку отриманих сигналів. Практичні інструкції зі збору Wi-Fi CSI показують, що навіть на доступних платформах можна організувати експериментальний цикл збирання та аналізу канальних даних [31].

Перший контур системи виконує пасивне спостереження за Wi-Fi середовищем і виділяє пристрої, поведінка яких схожа на передавання відеопотоку. Дослідження розпізнавання активності за CSI підтверджують, що зміни радіоканалу можуть відображати фізичні процеси у приміщенні [32].

Другий контур системи відповідає за азимутальну локалізацію підозрілого джерела сигналу. Методи device-free localization за CSI показують, що навіть без активної взаємодії з цільовим пристроєм можна оцінювати зміни просторового положення або стану середовища [33]. Кіберфізична логіка системи полягає в тому, що програма не просто спостерігає за сигналом, а керує механічним елементом, який створює контрольовану зміну умов поширення хвилі. Аналогічний принцип непрямого вимірювання використовується у Wi-Fi системах моніторингу стану людини, де фізичні процеси відображаються у параметрах радіоканалу [34].

У запропонованому рішенні користувач розміщує пристрій у приміщенні, запускає сканування, отримує список підозрілих MAC-адрес і для кожної цілі виконує локалізацію. Дослідження відстеження життєвих показників через Wi-Fi [35] демонструють, що сталі та повторювані зміни сигналу можуть бути використані як вимірювальна ознака.

Перевага такої концепції полягає в тому, що користувачеві не потрібно обходити всі стіни, рухатися за складною траєкторією або оглядати кожен предмет у кімнаті. Роботи з високочутливого аналізу Wi-Fi сигналів показують, що радіоканал здатний фіксувати навіть незначні зміни середовища, якщо правильно обробляти дані [36]. Система повинна працювати в умовах багатопроменевості, коли сигнал відбивається від стін, меблів, металевих поверхонь і побутових предметів. Моделі розпізнавання активності людини за Wi-Fi сигналами [37] підкреслюють необхідність фільтрації шуму та відокремлення корисної ознаки від випадкових коливань.

На відміну від методів машинного навчання, які потребують навчальних наборів даних для конкретного середовища, дифракційний підхід спирається на фізичну закономірність проходження перешкоди через зону Френеля [38]. Роботи

з ідентифікації ходи за Wi-Fi показують потенціал радіосигналів, але водночас демонструють залежність багатьох ML-рішень від умов навчання.

Концептуально запропонована система працює як активний експериментальний стенд: вона створює контрольовану зміну радіоканалу і фіксує її у вигляді провалу CSI [39]. Подібна ідея використання Wi-Fi сигналів для віддаленого сприйняття середовища лежить в основі систем розпізнавання жестів у приміщенні.

Таким чином, кіберфізична система має три ключові функції: виявлення кандидата, створення контрольованого впливу та обчислення азимуту. Дослідження 3D-відстеження [40] за радіовідбиттями підтверджують, що фізична інтерпретація сигналу є важливою умовою для побудови надійних просторових оцінок.

1.5 Фізичні основи використання CSI та дифракції

Фізичною основою запропонованого підходу є поширення електромагнітної хвилі між передавачем і приймачем у приміщенні. Дослідження смарт-приміщень, які відстежують дихання та серцевий ритм за радіосигналами, показують, що Wi-Fi хвилі можуть нести інформацію про фізичні процеси без прямого контакту з об’єктом [41].

Wi-Fi сигнал поширюється не тільки вздовж геометричної прямої, а й у просторовій області, що описується зонами Френеля. У задачах внутрішньої локалізації багатопроменевість часто вважається проблемою, однак при правильній постановці експерименту вона може бути врахована в алгоритмі обробки [42].

CSI містить амплітуду та фазу піднесучих, тому дає детальнішу інформацію, ніж звичайний RSSI. Системи на зразок SpotFi доводять, що комерційний Wi-Fi може забезпечити достатню просторову роздільну здатність для високоточної локалізації [43].

Коли металева пластина перетинає першу зону Френеля між камерою та приймачем, частина енергії хвилі екранується або дифрагує, а на графіку CSI

виникає характерний провал. Ідея використання антенної обробки та фазових характеристик у ArrayTrack [44] показує, що просторові параметри сигналу можуть бути виділені навіть на основі звичайного Wi-Fi обладнання.

Особливість DIFFLOC полягає в тому, що пластина не рухається довільно, а обертається навколо приймача, створюючи симетричний процес перетину зони Френеля. Дослідження Phaser підтверджує важливість фазової та антенної обробки для перетворення Wi-Fi сигналів на джерело просторової інформації [45]. Для підвищення точності важливо не тільки зафіксувати мінімум амплітуди, а й правильно зіставити його з часовою міткою та кутом повороту пластини. Методи точного профілювання затримок у Wi-Fi показують, що дрібні часові та просторові характеристики сигналу можуть бути відновлені з комерційних пристроїв [46].

У реальних приміщеннях сигнал може відбиватися від багатьох поверхонь, тому CSI містить як корисну, так і завадову складові. Дослідження IndoTrack [47] демонструє, що device-free відстеження в приміщенні потребує спеціальної обробки багатопроменевих компонентів. Дифракційне ослаблення є корисним саме тому, що воно формується контрольовано, а не випадково. Методи пасивного виявлення рухомих цілей за фізичним шаром Wi-Fi показують, що динамічні зміни каналу можуть бути використані для виділення подій у середовищі [48].

Якщо система знаходить два близькі провали або один домінуючий мінімум, локалізаційний момент визначається як середина області найбільшого ослаблення або найнижча точка кривої. У системі Widar також використовується аналіз швидкісних і часових характеристик Wi-Fi сигналу для пасивного відстеження, що підтверджує доцільність такого підходу [49].

Отже, використання CSI та дифракції переводить задачу локалізації з рівня суб’єктивного огляду до рівня контрольованого фізичного експерименту. Дослідження крос-доменної узагальнюваності Wi-Fi жестів підкреслює, що фізично обґрунтовані ознаки є стійкішими, ніж ознаки, підібрані лише статистично [50].

Прототип схеми DIFFLOC зображено на рис. 1.2.

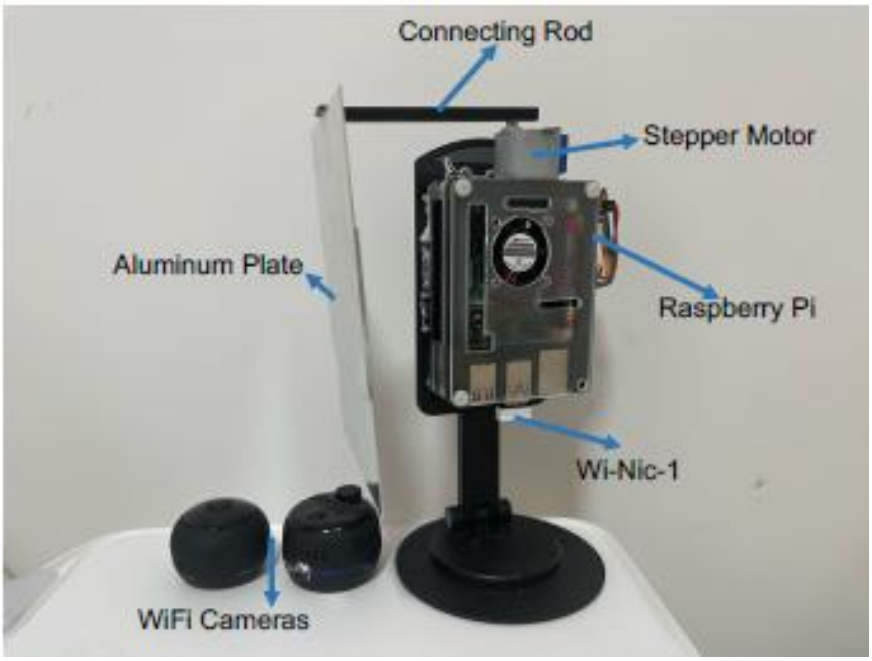


Рисунок 1.2 - Приклад прототипу системи з дифракційним елементом

1.6 Апаратно-програмна архітектура системи

Апаратна архітектура системи орієнтована на використання доступних компонентів: Raspberry Pi [83] (зображений на рис. 1.3), Wi-Fi адаптерів, крокового двигуна, драйвера ULN2003, металевої пластини та опорного механізму.

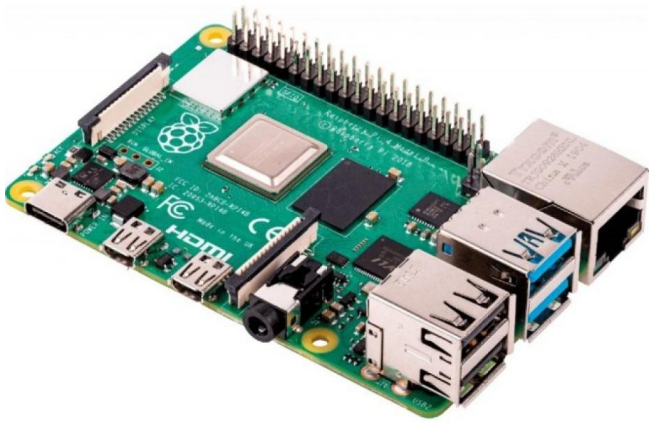


Рисунок 1.3 – Мікрокомп’ютер Raspberry Pi 4 Model B [83]

Дослідження BreathTrack [51] підтверджує, що звичайні Wi-Fi пристрої можуть бути використані як сенсорна база для вимірювання фізичних процесів.

Raspberry Pi обрано як центральний обчислювальний вузол через відкритість платформи, можливість роботи з Linux, Python, драйверами та monitor mode. Подібний підхід використовується в Anti-Fall [52], де недороге Wi-Fi обладнання виконує роль сенсорної системи для реального часу.

Програмна частина системи включає модулі сканування каналів, перехоплення пакетів, фільтрації трафіку, збору CSI, керування двигуном, синхронізації часових міток і обчислення азимуту. У системі WiGest показано, що для практичних Wi-Fi sensing [53] рішень важлива повна програмна схема від збору сигналу до інтерпретації результату.

Механічна частина забезпечує контрольований рух металевої пластини у визначеному секторі. Дослідження RF-sensing активностей із некооперативними суб'єктами підтверджує, що радіоканал може відображати фізичні зміни середовища навіть без активної участі цільового об'єкта [54]. Система повинна зберігати часові мітки кожного кроку двигуна, щоб потім зіставити положення пластини з мінімумом CSI. У радіотомографічних і device-free системах така синхронізація вимірювань є ключовою умовою для коректної реконструкції подій [55].

Інформаційний потік у системі починається з пасивного збирання 802.11 кадрів і завершується видачею користувачу напряму на підозрілу камеру. У класичних device-free підходах [56] також підкреслюється, що об'єкт може бути виявлений за змінами радіосередовища без власного передавача або спеціальної мітки. Для експериментальної перевірки важливо оцінити роботу системи в умовах різної геометрії кімнати, розташування меблів і кількості відбивних поверхонь. Радіотомографічні методи демонструють, що просторові зміни радіосигналу можуть бути використані для побудови уявлення про події в середовищі [57].

Перевагою запропонованої системи є те, що вона не потребує побудови повної карти приміщення, а видає практично корисний азимутальний напрямок.

Системи відстеження руху через стіни за радіотомографією показують, що навіть обмежені радіовимірювання можуть мати високу прикладну цінність [58].

У порівнянні з класичними методами позиціювання на основі відбитків сигналу, запропонований підхід менше залежить від попереднього навчання в конкретному приміщенні. Система RADAR [59] показала ефективність RF-відбитків для внутрішнього позиціювання, але також продемонструвала потребу в попередньому зборі даних для конкретного середовища.

Таким чином, апаратно-програмна архітектура має бути недорогою, мобільною, відтворюваною та достатньо відкритою для подальшого вдосконалення. Огляди бездротових методів внутрішнього позиціювання підтверджують, що вибір апаратної платформи та типу вимірюваного сигналу визначає практичну придатність системи [60]. На рис. 1.4 зображено приклад складеної системи DIFFLOC.

Рисунок 1.4 - Складений прототип апаратно-програмної системи

1.7 Методика виявлення, локалізації та реалізація прототипу

Методика роботи системи починається зі сканування Wi-Fi середовища і групування перехоплених пакетів за MAC-адресами. Основи бездротового зв’язку пояснюють, що рівень прийнятого сигналу, втрати на трасі та багатопроменевість є природними факторами, які впливають на будь-яку систему радіолокалізації [61].

Після первинного сканування система аналізує середній розмір пакетів, кількість переданих data frames [62] і співвідношення висхідного та низхідного

трафіку. Теорія бездротових комунікацій показує, що статистичні властивості каналу та передавання можуть бути використані для оцінювання поведінки пристроїв.

Кандидатами на приховану камеру вважаються пристрої, які стабільно передають значний обсяг даних і реагують на зміну руху в контрольованій області. Моделі сучасних бездротових систем підкреслюють, що відеопотоки формують характерне навантаження на канал зв’язку [63].

Після вибору цільової MAC-адреси система переходить до збору CSI на відповідному каналі. Основи теорії бездротового зв’язку пояснюють, що OFDM-канал може бути представлений набором піднесучих, кожна з яких має власну амплітудно-фазову характеристику [64]. На етапі цифрової обробки сигналу виконується фільтрація шуму, згладжування часових рядів і пошук локальних мінімумів. Класичні методи цифрового зв’язку показують, що правильна обробка шумових сигналів є необхідною умовою достовірного виділення корисної ознаки [65].

Для обробки CSI доцільно застосовувати методи дискретної фільтрації, усереднення та відбору найбільш інформативних піднесучих. Основи дискретної обробки сигналів дають математичний апарат для згладжування, спектрального аналізу та зменшення випадкових коливань у вимірюваннях.

Після знаходження мінімуму система зіставляє його часову мітку з журналом крокового двигуна. У теорії комунікаційних систем синхронізація часових подій є критичною для коректного приймання, вимірювання та інтерпретації сигналів.

Отриманий кут повороту пластини розглядається як оцінка азимуту на джерело Wi-Fi сигналу, тобто на потенційну приховану камеру. У цифрових комунікаціях просторові та часові параметри каналу розглядаються як важливі характеристики передавання, що можуть використовуватися не лише для зв’язку, а й для вимірювання.

Під час реалізації прототипу необхідно враховувати роботу антен, орієнтацію приймача, частотний діапазон 2,4 або 5 ГГц та можливі втрати на перешкодах.

Основи мікрохвильової інженерії пояснюють, як геометрія середовища, екрани та провідні об’єкти впливають на поширення електромагнітної хвилі.

Оскільки результат залежить від антени приймача та її взаємодії з навколишнім середовищем, у прототипі потрібно забезпечити стабільне положення системи під час вимірювання. Теорія антен показує, що напрямленість, поляризація й ефективність антени можуть суттєво впливати на форму прийнятого сигналу.

1.8 Висновки та постановка задачі

У першому розділі встановлено, що локалізація прихованих Wi-Fi камер є складною міждисциплінарною задачею, яка поєднує інформаційну безпеку, бездротовий зв’язок, цифрову обробку сигналів і фізику поширення хвиль. Теорія оптики та дифракції пояснює фундаментальну природу ослаблення сигналу під час проходження перешкоди через область поширення хвилі.

Проведений аналіз показав, що дифракційний підхід має перевагу над суто емпіричними методами, оскільки результат локалізації має фізичне пояснення. Математичні основи Фур’є-оптики дозволяють обґрунтувати зв’язок між геометрією перешкоди, хвильовим фронтом і просторовим розподілом енергії.

Визначено, що зона Френеля є ключовим поняттям для пояснення того, чому металева пластина здатна створювати вимірюваний провал CSI. Класичні положення оптики описують дифракцію, інтерференцію та поширення хвиль, що є теоретичною базою для запропонованого підходу.

У межах постановки задачі потрібно враховувати стандартизовану структуру Wi-Fi кадрів, канали, режими роботи та фізичний рівень 802.11. Стандарт IEEE 802.11 визначає основні механізми бездротової локальної мережі, на яких базується перехоплення кадрів і аналіз радіоканалу.

Система має бути придатною до роботи з сучасними високоефективними Wi-Fi мережами, де змінюються параметри доступу до середовища та фізичного рівня. Стандарт IEEE 802.11ax описує розвиток Wi-Fi у напрямі вищої ефективності, що потрібно враховувати під час подальшої адаптації системи.

У перспективі запропонована система може бути інтегрована з іншими бездротовими сенсорними або IoT-рішеннями, що потребує врахування суміжних стандартів низькошвидкісних мереж. Стандарт IEEE 802.15.4 є важливим для розуміння архітектури багатьох IoT-пристроїв, які можуть співіснувати з Wi-Fi середовищем.

Оскільки приховане відеоспостереження прямо пов’язане з ризиками для приватності та інформаційної безпеки, результати роботи мають відповідати загальним підходам до управління захистом інформації. ISO/IEC 27001 визначає вимоги до систем управління інформаційною безпекою, що є корисним контекстом для практичного застосування системи.

Для впровадження рішення в організаціях важливо враховувати не лише технічну точність, а й процедури контролю, оцінювання ризиків і захисту персональних даних. ISO/IEC 27002 містить набір засобів контролю інформаційної безпеки, які можуть бути використані як організаційне доповнення до технічної системи пошуку камер.

Оскільки значна частина прихованих камер належить до категорії споживчих IoT-пристроїв, система повинна враховувати типові ризики таких виробів: слабке налаштування, віддалений доступ, постійне передавання даних і недостатній захист. ETSI EN 303 645 визначає базові вимоги кібербезпеки для споживчого Інтернету речей і є важливим нормативним орієнтиром.

Підсумовуючи, у роботі поставлено задачу розробити кіберфізичну систему, яка виявляє підозрілий Wi-Fi пристрій за трафіковими ознаками, формує контрольований дифракційний вплив на радіоканал, аналізує CSI та видає користувачеві азимутальний напрямок пошуку. Закон України «Про захист персональних даних» підкреслює суспільну значущість технічних рішень, спрямованих на запобігання несанкціонованому збиранню відеоінформації про людину.

2 МОДЕЛІ ТА МЕТОДИ ВИЯВЛЕННЯ І ЛОКАЛІЗАЦІЇ ПРИХОВАНИХ WI-FI КАМЕР

2.1 Обґрунтування вибору теоретичних та експериментальних методів дослідження

Обґрунтування моделей, методів і засобів, які використовуються для розв’язання задачі виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу є ключовими пунктами. У цьому розділі основну увагу приділено не лише опису відомих рішень, а й побудові власної логіки дослідження: від вибору фізичної моделі поширення сигналу до розроблення методики комп’ютерного та натурного моделювання.

Об’єктом моделювання є процес зміни параметрів Wi-Fi радіоканалу між прихованою камерою, що виконує передавання даних, і пасивним приймачем кіберфізичної системи. Предметом моделювання є закономірність між контрольованим механічним впливом на радіоканал, змінами амплітуди CSI та оцінкою азимутального напряму на передавач.

Вибір методів дослідження зумовлений складністю предметної області. Прихована Wi-Fi камера є одночасно електронним пристроєм, мережевим вузлом, джерелом бездротового сигналу та фізичним об’єктом, замаскованим у приміщенні. Тому для її локалізації недостатньо лише мережевого аналізу або лише візуального огляду.

Теоретичні методи дослідження застосовуються для формалізації фізичних процесів, які лежать в основі локалізації. До них належать аналіз зон Френеля, дифракції електромагнітних хвиль, багатопроменевого поширення сигналу, параметрів CSI та залежності амплітуди каналу від положення перешкоди.

Експериментальні методи потрібні для перевірки працездатності моделі в умовах, наближених до реальних. У приміщенні радіоканал майже ніколи не є ідеальним: сигнал відбивається від стін, меблів, металевих предметів, побутової техніки та тіла людини. Тому навіть правильна теоретична модель може давати

похибку, якщо не врахувати шум, нестабільність пакетного потоку, зміни орієнтації антени та випадкові перешкоди.

Основними методами теоретичного дослідження є системний аналіз, абстрагування, формалізація, математичне моделювання та порівняльний аналіз. Системний аналіз дає змогу розглядати комплекс як сукупність взаємопов’язаних підсистем: підсистеми збирання Wi-Fi пакетів, підсистеми вилучення CSI, підсистеми керування дифракційним елементом, підсистеми обробки сигналів і підсистеми відображення результату.

Формалізація потрібна для перетворення фізичного опису на математичні залежності. У межах дослідження формалізуються такі величини: кутове положення металевої пластини, часова мітка пакета, амплітуда CSI, середній рівень сигналу, глибина провалу, тривалість інтервалу максимального ослаблення та оцінений азимут. Важливо, що ці величини мають бути вимірюваними або обчислюваними.

Математичне моделювання використовується для опису зв’язку між положенням перешкоди та зміною каналу. Базова ідея полягає в тому, що Wi-Fi сигнал поширюється не лише по геометричній прямій, а в межах першої зони Френеля, де зосереджується істотна частина енергії. Коли металева пластина проходить через цю область, виникає дифракційне ослаблення.

Експериментальні методи включають стендові вимірювання, повторювані серії спостережень, варіювання умов приміщення, статистичне порівняння результатів і аналіз похибки. Стендові вимірювання дають змогу отримати первинні дані CSI при контрольованому обертанні пластини. Повторювані серії потрібні для перевірки стабільності: один успішний вимір не доводить працездатності системи.

Важливим є вибір критерію ефективності. Для фази виявлення доцільно використовувати показники правильного виявлення підозрілих пристроїв, хибних спрацювань і пропусків. Для фази локалізації основним показником є кутова похибка, тобто різниця між фактичним азимутом камери і азимутом, оціненим системою.

Доцільність використання персонального комп’ютера або одноплатного комп’ютера обґрунтовується потребою в автоматизованій обробці великої кількості вимірювань. Один цикл локалізації може містити сотні або тисячі пакетів, для кожного з яких фіксуються амплітуди піднесучих, часові мітки та службова інформація. Ручна обробка таких даних неможлива.

У межах дипломної роботи доцільно розглядати персональний комп’ютер як засіб моделювання і аналізу, а одноплатний комп’ютер типу Raspberry Pi як засіб реалізації кіберфізичного прототипу. Персональний комп’ютер зручний для побудови графіків, порівняння варіантів фільтрації та документування результатів.

Методологічна особливість дослідження полягає в тому, що локалізація розглядається не як задача точного визначення координат у декартовій системі, а як задача оцінки азимутального напряму. Такий вибір відповідає практичній меті.

Таким чином, для дослідження обрано комплекс методів, що поєднує фізичне моделювання, алгоритмічну обробку CSI, комп’ютерне моделювання та натурну перевірку. Такий набір методів відповідає природі задачі, оскільки прихована Wi-Fi камера проявляє себе не тільки в мережевому трафіку, а й у параметрах радіоканалу.

2.2 Структурна модель кіберфізичної системи та зв’язок «модель – метод – засіб»

Структурна модель кіберфізичної системи описує склад компонентів, інформаційні потоки між ними та функціональні ролі кожного елемента. На верхньому рівні система складається з фізичного середовища, прихованої Wi-Fi камери, пасивного приймача, керованого дифракційного модуля, обчислювального блоку та модуля інтерпретації результату.

Пасивний приймач виконує збирання інформації про радіоканал без активної взаємодії з камерою. Це принципово важливо, оскільки користувач не має прав адміністратора мережі зловмисника і не повинен надсилати камері службові або

тестові пакети. Приймач працює в режимі моніторингу, перехоплює пакети цільової MAC-адреси та отримує CSI.

Керований дифракційний модуль створює передбачувану зміну радіоканалу. Його основними елементами є кроковий двигун, драйвер керування, механічний тримач і металева пластина. Пластина виконує роль контрольованої перешкоди, а кроковий двигун забезпечує відому кутову траєкторію.

Обчислювальний блок координує роботу сенсорної та виконавчої частин. Він запускає збирання CSI, задає швидкість і діапазон обертання пластини, фіксує часові мітки, зберігає вимірювання та виконує післяобробку. У прототипі цю функцію може виконувати Raspberry Pi або персональний комп’ютер з підключеними адаптерами.

Зв’язок «модель – метод – засіб» у цій системі можна подати у вигляді послідовності. Фізична модель стверджує, що проходження металевої пластини через першу зону Френеля викликає дифракційне ослаблення сигналу. Метод локалізації пропонує обертати пластину навколо приймача, знаходити інтервал максимального ослаблення CSI та зіставляти його середину з азимутом на камеру.

У структурній моделі доцільно виділити дві підсистеми: підсистему виявлення та підсистему локалізації. Підсистема виявлення працює з мережевими ознаками. Вона сканує Wi-Fi канали, групує пакети за MAC-адресами, відкидає службові кадри та аналізує інтенсивність висхідного трафіку. Пристрої, що демонструють характерні ознаки відеопередавання, потрапляють до списку кандидатів.

Такий поділ зменшує обчислювальне навантаження. Немає потреби виконувати повний цикл локалізації для кожного Wi-Fi пристрою, що присутній у приміщенні. Спочатку відсіюються очевидно безпечні пристрої, наприклад точки доступу, телефони без активного відеопотоку або пристрої з незначним трафіком. Лише після цього ресурси витрачаються на більш складну фазу локалізації.

Вхідними даними структурної моделі є набір Wi-Fi пакетів, CSI-вимірювання, часові мітки, кутові положення пластини та налаштування експерименту. Вихідними даними є список підозрілих пристроїв, оцінений азимут

для кожної цілі, показник довіри до результату та службова інформація про якість вимірювання. Показник довіри може враховувати кількість пакетів, глибину провалу, узгодженість результатів у повторних циклах і рівень шуму.

Функціональна модель системи включає такі етапи: сканування доступних каналів; визначення підозрілих MAC-адрес; вибір цільового пристрою; запуск обертання пластини; синхронне збирання CSI; попередня обробка сигналу; виявлення інтервалу максимального ослаблення; розрахунок азимуту; відображення напряму користувачеві; за потреби повторний вимір. Така послідовність забезпечує завершений цикл роботи від невідомої мережевої ситуації до практичної підказки для пошуку камери.

У структурній моделі важливо врахувати обмеження з боку апаратури. Wi-Fi адаптер повинен підтримувати режим моніторингу та можливість отримання CSI. Не всі комерційні адаптери придатні для цього. Також потрібно врахувати, що один мережевий інтерфейс може бути зайнятий вилученням CSI, тому для службового зв’язку або паралельного перехоплення пакетів може знадобитися додатковий адаптер.

Механічна частина також є суттєвою. Металева пластина повинна мати розміри, порівнянні з довжиною хвилі або більші за неї, щоб викликати помітну дифракцію. Для частоти 2,4 ГГц довжина хвилі становить приблизно 12,5 см, а для 5 ГГц – приблизно 6 см. Тому пластина шириною близько 10 см є компромісом: вона достатньо велика для створення ослаблення, але залишається компактною для переносного пристрою.

Інформаційні зв’язки в системі мають часову природу. Кожне CSI-вимірювання повинно бути пов’язане з моментом часу, а кожен момент часу – з кутовим положенням пластини. Якщо синхронізація порушена, то мінімум сигналу буде зіставлено з неправильним кутом. Тому в програмній реалізації доцільно вести журнал подій: запуск двигуна, номер кроку, розрахований кут, час прийому пакета, амплітуда CSI та результат фільтрації.

Структурна модель також повинна враховувати середовище застосування. У кімнаті можуть бути декілька точок доступу, декілька камер, інші користувачі Wi-

Fi та рухомі об’єкти. Через це система не повинна спиратися на припущення про ідеальну тишу радіоефіру. Навпаки, вона має бути здатною працювати за умов часткового шуму.

З погляду кіберфізичної архітектури система має замкнений контур дії. У табл. 2.1 можна побачити відповідність між моделлю, методом і засобом реалізації. Цифровий блок керує двигуном, двигун змінює фізичне положення пластини, пластина змінює радіоканал, радіоканал відображається у CSI, CSI аналізується програмою, а результат впливає на рішення користувача щодо подальшого пошуку. Такий контур підтверджує, що система не є лише програмним аналізатором мережі.

Таблиця 2.1 – Відповідність між моделлю, методом і засобом реалізації

№	Компонент моделі	Метод дослідження	Засіб реалізації
1.	Поширення Wi-Fi сигналу	Аналіз зони Френеля і дифракції	Теоретичні розрахунки, модель радіоканалу
2.	Зміна CSI під час ослаблення	Цифрова обробка сигналів	Python, NumPy, фільтрація часових рядів
3.	Керований рух перешкоди	Механічне позиціювання	Кроковий двигун, драйвер, металева пластина
4.	Виділення підозрілих пристроїв	Аналіз мережевого трафіку	Wi-Fi адаптер у monitor mode, фільтрація MAC-адрес
5.	Оцінювання азимуту	Пошук середини інтервалу максимального ослаблення	Програмний модуль локалізації

Отже, структурна модель задає логіку побудови системи і визначає, які дані потрібні для подальшого математичного моделювання. Вона показує, що

ефективність рішення залежить не від одного алгоритму, а від узгодженості апаратних, програмних і фізичних компонентів. Саме тому подальша математична модель повинна бути достатньо простою для практичної реалізації, але достатньо змістовною для пояснення реальних змін CSI.

2.3 Математична модель радіоканалу, CSI та керованої дифракції

Математична модель радіоканалу потрібна для кількісного опису того, як прихована Wi-Fi камера проявляється у вимірюваннях приймача. У стандартних бездротових мережах сигнал між передавачем і приймачем проходить через складне середовище, у якому існують пряма траєкторія, відбиття, розсіювання та дифракція. Channel State Information відображає комплексну частотну характеристику каналу для піднесучих OFDM.

$$H(f) = |H(f)|e^{j\theta(f)} \tag{2.1}$$

де $H(f)$ – комплексна частотна характеристика радіоканалу на частоті f;
$|H(f)|$ – амплітуда CSI;
$\theta(f)$ – фаза CSI на частоті f;
j – уявна одиниця.

Для задачі локалізації головну роль відіграє амплітуда, оскільки саме в ній помітно проявляється дифракційне ослаблення.

Радіоканал у приміщенні можна описати як суму статичних і динамічних компонентів. Статична компонента формується стінами, меблями та нерухомими предметами. Динамічна компонента виникає через рух людей, відкривання дверей, переміщення предметів і, у нашому випадку, через обертання металевої пластини. Якщо інші об’єкти під час експерименту нерухомі, то контрольована пластина стає основним джерелом зміни CSI.

Базове припущення моделі полягає в тому, що прихована камера передає достатню кількість Wi-Fi пакетів, а приймач може фіксувати CSI для цих пакетів.

Друге припущення – камера має хоча б частково відкритий радіотракт до контрольованої області.

Для опису поширення хвилі між передавачем Tx і приймачем Rx використовується поняття першої зони Френеля. Межа n-ї зони задається умовою:

$$|\mathrm{Tx}Q_n| + |Q_n\mathrm{Rx}| - |\mathrm{TxRx}| = \frac{n\lambda}{2}, \tag{2.2}$$

де T_x – передавач, тобто Wi-Fi камера;

R_x – приймач кіберфізичної системи;

Q_n – точка на межі n-ї зони Френеля;

λ – довжина хвилі;

n – номер зони Френеля.

Перша зона Френеля є найважливішою, оскільки в ній зосереджується значна частина енергії сигналу. Якщо перешкода перетинає цю зону, то частина енергії блокується або огинає перешкоду, внаслідок чого виникає вимірюване ослаблення.

Радіус першої зони Френеля у точці, що має відстані d1 і d2 до передавача і приймача, наближено визначається як:

$$r_1 = \sqrt{\frac{\lambda d_1 d_2}{d_1 + d_2}}, \tag{2.3}$$

де r_1 – радіус першої зони Френеля;

λ – довжина хвилі Wi-Fi сигналу;

d_1 – відстань від передавача до точки перетину зони;

d_2 – відстань від цієї точки до приймача.

Ця формула показує, що розмір зони залежить від довжини хвилі та взаємного розташування пристроїв. Для частоти 2,4 ГГц зона ширша, ніж для 5 ГГц, оскільки довжина хвилі більша. Це означає, що геометрія експерименту і розміри пластини повинні узгоджуватися з частотним діапазоном, у якому працює камера.

Поведінку дифракційного ослаблення можна описати через параметр Френеля–Кірхгофа v. У спрощеному вигляді він пов’язує висоту перешкоди відносно лінії прямої видимості h з радіусом зони Френеля:

$$v = \frac{h\sqrt{2}}{r_1}, \tag{2.4}$$

де v – параметр Френеля–Кірхгофа;

h – зміщення перешкоди відносно лінії прямої видимості;

r_1 – радіус першої зони Френеля.

Значення v визначає, наскільки істотно перешкода впливає на хвилю. Коли перешкода знаходиться далеко від лінії прямої видимості, вплив малий. Коли вона проходить поблизу центральної частини першої зони Френеля, виникає найпомітніше ослаблення.

Для нескінченної перешкоди дифракційний внесок може описуватися інтегралами Френеля, але в практичній системі використовується пластина скінченної ширини. Тому модель враховує передню і задню кромки пластини. Кожна кромка має своє положення відносно лінії прямої видимості, а сумарний ефект визначає глибину ослаблення.

Ключовим внеском керованої дифракції є перехід від довільного руху перешкоди до обертального руху навколо приймача. Якщо пластина рухається по прямій траєкторії, то інтерпретація ослаблення залежить від невідомої відстані до камери та кута перетину зони Френеля. Якщо ж пластина обертається навколо приймача, її рух стає симетричним відносно напряму на передавач.

Позначимо θ як кут між поточним положенням пластини і напрямом на камеру. Якщо центр обертання збігається з положенням приймача, то θ=0 відповідає моменту, коли пластина орієнтована у напрямі цільового пристрою. Для практичної реалізації безпосередньо θ невідомий, оскільки азимут камери і є шуканою величиною. Проте система знає власний кут повороту α(t) у кожен момент часу.

Формально оцінку можна записати як:

$$\alpha_{\text{est}} = \alpha(t_{\text{mid}}), \tag{2.5}$$

де α_{est} – оцінений азимут прихованої камери;

$\alpha(t_{mid})$ – кутове положення пластини в момент середини інтервалу максимального ослаблення;

t_{mid} – середина інтервалу максимального ослаблення.

Інтервал максимального ослаблення визначається не за одиничним мінімальним відліком, а за групою послідовних відліків, у яких нормалізована амплітуда CSI є нижчою за встановлений поріг.

Для обробки CSI доцільно використовувати агреговану амплітуду. Якщо для кожного пакета доступні амплітуди кількох піднесучих, можна обчислити середнє значення, медіану або енергію сигналу за піднесучими. Наприклад,

$$A(t) = \text{median}(|H_k(t)|), \tag{2.6}$$

де $A(t)$ – агрегована амплітуда CSI у момент часу t;

$H_k(t)$ – CSI на k-й піднесучій;

$median(\cdot)$ – медіанне значення за піднесучими.

Медіана є корисною, оскільки зменшує вплив окремих аномальних піднесучих. Після цього часовий ряд A(t) нормалізується відносно базового рівня, отриманого до початку або після завершення проходження пластини.

Нормалізація може бути виконана як:

$$\Delta A(t) = A(t) - A_{\text{base}}, \tag{2.7}$$

де $\Delta A(t)$ – зміна амплітуди CSI у момент часу t;

$A(t)$ – поточне значення агрегованої амплітуди;

A_{base} – базовий рівень амплітуди CSI.

Для пошуку інтервалу максимального ослаблення доцільно згладити ряд за допомогою ковзного середнього, медіанного фільтра або фільтра Савіцького–Голея. Вибір фільтра залежить від частоти надходження пакетів: якщо пакетів мало, надмірне згладжування може приховати корисний провал.

У математичній моделі вводяться критерії якості вимірювання. Перший критерій – глибина провалу:

$$D = A_{\text{base}} - A_{\text{min}} \tag{2.8}$$

де D – глибина провалу CSI;

A_{base} – базовий рівень амплітуди;

A_{min} – мінімальне значення амплітуди під час проходження перешкоди.

Якщо D занадто малий, то ослаблення може бути невідрізнимим від шуму. Другий критерій – ширина інтервалу W, тобто тривалість області, де сигнал нижчий за поріг. Надто вузький інтервал може бути випадковим, а надто широкий може свідчити про сторонній вплив. Третій критерій – симетричність форми провалу відносно оціненого центру. Симетричний провал краще відповідає моделі обертальної дифракції.

Оцінювання похибки виконується порівнянням α_{est} з фактичним азимутом α_{true}. Кутова похибка визначається як:

$$e = \min(|\alpha_{\text{est}} - \alpha_{\text{true}}|, 360^\circ - |\alpha_{\text{est}} - \alpha_{\text{true}}|) \tag{2.9}$$

де e – кутова похибка локалізації;

α_{est} – оцінений азимут прихованої камери;

α_{true} – фактичний азимут камери;

$360°$ – повний кутовий оберт.

Така формула враховує циклічну природу кутів: різниця між 350° і 10° становить не 340°, а 20°. Для серії вимірювань розраховуються середня похибка,

медіана, стандартне відхилення та максимальне відхилення. Ці показники дають змогу порівнювати різні налаштування системи.

Модель виявлення підозрілих пристроїв має іншу природу. Вона базується не на дифракції, а на мережевому трафіку. Прихована камера, яка передає відео, зазвичай має стабільний висхідний потік даних. Для кожної MAC-адреси можна обчислити кількість пакетів за інтервал, середній розмір кадру, частку data-кадрів і зміну пропускної здатності після того, як користувач залишає поле зору.

У спрощеному вигляді умову підозрілості можна подати як S_{mac}=true, якщо середній розмір корисного навантаження перевищує поріг Ts, кількість пакетів перевищує поріг Tl, а MAC-адреса не належить точці доступу. Ця умова не є остаточним доказом наявності камери, але вона зменшує простір пошуку. Далі кореляційний аналіз між активністю у кімнаті та трафіком кандидата підвищує впевненість у класифікації.

Адекватність математичної моделі визначається тим, чи відповідають її припущення реальним умовам. Якщо камера передає дуже мало пакетів, CSI не дає достатньої часової роздільності. Якщо у кімнаті рухаються люди, динамічна компонента від них може змішуватися з ефектом пластини. Якщо камера знаходиться за металевим екраном, прямий радіотракт може бути сильно спотворений.

Перевагою запропонованої математичної моделі є її безпараметричність щодо відстані до камери. Багато методів локалізації потребують знати або оцінити відстань між передавачем і приймачем. У реальному пошуку прихованої камери це майже неможливо, оскільки сама позиція пристрою невідома. Основні параметри математичної моделі показано у табл. 2.2.

Таким чином, математична модель поєднує два рівні опису. На фізичному рівні вона пояснює появу дифракційного провалу через перетин першої зони Френеля. На алгоритмічному рівні вона задає спосіб перетворення цього провалу у кутову оцінку. Саме ця подвійність робить модель придатною для практичного використання: вона не є надмірно складною, але зберігає фізичну інтерпретованість результату.

Таблиця 2.2 – Основні параметри математичної моделі

№	Позначення	Зміст параметра	Спосіб отримання
1.	(λ)	Довжина хвилі Wi-Fi сигналу	Розрахунок за частотою каналу
2.	(H(f))	Комплексна характеристика каналу	Вилучення CSI з прийнятих пакетів
3.	(A(t))	Агрегована амплітуда CSI	Обробка піднесучих
4.	(α(t))	Кутове положення пластини	Розрахунок за кроками двигуна
5.	(D)	Глибина провалу CSI	Порівняння з базовим рівнем
6.	(αest)	Оцінений азимут камери	Середина інтервалу максимального ослаблення

2.4 Методика комп’ютерного моделювання та алгоритми обробки даних

Комп’ютерне моделювання використовується для перевірки алгоритмів до проведення натурних експериментів, а також для аналізу отриманих вимірювань. Його основне завдання – відтворити очікувану форму CSI-провалу при різних кутах, рівнях шуму, швидкості обертання пластини та частоті надходження пакетів. Завдяки моделюванню можна визначити, які параметри обробки є стійкими, а які призводять до нестабільних оцінок.

Перший етап комп’ютерного моделювання полягає у створенні синтетичного часового ряду CSI. Базовий рівень сигналу задається як відносно стабільна величина з невеликим шумом. Дифракційний провал моделюється функцією з мінімумом у момент, що відповідає істинному азимуту. Форма провалу може бути наближена гаусовою, подвійною гаусовою або емпіричною кривою, отриманою з реальних вимірювань.

Другий етап – моделювання кутової траєкторії пластини. Якщо двигун обертається з постійною швидкістю, то кут можна описати як:

$$\alpha(t) = \alpha_0 + \omega t \qquad (2.10)$$

де $\alpha(t)$ – поточний кут пластини в момент часу t;

α_0 – початковий кут;

ω – кутова швидкість обертання;

t – час.

Для крокового двигуна точніше використовувати дискретну модель: кожному кроку відповідає приріст Δα. У програмній реалізації доцільно зберігати таблицю відповідності «час – номер кроку – кут», оскільки реальна швидкість може не бути ідеально сталою через затримки керування.

Третій етап – тестування алгоритму виявлення провалу. На вхід подається синтетичний або реальний ряд A(t), а на виході алгоритм повинен повернути оцінений час t_{mid} і відповідний кут α_{est}. Для порівняння використовуються різні підходи: вибір глобального мінімуму, порогове виділення області ослаблення, пошук локального мінімуму після згладжування, аналіз похідної та апроксимація провалу параметричною функцією.

Тут доцільно використати комбінований алгоритм. Спочатку CSI агрегується за піднесучими, потім ряд згладжується медіанним фільтром, після чого визначається базовий рівень. Далі обирається область, де сигнал нижчий за поріг, наприклад на 30–50 % від максимальної глибини провалу. Якщо знайдено кілька областей, обирається та, що має найбільшу інтегральну глибину або найкращу симетричність.

Псевдокод алгоритму локалізації можна описати так. Вхід: масив CSI, часові мітки пакетів, журнал кутів пластини. Вихід: оцінений азимут і показник довіри. Крок 1 – відфільтрувати пакети цільової MAC-адреси. Крок 2 – обчислити агреговану амплітуду для кожного пакета. Крок 3 – нормалізувати амплітуду відносно базового рівня. Крок 4 – згладити ряд. Крок 5 – знайти інтервал максимального ослаблення. Крок 6 – визначити середину інтервалу.

Для комп’ютерної реалізації доцільно використовувати Python, оскільки він має розвинені бібліотеки для роботи з масивами, сигналами та графіками. NumPy

зручний для векторних обчислень, SciPy – для фільтрації та статистичного аналізу, Pandas – для роботи з таблицями вимірювань, Matplotlib – для побудови графіків.

Особливу увагу потрібно приділити попередній обробці CSI. Сирі вимірювання можуть містити пропуски, різкі викиди, різні масштаби по піднесучих і зміну базового рівня. Тому перед пошуком провалу доцільно виконати очищення даних. Пропуски можна інтерполювати лише тоді, коли вони короткі; довгі пропуски краще позначати як ненадійні ділянки. Викиди можна обмежувати за медіанним абсолютним відхиленням.

У модулі виявлення підозрілих пристроїв алгоритм має іншу структуру. Система послідовно сканує канали, збирає пакети, групує їх за джерельною MAC-адресою та аналізує лише data-кадри. Для кожного пристрою розраховуються середній розмір пакета, кількість пакетів за одиницю часу, частка висхідного трафіку і стабільність потоку. Якщо значення перевищують установлені пороги, пристрій позначається як кандидат.

Кореляційний аналіз трафіку і активності у кімнаті базується на тому, що відеокодеки H.264 і H.265 зменшують обсяг даних у статичних сценах і збільшують його при русі. Тому якщо користувач залишає приміщення або зупиняє рух, а трафік підозрілого пристрою зменшується, це підсилює припущення про камеру. У комп’ютерній моделі це можна перевірити через часовий ряд пропускної здатності B(t) і подію зміни активності.

Під час моделювання необхідно підібрати пороги. Надто низький поріг для підозрілого трафіку призведе до великої кількості хибних кандидатів, а надто високий – до пропуску камер з низькою якістю відео або сильним стисненням. Так само поріг для CSI-провалу впливає на точність азимуту. Тому пороги слід добирати не довільно, а через серії тестів.

Важливим результатом комп’ютерного моделювання є оцінка чутливості алгоритму до шуму. Для цього до синтетичних даних додається шум різної амплітуди, після чого розраховується середня кутова похибка. Якщо похибка різко зростає вже при малому шумі, алгоритм непридатний для реальних умов. Якщо ж похибка зростає поступово, система має запас стійкості.

Ще один напрям моделювання – вплив швидкості обертання пластини. Якщо пластина обертається занадто швидко, за час проходження через інтервал ослаблення може бути прийнято мало пакетів. Якщо занадто повільно, збільшується загальний час вимірювання, а середовище може змінитися через рух користувача або сторонні фактори. Тому швидкість повинна бути компромісною.

Для перевірки алгоритмів корисно формувати графіки. Перший графік – амплітуда CSI від часу з позначеним інтервалом максимального ослаблення. Другий – амплітуда CSI від кута пластини, що безпосередньо показує зв’язок між провалом і азимутом. Третій – порівняння фактичного і оціненого азимутів для серії експериментів. Четвертий – залежність похибки від відстані, кута, швидкості обертання або рівня шуму.

У програмній архітектурі доцільно виділити окремі модулі: модуль захоплення пакетів, модуль читання CSI, модуль керування двигуном, модуль синхронізації, модуль обробки сигналу, модуль локалізації, модуль збереження результатів і модуль візуалізації. Така модульність дозволяє замінювати окремі компоненти без переписування всієї системи.

Комп’ютерна модель також повинна забезпечувати відтворюваність. Для кожного експерименту необхідно зберігати параметри: частоту Wi-Fi, номер каналу, MAC-адресу, швидкість обертання, крок двигуна, довжину пластини, місце встановлення прототипу, фактичний азимут камери і час вимірювання. Без цих метаданих складно пояснити різницю між результатами серій. У табл. 2.3 представлено послідовність комп’ютерної обробки даних.

Для формалізації етапів обробки даних у комп’ютерній моделі доцільно подати послідовність перетворення вхідних параметрів радіоканалу у кінцевий результат локалізації прихованої камери. Така послідовність охоплює захоплення Wi-Fi пакетів, агрегацію CSI-даних, нормалізацію амплітуд піднесучих, фільтрацію шумів, пошук характерного провалу сигналу та оцінювання кута розташування пристрою. Узагальнений порядок комп’ютерної обробки даних наведено в таблиці 2.3.

Результатом комп’ютерного моделювання має бути набір перевірених алгоритмічних рішень, які можна перенести у натурний експеримент. Моделювання не замінює фізичні вимірювання, але дозволяє підготувати систему до них: підібрати фільтри, пороги, формат журналів, швидкість обертання та критерії якості.

Таблиця 2.3 – Послідовність комп’ютерної обробки даних

Етап	Вхідні дані	Результат
Захоплення пакетів	Wi-Fi ефір, MAC-адреса цілі	Набір пакетів і CSI
Агрегація CSI	Амплітуди піднесучих	Один часовий ряд (A(t))
Нормалізація	(A(t)), базовий рівень	Відносна зміна амплітуди
Фільтрація	Нормалізований ряд	Згладжена крива ослаблення
Пошук провалу	Згладжена крива	Інтервал максимального ослаблення
Оцінювання кута	Інтервал, журнал кутів	Азимут прихованої камери

2.5 Методика натурного експерименту та організація вимірювань

Натурний експеримент призначений для перевірки того, чи працює запропонована модель у реальному приміщенні, де присутні багатопроменевість, шум, меблі та інші бездротові пристрої. На відміну від комп’ютерного моделювання, тут неможливо повністю контролювати всі параметри середовища. Саме тому експериментальна методика повинна бути чіткою, повторюваною і достатньо гнучкою для різних сценаріїв.

Першим етапом є підготовка приміщення і обладнання. Обирається кімната, в якій можна встановити камеру в кількох контрольних точках. Камера

підключається до Wi-Fi мережі і переводиться в режим передавання відео. Прототип системи розміщується на столі, тумбі або іншій стабільній поверхні. Нульовий напрям фіксується відносно стіни, дверей або іншого орієнтира.

Другим етапом є калібрування системи. Перевіряється робота Wi-Fi адаптера у режимі моніторингу, доступність CSI, правильність фільтрації MAC-адреси та стабільність керування кроковим двигуном. Пластина повинна обертатися без заїдань, а її кутове положення має відповідати програмному журналу. Також перевіряється, чи не перекривають пластину великі металеві предмети поблизу прототипу.

Третій етап – виявлення підозрілого пристрою. Система сканує канали, виділяє пристрої з інтенсивним висхідним трафіком і за потреби перевіряє зміну трафіку після виходу користувача з поля зору камери. У контрольному експерименті MAC-адреса камери може бути відома, але для наближення до реального сценарію доцільно проводити тест і з невідомою MAC-адресою. Це дозволяє оцінити не лише локалізацію, а й повний цикл роботи системи.

Четвертий етап – власне локалізація. Приймач налаштовується на потрібний канал і цільову MAC-адресу. Запускається запис CSI і синхронно починається обертання пластини. Один повний цикл може охоплювати 180° або 360° залежно від конструкції і завдання. Після завершення циклу дані зберігаються у файл, обробляються алгоритмом, а система повертає оцінений азимут.

П’ятий етап – порівняння результату з еталоном. Для кожного повтору обчислюється кутова похибка. Якщо камера розміщена на азимуті 70°, а система оцінила 82°, похибка становить 12°. Якщо камера розміщена на 350°, а система оцінила 5°, похибка становить 15°, оскільки кути мають циклічну природу.

Шостий етап – аналіз причин похибок. Якщо система помиляється, потрібно визначити, чи пов’язано це з малою кількістю пакетів, слабким CSI-провалом, рухом сторонніх об’єктів, неправильним нульовим кутом, нестабільною швидкістю двигуна або сильними відбиттями. Для цього аналізуються графіки CSI, журнал кутів, кількість пакетів і форма провалу.

У методиці експерименту доцільно передбачити кілька типів приміщень. Перший тип – відносно проста кімната з невеликою кількістю меблів. Вона потрібна для базової перевірки моделі. Другий тип – житлова кімната з меблями, дзеркалами, побутовою технікою та неоднорідними поверхнями. Третій тип – офіс або аудиторія, де присутні столи, стільці, комп’ютери та кілька Wi-Fi пристроїв.

Також варто змінювати положення камери. Її можна розміщувати на різних азимутах, різній висоті та різній відстані від прототипу. Особливо важливо перевірити випадки, коли камера знаходиться не строго на рівні пластини, оскільки в реальному приміщенні вона може бути на полиці, у зарядному пристрої або на стіні.

2.6 Оцінювання адекватності моделей та точності локалізації

Адекватність моделі оцінюється за кількома ознаками. Перша – наявність відтворюваного CSI-провалу під час проходження пластини через напрям на камеру. Друга – близькість середини провалу до фактичного азимуту. Третя – стабільність оцінки при повторних циклах. Четверта – збереження працездатності при зміні приміщення або моделі камери. Якщо всі ці умови виконуються, модель можна вважати адекватною для заявленого класу задач.

Для визначення практичної придатності системи необхідно враховувати не лише точність, а й час роботи. Система, яка дає малу похибку, але потребує тривалого сканування кожного кута, може бути незручною. Тому доцільно фіксувати час підготовки, час сканування каналів, час одного циклу локалізації та час післяобробки. Для користувача важливо, щоб перевірка кімнати займала хвилини, а не десятки хвилин.

Важливою частиною експерименту є перевірка хибних спрацювань. У кімнаті можуть бути пристрої, які передають багато даних, але не є камерами: ноутбуки, телефони, телевізори, відеодомофони або пристрої розумного дому. Тому підсистема виявлення повинна не лише знаходити кандидатів, а й не позначати кожен активний пристрій як камеру.

Для оцінювання результатів можна використати таблицю експериментів. У ній для кожного запуску зазначаються номер досліду, приміщення, модель камери, частотний діапазон, фактичний азимут, оцінений азимут, похибка, кількість пакетів, глибина провалу і коментар щодо умов. Така таблиця дозволяє швидко побачити, в яких сценаріях система працює краще, а в яких гірше. Крім того, вона є основою для статистичного аналізу.

Окремо слід визначити критерії прийнятності. Для практичного пошуку прихованої камери абсолютна точність у кілька градусів не є обов'язковою, оскільки користувач все одно оглядає певний сектор. Якщо середня похибка перебуває в межах 10–20°, система може істотно скоротити область ручного пошуку. Якщо похибка перевищує 45°, практична користь зменшується, оскільки сектор стає занадто широким (табл. 2.4).

Таблиця 2.4 – Рекомендована форма фіксації результатів експерименту

№ досліду	Приміщення	Азимут фактичний	Азимут оцінений	Похибка	Кількість пакетів	Коментар
1.	Житлова кімната	45°	56°	11°	820	Провал чіткий
2.	Офіс	120°	136°	16°	640	Помітні відбиття
3.	Аудиторія	270°	258°	12°	910	Результат стабільний

Методика повинна враховувати безпекові та етичні обмеження. Експерименти з камерами слід проводити лише у контрольованому середовищі, де всі учасники знають про зйомку. Метою дослідження є захист приватності, а не створення засобів несанкціонованого доступу до чужих мереж. Система працює пасивно з радіоефіром і не повинна виконувати атак на камеру, підбір паролів або втручання в роботу мережі.

Перевірка адекватності також може включати порівняння з альтернативними підходами. Наприклад, для тієї самої кімнати можна оцінити, скільки часу займає ручний оптичний пошук, пошук за RSSI або локалізація за переміщенням користувача. Навіть якщо DIFFLOC-подібний підхід не дає точних координат, він може бути вигіднішим за критерієм часу, вартості і зручності. Таке порівняння підсилює практичне обґрунтування вибраної методики.

У разі невдалого вимірювання методика передбачає повторний запуск з іншої точки або зміною налаштувань. Наприклад, якщо провал слабкий, можна зменшити швидкість обертання пластини, змінити висоту встановлення прототипу або повторити цикл при меншій кількості рухів у кімнаті. Якщо підозрюється сильна багатопроменевість, доцільно виконати два вимірювання з різних позицій і порівняти отримані сектори.

Узагальнений алгоритм експериментальної перевірки включає такі кроки: підготувати приміщення; встановити камеру; зафіксувати еталонний азимут; запустити сканування і виявлення; виконати цикл локалізації; зберегти CSI та журнал кутів; обчислити оцінений азимут; розрахувати похибку; повторити для різних положень; сформувати статистичні висновки. Така процедура відповідає вимогам до дослідження технічних систем, оскільки поєднує контрольовані умови, повторюваність і кількісну оцінку.

Розроблена методика натурного експерименту дозволяє перевірити не лише окремий алгоритм, а всю кіберфізичну систему. Вона охоплює підготовку обладнання, виявлення підозрілих пристроїв, збір CSI, керовану дифракцію, оцінку азимуту, аналіз похибки і перевірку адекватності моделі.

2.7 Висновки

У другому розділі було обґрунтовано вибір теоретичних та експериментальних методів дослідження для задачі виявлення і локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу. Показано, що поставлена задача має міждисциплінарний характер, оскільки

поєднує аналіз бездротових мереж, фізику поширення радіохвиль, цифрову обробку сигналів, математичне моделювання та кіберфізичну взаємодію між програмною і апаратною частинами системи.

Запропонована структурна модель системи дала змогу виділити основні компоненти: приховану Wi-Fi камеру як джерело пакетів, пасивний приймач CSI, керований дифракційний модуль, обчислювальний блок і модуль інтерпретації результату. Окремо встановлено зв’язок між моделлю, методом і засобом реалізації, що дозволяє перейти від фізичного пояснення явища дифракційного ослаблення до практичного алгоритму визначення азимутального напряму на передавач.

У розділі сформовано математичну модель радіоканалу, яка враховує параметри CSI, першу зону Френеля, кероване проходження металевої пластини через область поширення сигналу та появу характерного провалу амплітуди. Така модель є достатньо простою для програмної реалізації, але водночас зберігає фізичну інтерпретованість, оскільки результат локалізації пов’язується не з випадковими змінами сигналу, а з контрольованою зміною умов поширення радіохвилі.

Розроблена методика комп’ютерного моделювання визначає порядок створення синтетичних часових рядів CSI, моделювання кутової траєкторії пластини, фільтрації шуму, пошуку інтервалу максимального ослаблення і перетворення часової координати у кутову оцінку. Це дозволяє попередньо перевірити стійкість алгоритмів до шуму, пропусків пакетів, різної швидкості обертання та нестабільності реального радіоефіру.

Методика натурного експерименту описує послідовність підготовки приміщення, калібрування апаратури, виявлення підозрілого пристрою, збирання CSI, виконання циклу локалізації та порівняння оціненого азимуту з еталонним значенням. Для оцінювання якості запропоновано використовувати кутову похибку, глибину CSI-провалу, кількість прийнятих пакетів, стабільність повторних вимірювань і час виконання повного циклу перевірки.

Отже, у другому розділі сформовано повну теоретико-методичну основу подальшої реалізації кіберфізичної системи. Отримані моделі, алгоритмічні

підходи та експериментальна методика можуть бути використані у наступних розділах для проєктування програмно-апаратної архітектури, реалізації окремих модулів системи та аналізу результатів експериментальної перевірки.

3 РОЗРОБЛЕННЯ АЛГОРИТМІВ ТА АРХІТЕКТУРНЕ ПРОЄКТУВАННЯ ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ

3.1 Концепція використання розроблених моделей та методів у програмно-апаратній системі

Третій розділ розкриває перехід від теоретичних моделей до практичної реалізації кіберфізичної системи виявлення та локалізації прихованих Wi-Fi камер. Основна увага зосереджена на алгоритмах, вимогах до програмно-апаратних засобів і структурі комплексу, який поєднує пасивне спостереження за Wi-Fi ефіром з керованим впливом на радіоканал.

Загальна ідея полягає у послідовному робочому циклі. Спочатку система аналізує 802.11-пакети та виділяє пристрої з ознаками відеопередавання. Після цього для вибраної MAC-адреси запускається локалізаційний контур: металева пластина обертається біля приймача, приймач фіксує CSI, а програма зіставляє момент максимального ослаблення з кутом положення пластини.

Розроблені моделі використовуються на трьох рівнях. На фізичному рівні враховується дифракційне ослаблення у першій зоні Френеля, на інформаційному рівні застосовується CSI як джерело вимірювань, а на алгоритмічному рівні формується правило перетворення часової координати провалу амплітуди у кутову оцінку азимуту.

Кіберфізичний характер системи полягає в наявності замкненого циклу: програма керує двигуном, двигун змінює положення пластини, пластина змінює умови поширення хвилі, а змінений канал відображається у CSI. Завдяки цьому система не просто спостерігає за трафіком, а створює контрольовані умови для отримання інформативної ознаки.

Доцільно можна виділяти два контури роботи: контур попереднього виявлення і контур азимутальної локалізації. Перший контур працює з пакетною статистикою, інтенсивністю висхідного трафіку та реакцією на зміну активності у приміщенні. Другий контур працює з CSI, часовими мітками, журналом кутів і алгоритмом пошуку інтервалу максимального ослаблення.

Практичним результатом є не точні декартові координати камери, а сектор пошуку. Такий результат є достатнім для прикладного огляду кімнати, оскільки користувач отримує напрямок, у якому слід перевіряти предмети, адаптери живлення, полиці, датчики або інші місця можливого маскування пристрою.

3.2 Алгоритм попереднього виявлення підозрілих Wi-Fi пристроїв

Алгоритм попереднього виявлення призначений для зменшення множини Wi-Fi пристроїв до невеликого списку кандидатів, які можуть бути прихованими камерами. У типовому приміщенні одночасно працюють смартфони, ноутбуки, телевізори, точки доступу та IoT-пристрої, тому без цього етапу локалізаційний цикл довелося б виконувати для кожного вузла.

Вхідними даними є 802.11-пакети, прийняті адаптером у режимі моніторингу. Для кожного кадру фіксуються часова мітка, MAC-адреси джерела й отримувача, канал, тип кадру, розмір і напрям передавання. Основна увага приділяється data frames, оскільки саме вони відображають прикладний трафік, пов’язаний із відеопотоком.

Першим кроком є сканування каналів. На кожному каналі система збирає пакети протягом короткого інтервалу та формує статистику за MAC-адресами. Далі кадри групуються, а для кожного пристрою обчислюються кількість пакетів, сумарний обсяг даних, середній розмір кадру, частка висхідного трафіку і стабільність потоку.

Прихована камера, що передає відео, зазвичай має відносно стабільний висхідний трафік. Проте схожі ознаки можуть створювати відеодзвінки або завантаження файлів, тому пакетний аналіз використовується не як доказ, а як фільтр. Для підвищення достовірності застосовується кореляційна перевірка: якщо після виходу користувача з поля зору трафік кандидата зменшується, підозра посилюється.

Для ранжування пристроїв вводиться інтегральний коефіцієнт підозрілості, який поєднує кілька нормованих ознак. Ваги можуть задаватися емпірично залежно від умов експерименту, кількості активних пристроїв і рівня мережевого шуму.

$$S_i = w_1 P_i + w_2 L_i + w_3 U_i + w_4 C_i + w_5 R_i \quad (3.1)$$

де S_i – інтегральний коефіцієнт підозрілості і-го Wi-Fi пристрою;

P_i – нормована інтенсивність пакетів;

L_i – нормований середній розмір кадру;

U_i – частка висхідного трафіку;

C_i – показник стабільності потоку;

R_i – показник реакції трафіку на зміну активності у приміщенні;

w_1, w_2, w_3, w_4, w_5 – вагові коефіцієнти ознак.

Після розрахунку коефіцієнта формується список кандидатів, що містить MAC-адресу, канал, кількість пакетів, середню швидкість передавання і причину відбору. Якщо кандидатів кілька, вони сортуються за спаданням коефіцієнта, а локалізація запускається спочатку для найімовірнішого пристрою.

З алгоритмічної точки зору модуль має лінійну складність відносно кількості пакетів. Кожний пакет обробляється один раз, а в пам’яті зберігаються лише агреговані статистики для унікальних MAC-адрес. Це дозволяє виконувати попереднє виявлення на одноплатному комп’ютері у реальному часі.

3.3 Алгоритм азимутальної локалізації на основі CSI та керованої дифракції

Після визначення підозрілого пристрою система переходить до локалізації. Мета цього етапу – визначити азимутальний напрям на джерело сигналу без активної взаємодії з камерою і без обходу приміщення користувачем. Основою є кероване обертання металевої пластини навколо приймача, що створює дифракційний провал амплітуди CSI.

Вхідними даними є CSI-послідовність, часові мітки пакетів, MAC-адреса цілі, номер каналу, журнал кроків двигуна і початковий нульовий напрям. Виходом є оцінений азимут, показник довіри та службові параметри якості: кількість пакетів, глибина провалу, ширина інтервалу ослаблення і точність часової синхронізації.

На етапі збору даних приймач налаштовується на канал цілі, фільтр обмежує пакети заданою MAC-адресою, а двигун обертає пластину у секторі 180 або 360 градусів. Для кожного кроку фіксується час і кут. Синхронізація важлива, оскільки помилка у часі безпосередньо переходить у кутову похибку.

Сирі CSI-дані попередньо обробляються: відбираються стійкі піднесучі, амплітуди агрегуються в один часовий ряд, після чого виконується нормалізація і згладжування. Це зменшує вплив викидів, нерівномірної частоти пакетів і багатопроменевого поширення.

$$A(t_j) = \frac{1}{K} \cdot \sum_{k=1}^{K} \left| H_k(t_j) \right| \tag{3.2}$$

де $A(t_j)$ – агрегована амплітуда CSI для пакета з часовою міткою t_j;

K – кількість вибраних піднесучих;

$H_k(t_j)$ – комплексне значення CSI на k-й піднесучій;

$|H_k(t_j)|$ – амплітуда відповідної піднесучої.

Після фільтрації визначається інтервал максимального ослаблення. У складному приміщенні корисний провал може мати дві близькі западини або супроводжуватися паразитними мінімумами, тому доцільно аналізувати не тільки глобальний мінімум, а й ширину, глибину і симетричність провалу.

$$\alpha_{est} = \alpha(t^*) \tag{3.4}$$

де α_{est} – оцінений азимут прихованої Wi-Fi камери;

$\alpha(t^*)$ – кутове положення металевої пластини у момент t^*;

t^* – часова мітка, визначена за CSI-провалом.

Для контролю надійності вводиться показник довіри, який враховує глибину провалу, кількість пакетів у зоні ослаблення, симетричність кривої та часову неузгодженість між CSI і журналом двигуна. Якщо довіра нижча за поріг, система має рекомендувати повторне вимірювання.

$$Q = \beta_1 D + \beta_2 N_p + \beta_3 M_s - \beta_4 J_t \quad (3.5)$$

де Q – інтегральний показник довіри до локалізації;

D – нормована глибина CSI-провалу;

N_p – нормована кількість пакетів у зоні ослаблення;

M_s – показник симетричності провалу;

J_t – показник часової неузгодженості;

β_1, β_2, β_3, β_4 – вагові коефіцієнти якості.

Псевдокод алгоритму включає такі дії: прийняти MAC-адресу і канал, запустити CSI-збір та обертання пластини, записати пакети і кроки двигуна, вибрати піднесучі, агрегувати амплітуду, нормалізувати ряд, знайти провал, визначити t*, перетворити час у кут, розрахувати довіру і вивести сектор пошуку.

Блок-схема (рис. 3.1) показує послідовність роботи методу виявлення та локалізації прихованої Wi-Fi камери в приміщенні. Спочатку система виконує сканування Wi-Fi каналів, збирає пакети стандарту 802.11 і групує знайдені пристрої за MAC-адресами. Після цього проводиться аналіз мережевого трафіку, щоб визначити, чи є серед підключених пристроїв підозрілий об’єкт. Якщо підозрілий пристрій не виявлено, система повертається до повторного сканування Wi-Fi каналів. Якщо пристрій виявлено, система вибирає його MAC-адресу і канал для подальшого дослідження. Далі запускається обертання металевої пластини, синхронно збираються CSI-дані, виконується їх попередня обробка та пошук інтервалу максимального ослаблення сигналу. Якщо провал CSI достатньо виражений, система обчислює азимут прихованої камери та виводить сектор пошуку або напрямок на неї.

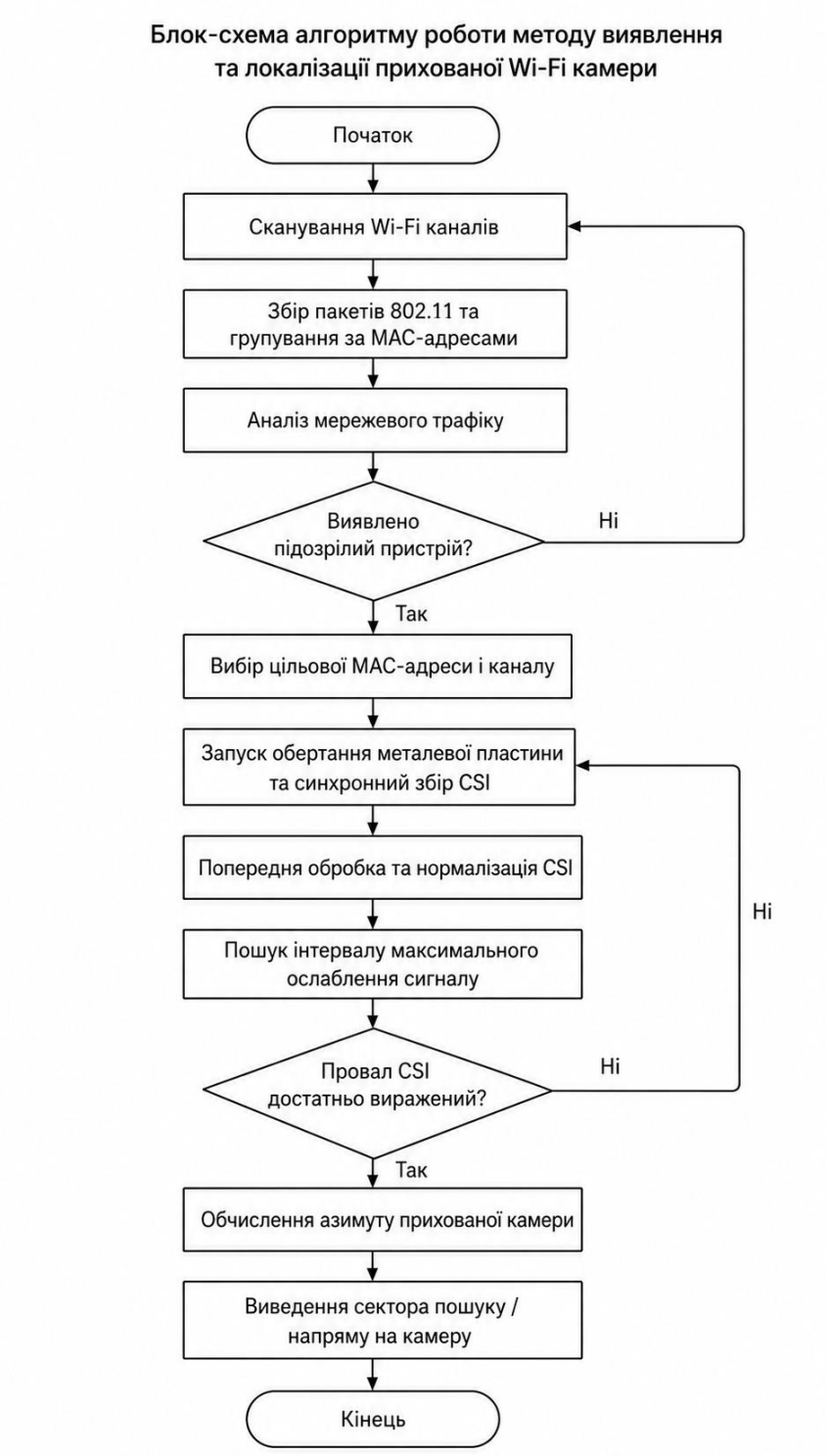


Рисунок 3.1 – Блок-схема алгоритму роботи методу виявлення та локалізації прихованої Wi-Fi камери

Алгоритм масштабується на кілька підозрілих пристроїв: для кожної MAC-адреси повторюється той самий локалізаційний цикл, а фізична траєкторія руху пластини залишається незмінною. Основними умовами успішної роботи є достатня

частота пакетів, стабільний двигун, відсутність активного руху людей і коректний вибір CSI-провалу. Послідовність алгоритму азимутальної локалізації зображено на табл. 3.2.

Таблиця 3.2 – Послідовність алгоритму азимутальної локалізації

Етап	Вхідні дані	Результат
Налаштування приймача	MAC-адреса, канал	Фільтр пакетів
Збір CSI	Wi-Fi пакети цілі	Часовий ряд CSI
Керування двигуном	Крок і швидкість	Журнал кутів
Попередня обробка	Амплітуди піднесучих	Згладжений ряд
Пошук провалу	CSI-крива	t*
Оцінка азимуту	t*, журнал кутів	α_{est}
Контроль якості	D, Np, Ms, Jt	Показник Q

3.4 Вимоги до програмних та апаратно-програмних засобів

Проєктування системи потребує визначення функціональних, апаратних, програмних, експлуатаційних і безпекових вимог. Функціонально система повинна сканувати канали, захоплювати 802.11-пакети, визначати кандидатів, отримувати CSI, керувати двигуном, вести журнал кутів, обробляти сигнал і відображати азимутальний сектор.

До апаратних вимог належить наявність обчислювальної платформи, сумісної з Wi-Fi адаптером, CSI-інструментами і GPIO або іншим інтерфейсом керування двигуном. Одноплатний комп’ютер Raspberry Pi є придатною базою через компактність, підтримку Linux і можливість роботи з Python, але архітектура має залишатися переносною на інші платформи.

Wi-Fi частина повинна підтримувати режим моніторингу та отримання CSI. Для прототипу можна застосовувати сумісний чипсет із nexmon_csi. Механічна частина повинна забезпечувати повторюваний рух пластини без люфтів, а ширина пластини має бути співмірною з довжиною хвилі Wi-Fi сигналу.

Програмні вимоги охоплюють модульність, журналювання, обробку помилок, збереження сирих і проміжних даних, а також можливість повторного аналізу експерименту. Інтерфейс користувача може бути консольним на етапі прототипу, але має зрозуміло показувати список кандидатів, статус локалізації, азимут і рівень довіри.

Безпекова вимога полягає у пасивності. Система не повинна підбирати паролі, порушувати шифрування, надсилати шкідливі кадри або втручатися у роботу мережі. Вона аналізує доступні радіоприймачу фізичні та пакетні характеристики, що робить її придатною для етичного застосування у контрольованому приміщенні.

Далі наведено основні групи вимог до програмно-апаратної реалізації кіберфізичної системи виявлення та локалізації прихованих Wi-Fi камер. До функціональних вимог належать сканування бездротового середовища, отримання CSI-даних, керування двигуном і виконання локалізації, а критерієм їх перевірки є забезпечення повного циклу роботи системи. Апаратні вимоги передбачають підтримку режиму monitor mode, отримання CSI, наявність GPIO-інтерфейсу та підключення двигуна; їх виконання перевіряється через сумісність усіх компонентів системи. Програмні вимоги включають модульність, ведення логів і фільтрацію даних, а критерієм перевірки є наявність відповідних програмних модулів і журналів роботи. Експлуатаційні вимоги пов’язані з простим запуском системи та її переносністю, що забезпечує мінімальну участь користувача під час роботи. Безпекові вимоги передбачають пасивне спостереження за радіоефіром без активного втручання в роботу мережі, а критерієм їх виконання є відсутність дій, які можуть порушити функціонування бездротової інфраструктури.

3.5 Архітектурне проєктування програмно-апаратного комплексу

Архітектура комплексу визначає склад підсистем, потоки даних і порядок взаємодії під час повного циклу виявлення та локалізації. Доцільною є багаторівнева структура: фізичний рівень, рівень збору даних, рівень керування

механізмом, рівень обробки сигналу, рівень прийняття рішення, сховище експериментів і користувацький інтерфейс.

Фізичний рівень включає приховану камеру, радіоканал приміщення, металеву пластину, кроковий двигун, кріплення і приймальний Wi-Fi модуль. Геометрія приміщення та положення камери невідомі, але положення пластини і режим її руху повністю контролюються системою.

Рівень збору даних складається з підсистеми перехоплення 802.11-пакетів і підсистеми вилучення CSI. У простому варіанті ці функції можуть виконуватися одним адаптером, а у розширеному – різними інтерфейсами: один адаптер сканує канали, другий стабільно збирає CSI на вибраному каналі.

Рівень керування двигуном формує команди обертання, задає швидкість, напрям, крок і початкове положення. Він повертає журнал часових міток і кутів, який використовується модулем локалізації. У разі збою двигуна система повинна зупинити експеримент і повідомити користувача.

Рівень обробки сигналів виконує очищення CSI, вибір піднесучих, агрегацію, нормалізацію, згладжування і пошук провалу. Рівень прийняття рішення складається з класифікатора кандидатів і локалізатора азимуту. Обидва блоки мають повертати не тільки рішення, а й пояснювальні показники.

Сховище експериментів зберігає дату, час, MAC-адресу, канал, параметри обертання, файл CSI, журнал двигуна і підсумковий кут. Уніфіковані CSV або JSONL-файли дають змогу повторно обробляти дані без повторення фізичного експерименту. Це важливо для відлагодження і порівняння алгоритмів.

Архітектура має підтримувати ізоляцію помилок. Якщо не працює виявлення, MAC-адресу можна задати вручну; якщо недоступний CSI, можна окремо перевірити механіку; якщо виникає проблема з двигуном, можна аналізувати вже записані дані. Такий підхід спрощує поетапну розробку прототипу.

3.6 Оцінка обчислювальної складності, стійкості та практичної придатності алгоритмів

Оцінка складності потрібна для підтвердження можливості роботи системи на одноплатній платформі. Більшість операцій має лінійну складність відносно кількості пакетів або CSI-вимірювань, тому система не потребує графічного процесора чи тривалого навчання моделей.

Попереднє виявлення обробляє кожний пакет один раз, тому його складність становить O(N), де N – кількість перехоплених пакетів. Пам’ять залежить від кількості унікальних MAC-адрес M і дорівнює O(M). Обробка CSI має складність O(TK), де T – кількість вимірювань, а K – кількість вибраних піднесучих.

$$C_{total} = O(N) + O(TK) + O(T) \quad (3.7)$$

де C_{total} – узагальнена обчислювальна складність одного циклу;

N – кількість перехоплених Wi-Fi пакетів;

T – кількість CSI-вимірювань;

K – кількість піднесучих, використаних для агрегації.

Діаграма на рис. 3.2 показує, як розподіляється обчислювальний час між основними етапами методу виявлення та локалізації прихованої Wi-Fi камери. Найбільше часу займає збір CSI та обертання пластини, оскільки цей етап потребує синхронного отримання радіоканальних параметрів і механічного позиціонування. Сканування Wi-Fi каналів становить 20% загального часу, тому воно також є важливою частиною роботи системи. Збір пакетів і аналіз трафіку, обробка CSI, а також пошук провалу та оцінка азимуту займають по 15% часу кожен.

Найменше часу витрачається на формування результату, адже після обчислення напряму система лише виводить сектор пошуку або ймовірний напрямок на камеру. Це свідчить про те, що основне навантаження методу припадає не на кінцеве обчислення результату, а на етапи отримання та підготовки вимірювальних даних. Такий розподіл є логічним, оскільки точність локалізації залежить від якості зібраних параметрів радіоканалу та коректної синхронізації з рухом пластини.

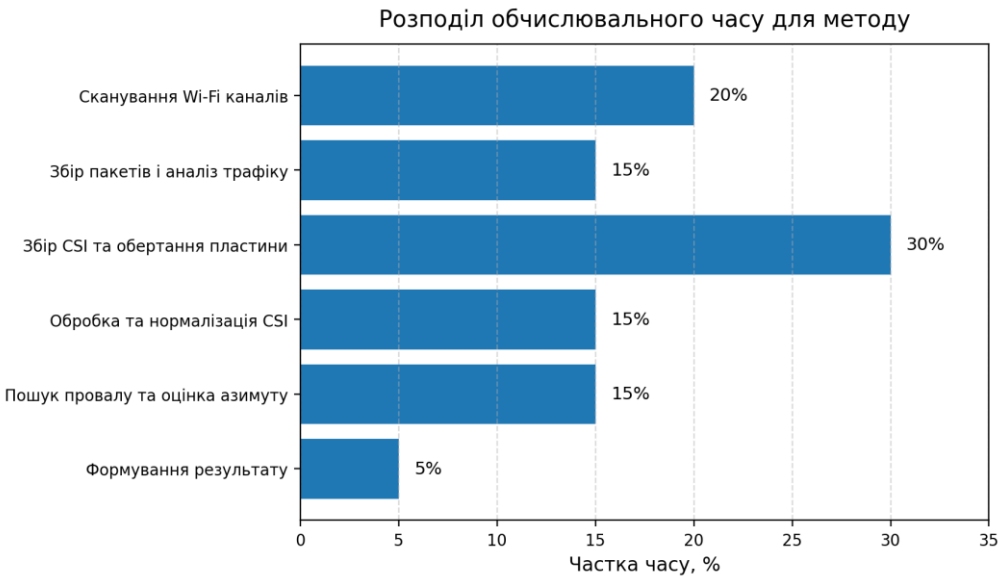


Рисунок 3.2 – Розподіл обчислювального часу для методу

Стійкість алгоритму визначається частотою пакетів, багатопроменевістю, рухом сторонніх об’єктів і механічною похибкою. Якщо пакетів мало, провал CSI може бути пропущений; якщо у кімнаті є активний рух, фон стає нестабільним; якщо двигун має люфт, порушується кутова прив’язка. Для зменшення впливу цих чинників застосовуються повторні вимірювання, фільтрація, вибір стійких піднесучих і показник довіри.

Система є практично придатною, якщо її середня похибка дозволяє суттєво звузити сектор ручного пошуку. Для користувача важливо отримати напрямок на групу предметів, а не координати з сантиметровою точністю. Основні ризики пов’язані не з обчисленнями, а з якістю радіоданих, синхронізацією та фізичними умовами експерименту (табл. 3.3). Тому під час практичного застосування системи необхідно контролювати стабільність положення приймача, швидкість обертання пластини та кількість зібраних пакетів. Якщо вимірювання виконуються занадто швидко або в умовах сильних завад, характерний провал CSI може бути нечітким, що збільшує похибку оцінки азимуту. Для зменшення цього ризику доцільно виконувати кілька повторних циклів локалізації та усереднювати отримані результати. Для зменшення цього ризику доцільно виконувати кілька повторних циклів локалізації та усереднювати отримані результати.

Таблиця 3.3 – Джерела похибок і способи їх зменшення

Джерело похибки	Можливий прояв	Спосіб зменшення
Низька частота пакетів	Провал CSI не фіксується	Збільшення часу запису
Багатопроменевість	Додаткові мінімуми	Фільтрація і повтори
Рух людей	Нестабільний фон CSI	Вимірювання без руху
Люфт двигуна	Помилка кута	Калібрування
Слабкий сигнал	Мала глибина провалу	Зміна позиції приймача
Паразитні пристрої	Хибні кандидати	Білий список

Отже, практична ефективність методу визначається сукупністю чинників: кількістю пакетів, якістю CSI, стабільністю механічного руху, правильністю фільтрації, формою провалу та зрозумілістю інтерфейсу. Саме тому у програмно-апаратній реалізації необхідно поєднати прості алгоритми обробки з механізмами контролю якості й повторної перевірки результату.

Збереження проміжних даних є важливим для наукової перевірки результатів. Файли з CSI, журналами двигуна і параметрами експерименту дозволяють повторно обчислити азимут, порівняти різні фільтри, змінити пороги та перевірити вплив окремих налаштувань без повторного фізичного досліду. Це робить систему придатною не тільки для демонстрації, а й для подальшого вдосконалення.

З позиції експлуатації система повинна формувати зрозумілі повідомлення про причини невдалого запуску. Наприклад, якщо пакетів недостатньо, користувач має бачити рекомендацію збільшити час запису; якщо CSI-провал слабкий – змінити положення пристрою; якщо трафік нестабільний – повторити вимірювання після усунення руху в кімнаті. Такий підхід підвищує практичну придатність прототипу.

Важливо також враховувати, що виявлення і локалізація мають різні джерела помилок. На етапі виявлення помилки виникають через подібність відеотрафіку камери до інших потоків даних. На етапі локалізації основні помилки пов’язані з

формою CSI-провалу, синхронізацією з двигуном і багатопроменевістю. Тому критерій довіри має об’єднувати мережеві та фізичні показники, а не спиратися лише на один параметр.

Окремим елементом стійкості є повторюваність результату. Якщо два або три послідовні цикли локалізації дають близькі азимути, результат можна вважати більш надійним. Якщо ж оцінки значно відрізняються, система повинна не усереднювати їх механічно, а повідомляти про нестабільність і рекомендувати змінити місце встановлення приймача або повторити вимірювання за меншого руху в приміщенні.

У програмній реалізації доцільно передбачити два режими роботи. Швидкий режим використовується для первинної перевірки кімнати і працює з коротким інтервалом сканування. Розширений режим застосовується тоді, коли швидка перевірка виявила підозрілий пристрій або коли рівень довіри до локалізації є недостатнім. Такий поділ дозволяє поєднати зручність для користувача і надійність дослідження.

Розподіл обчислювального часу, наведений на рисунку 3.2, показує, що алгоритм має змішану природу: частина затримки залежить від радіоефіру та активності камери, а частина – від програмної обробки. Тому оптимізація має виконуватися не тільки на рівні коду, але й на рівні налаштування тривалості сканування, швидкості обертання пластини та мінімальної кількості пакетів, потрібних для достовірного висновку.

Для практичної оцінки часу роботи метод доцільно розглядати не лише за асимптотичною складністю, а й за структурою реального циклу. Найбільше часу займає очікування пакетів під час сканування каналів і локалізаційного збору CSI. Обчислювальні операції, зокрема нормалізація, фільтрація та пошук мінімумів, виконуються швидко порівняно з фізичним обертанням пластини й не є вузьким місцем системи.

У результаті архітектурне проєктування має забезпечити не тільки виконання алгоритму, а й можливість його перевірки, повторення та вдосконалення. Саме

тому в системі передбачено журналювання, модульність, збереження проміжних даних і контроль довіри до результату.

Ще одним можливим удосконаленням є автоматичний вибір піднесучих. Замість фіксованого набору піднесучих система може оцінювати дисперсію, рівень шуму і середню амплітуду кожної піднесучої, після чого залишати лише ті компоненти, які найкраще відображають дифракційне ослаблення. Такий підхід підвищує стійкість до багатопроменевості.

Найбільш перспективним напрямом подальшого вдосконалення є адаптивне керування швидкістю обертання. Якщо система бачить високу частоту пакетів, пластину можна обертати швидше; якщо пакетів мало, швидкість доцільно зменшити, щоб у зоні провалу накопичилося більше CSI-вимірювань. Це дозволить підвищити точність без зміни апаратної частини.

3.7 Висновки

У третьому розділі розкрито практичне використання розроблених моделей і методів у вигляді алгоритмів та архітектури програмно-апаратної кіберфізичної системи. Показано, що модель керованої дифракції реалізується через цикл: попереднє виявлення, збір CSI, керування металевою пластиною, пошук максимального ослаблення та розрахунок азимуту.

Розроблено алгоритм попереднього виявлення підозрілих пристроїв за статистикою Wi-Fi пакетів, розміром кадру, часткою висхідного трафіку, стабільністю потоку і реакцією на зміну активності у приміщенні. Цей алгоритм передає до локалізаційного модуля MAC-адресу і канал цілі. Сформовано алгоритм азимутальної локалізації на основі CSI і журналу положення металевої пластини. Алгоритм передбачає агрегацію амплітуди, нормалізацію, фільтрацію, пошук інформативного провалу, визначення часової мітки та перетворення її у кутову оцінку з контролем довіри.

Визначено вимоги до програмних та апаратно-програмних засобів і запропоновано архітектуру комплексу з модулями сканування, аналізу трафіку,

збору CSI, керування двигуном, обробки сигналу, локалізації та інтерфейсу. Оцінка складності показала, що основні процедури мають лінійну складність і можуть бути реалізовані на недорогій одноплатній платформі.

4 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ПРОВЕДЕННЯ ЕКСПЕРЕМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

4.1 Обґрунтування вибору інструментальних засобів та архітектура програмної моделі

Побудова програмної реалізації системи виявлення та локалізації прихованих Wi-Fi камер потребує вибору таких інструментальних засобів, які забезпечують одночасне виконання трьох груп задач: пасивне спостереження за бездротовим середовищем, керування фізичним дифракційним елементом та обробку отриманих вимірювань. Для цього доцільно використовувати апаратну платформу з підтримкою Linux, мережеві інтерфейси, здатні працювати в режимі моніторингу, та мову програмування, придатну для швидкої обробки сигналів і взаємодії з периферією.

Як базову обчислювальну платформу для реалізації системи обрано Raspberry Pi. Такий вибір пояснюється компактністю, невисокою вартістю, наявністю GPIO-інтерфейсу для керування виконавчими пристроями, підтримкою зовнішніх USB Wi-Fi адаптерів та можливістю встановлення спеціалізованих інструментів для роботи з CSI. Крім того, Raspberry Pi може бути використаний як переносний вузол кіберфізичної системи, який легко розмістити на столі, підвіконні або іншій поверхні у приміщенні.

Програмна частина реалізується мовою Python. Ця мова зручна для побудови прототипу, оскільки має велику кількість бібліотек для обробки масивів даних, роботи з файлами, побудови графіків, керування GPIO та аналізу мережевих пакетів. Для числової обробки можуть використовуватися бібліотеки NumPy та Pandas, для візуалізації - Matplotlib, для обробки Wi-Fi пакетів - Scapy або tshark, а для керування кроковим двигуном - бібліотеки роботи з GPIO.

Архітектура програмної моделі складається з кількох модулів. Модуль сканування Wi-Fi середовища визначає доступні канали, точки доступу та активні пристрої. Модуль попереднього виявлення аналізує MAC-адреси, розмір пакетів, кількість кадрів та характер трафіку. Модуль збору CSI/RSSI реєструє параметри

радіоканалу від вибраного пристрою. Модуль керування двигуном задає кутове положення металевої пластини та синхронізує його з часовими мітками вимірювань. Модуль обробки сигналу виконує фільтрацію, пошук провалів амплітуди і розрахунок азимуту. Завершальний модуль формує результат для користувача у вигляді напряму пошуку.

Таблиця 4.1 показує призначення кожного компонента та очікуваний результат його роботи, що дозволяє зрозуміти роль окремих елементів у загальному процесі збору, обробки й відображення результатів локалізації.

Таблиця 4.1 – Основні компоненти програмно-апаратної реалізації системи

Компонент системи	Призначення	Очікуваний результат
Raspberry Pi	Обчислювальний вузол, запуск програмних модулів і керування периферією	Єдина платформа для збору та обробки даних
Wi-Fi адаптер у monitor mode	Пасивне перехоплення 802.11 пакетів і збір даних про канал	MAC-адреси, канали, RSSI/CSI-показники
Крокoвий двигун	Кероване обертання дифракційного елемента	Відомий кут положення пластини
Металева пластина	Створення контрольованого дифракційного ослаблення	Поява характерного провалу CSI
Python-модулі	Фільтрація, аналіз, візуалізація і розрахунок азимуту	Результат локалізації для користувача

Важливою особливістю архітектури є її модульність. Кожен блок може бути замінений або вдосконалений без повної перебудови системи. Наприклад, замість

одного інструменту збору CSI можна використати інший сумісний драйвер або мережевий адаптер, а замість простого методу пошуку мінімумів у сигналі - більш складний алгоритм статистичного виявлення аномалій. Така гнучкість є важливою для подальшого розвитку системи.

З погляду інформаційних потоків система працює таким чином: із бездротового середовища отримуються кадри 802.11 і параметри каналу; після фільтрації визначається підозрілий пристрій; далі запускається процедура керованого фізичного впливу на радіоканал; отримана крива CSI зіставляється з кутами обертання пластини; у підсумку формується оцінка азимуту на прихований пристрій.

На рисунку 4.1 показано, що система складається з двох взаємопов’язаних частин: підсистеми виявлення прихованої Wi-Fi камери та підсистеми локалізації. Перша частина формує MAC-адресу і номер Wi-Fi каналу цільового пристрою, а друга частина використовує ці дані для збирання CSI і визначення азимутального напрямку.

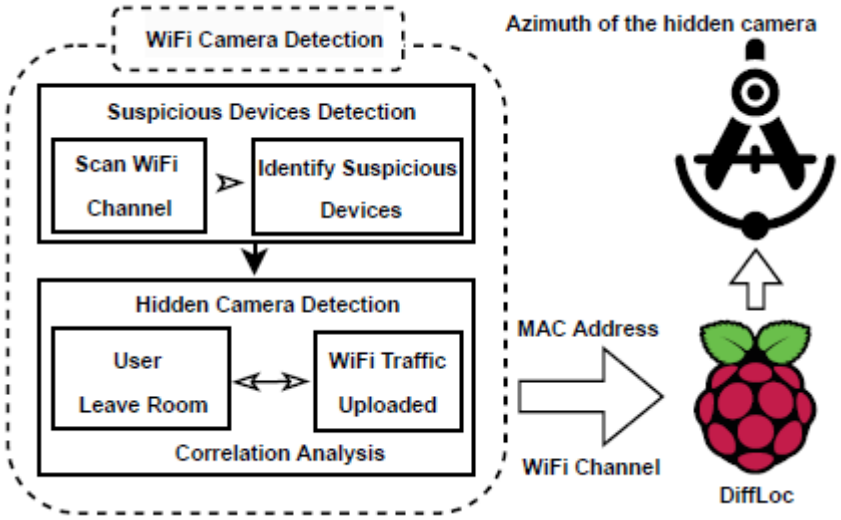


Рисунок 4.1 – Загальна схема системи виявлення та локалізації прихованої Wi-Fi камери

Прототип для схеми містить Raspberry Pi, Wi-Fi адаптер, кроковий двигун, з’єднувальну тягу і тонку алюмінієву пластину. Саме пластина є фізичним

елементом, який створює контрольоване ослаблення сигналу. Її обертання навколо приймача дає змогу отримати вимірювану залежність між положенням пластини і зміною параметрів радіоканалу.

4.2 Програмна реалізація розробленого алгоритму

Програмна реалізація розробленого алгоритму охоплює повний цикл роботи системи: від початкового сканування Wi-Fi середовища до розрахунку напряму на приховану камеру. Алгоритм побудований так, щоб користувачеві не потрібно було переміщатися по всьому приміщенню або виконувати складні ручні вимірювання. Основні дії виконуються автоматично після запуску програми.

На першому етапі мережева карта переводиться у режим моніторингу. У цьому режимі пристрій може пасивно приймати Wi-Fi кадри без підключення до конкретної точки доступу. Програма послідовно переглядає доступні канали, фіксує активні MAC-адреси та групує отримані пакети за джерелом. Службові та керувальні кадри не використовуються для основного аналізу, оскільки вони не містять корисного навантаження відеопотоку. Для оцінювання підозрілості беруться насамперед Data frames.

Прихована Wi-Fi камера, яка передає відео, зазвичай формує відносно стабільний висхідний трафік. Тому для попереднього відбору пристроїв використовуються такі ознаки: середній розмір корисного навантаження, кількість пакетів за інтервал спостереження, повторюваність передавання даних і відсутність належності MAC-адреси до точки доступу. Якщо пристрій перевищує задані пороги, він заноситься до списку підозрілих.

Для подальшого підтвердження підозрілий пристрій аналізується за зміною трафіку під час зміни сцени. Оскільки відеокодеки стискають статичне зображення ефективніше, трафік камери може зменшуватися, коли користувач залишає кімнату. Якщо після виходу користувача пропускна здатність потоку падає, це є додатковою ознакою того, що пристрій може виконувати відеоспостереження.

Після визначення MAC-адреси та каналу цільового пристрою запускається етап локалізації. Система починає збір CSI від вибраного джерела та одночасно керує крововим двигуном. Кожному кроку двигуна відповідає певний кут положення металевої пластини. Тому програма обов’язково зберігає часову мітку, номер кроку, кут повороту і поточне значення амплітуди CSI.

Коли металева пластина потрапляє до першої зони Френеля між передавачем і приймачем, у прийнятому сигналі виникає ослаблення. Це ослаблення не є випадковим шумом, а фізично обумовленим дифракційним ефектом. Тому за часовим положенням провалу CSI можна оцінити геометричне положення джерела сигналу відносно приймача.

На практиці прямолінійний рух пластини не завжди зручний, оскільки він вимагає точного знання взаємного розташування передавача, приймача і перешкоди. Тому в системі використовується обертання пластини навколо приймача. Такий підхід забезпечує симетричність руху відносно лінії прямої видимості та зменшує залежність від невідомої відстані до камери.

Обробка CSI-даних виконується у кілька кроків. Спочатку сигнал згладжується низькочастотним або медіанним фільтром, що дає змогу зменшити вплив випадкових коливань. Далі з набору піднесучих вибираються ті, які мають найстабільніші середні значення і менше спотворюються шумами. Після цього програма виконує пошук локальних мінімумів, які відповідають значному дифракційному ослабленню.

Якщо у кривій CSI виявлено один виражений мінімум, його часове положення використовується як момент локалізації. Якщо виявлено два близькі за амплітудою мінімуми, то обирається середина між ними. Саме цей момент відповідає положенню, коли металева пластина орієнтована на джерело сигналу. Після цього за таблицею відповідності часових міток і кроків двигуна визначається кут, який приймається як оцінка азимуту прихованої камери.

Таблиця 4.2 відображає послідовність програмної реалізації алгоритму виявлення та локалізації прихованої Wi-Fi камери. У ній подано основні етапи роботи системи: від сканування каналів і фільтрації трафіку до підтвердження

підозрілого пристрою, збору параметрів радіоканалу та обробки сигналу. Така структура дозволяє показати, які вхідні дані використовуються на кожному етапі та який результат формується для подальшого визначення ймовірного місця розташування камери.

Таблиця 4.2 – Послідовність програмної реалізації алгоритму виявлення та локалізації

Етап алгоритму	Вхідні дані	Результат
Сканування каналів	802.11 кадри з ефіру	Перелік активних пристроїв
Фільтрація трафіку	MAC-адреси, Data frames, RSSI	Список підозрілих пристроїв
Підтвердження камери	Зміна трафіку під час виходу користувача	Цільова MAC-адреса і канал
Збір CSI	Пакети від цільового пристрою	Часовий ряд параметрів каналу
Обертання пластини	Кроки двигуна і часові мітки	Кутове положення дифракційного елемента
Обробка сигналу	CSI-крива та кути	Оцінка азимуту камери

У вигляді узагальненого псевдокоду алгоритм можна подати так: спочатку виконати сканування Wi-Fi каналів; для кожної MAC-адреси розрахувати статистику трафіку; відібрати пристрої, що мають ознаки відеопередавання; для кожного кандидата перевірити зміну трафіку після виходу користувача; для підтвердженого пристрою запустити збір CSI; синхронно обертати пластину; знайти момент максимального ослаблення; зіставити цей момент із кутом двигуна; вивести користувачу азимутальний напрямок.

На рисунку 4.2 наведено приклади кривих CSI, на яких позначено моменти визначення дифракційного ослаблення. У різних положеннях камери форма провалу може відрізнятися: іноді спостерігається один глибокий мінімум, іноді - два мінімуми. Проте в обох випадках алгоритм може визначити характерну точку та перетворити її на кутовий напрямок.

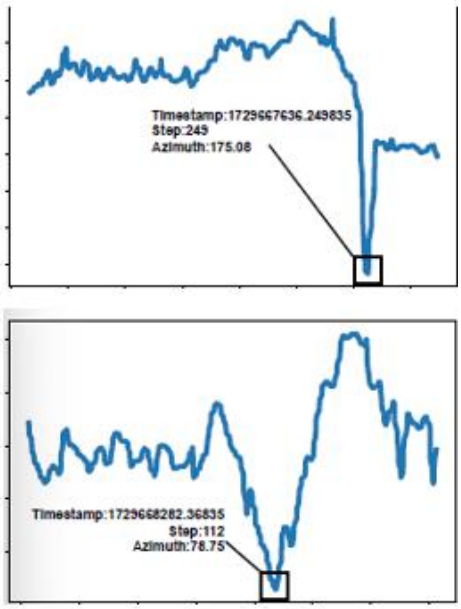


Рисунок 4.2 – Приклади роботи алгоритму локалізації для різних азимутів камери

Демонстраційний кадр (рис. 4.3) підтверджує, що програмна частина може відображати поточний стан вимірювань, положення пластини та результат оцінювання азимуту. Це є важливим для практичного використання системи, оскільки користувач повинен отримати не лише числовий результат, а й зрозуміле пояснення напряму подальшого пошуку. Відображення кута повороту пластини дозволяє перевірити, чи правильно синхронізуються механічний модуль і програмний алгоритм. Наявність графічного або табличного результату спрощує аналіз експерименту, оскільки користувач може побачити момент виникнення найбільшого ослаблення сигналу. Це також дає змогу швидко виявити некоректні вимірювання, наприклад різкі випадкові стрибки або відсутність вираженого мінімуму. Інтерфейс програмної частини повинен бути простим, щоб ним міг користуватися оператор без спеціальної підготовки у сфері радіовимірювань.

Рисунок 4.3 – Кадр демонстраційного відео з роботою системи локалізації

4.3 Проведення експериментальних досліджень

Експериментальне дослідження розробленої системи проводиться для перевірки працездатності алгоритмів, оцінювання точності локалізації та визначення впливу реальних умов приміщення на результат. Під час експерименту потрібно враховувати, що Wi-Fi сигнал у приміщенні поширюється не лише прямою траєкторією, а й відбивається від стін, меблів, металевих поверхонь і побутових предметів. Тому перевірка має виконуватися не лише в порожньому просторі, а й у кімнатах із типовими перешкодами.

Підготовка експерименту включає налаштування Raspberry Pi, переведення Wi-Fi адаптера в режим моніторингу, перевірку збору CSI, підключення і тестування крокового двигуна, калібрування початкового положення металевої пластини та визначення координат контрольних точок розміщення камери. Для кожного досліду фіксуються фактичний азимут камери, оцінений системою азимут, кутова похибка, кількість пакетів, тип приміщення і особливості розміщення.

Дослідження доцільно проводити у кількох приміщеннях різного типу: житловій кімнаті, спальні, офісі, аудиторії або переговорній. У кожному приміщенні камера розміщується в кількох положеннях. Система встановлюється в контрольній точці, зазвичай біля стіни або на столі. Такий спосіб розміщення

полегшує інтерпретацію результату, оскільки камера шукається вздовж визначеного азимутального напряму.

На рисунку 4.4 подано приклади шести приміщень, у яких можуть проводитися дослідження. Кожне приміщення має власні розміри, кількість перешкод і характер поширення сигналу. Такий набір умов дає змогу перевірити роботу системи не лише в простій кімнаті, а й у просторі з меблями, відбивними поверхнями та різною відстанню між камерою і приймачем.

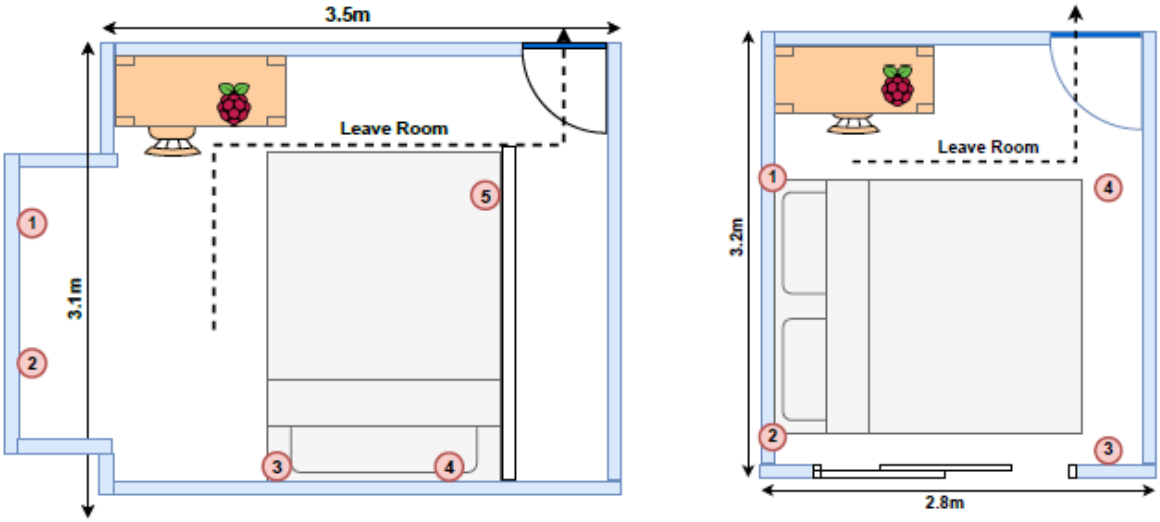


Рисунок 4.4 – Схеми приміщень і варіанти розміщення камер під час експериментів

Процедура експерименту складається з двох основних фаз. У першій фазі перевіряється виявлення підозрілого пристрою. Для цього система збирає Wi-Fi трафік, групує пакети за MAC-адресами та визначає пристрої, що мають ознаки стабільного передавання даних. Далі користувач залишає кімнату, а система аналізує, чи змінюється трафік кандидата. Якщо спостерігається характерне зменшення трафіку, пристрій переходить до фази локалізації.

У другій фазі запускається збір CSI від підтвердженого пристрою. Кроковий двигун обертає металеву пластину в заданому секторі, а програма одночасно записує часові мітки та амплітуду CSI. Після завершення обертання виконується фільтрація сигналу, пошук ділянки максимального ослаблення і розрахунок

азимуту. Фактичний азимут порівнюється з розрахованим. На табл. 4.3 показані параметри організації експериментального дослідження.

Таблиця 4.3 – Параметри організації експериментального дослідження

№	Параметр експерименту	Значення або спосіб фіксації
1	Тип приміщення	Житлова кімната, спальня, офіс, аудиторія
2	Кількість положень камери	Кілька контрольних точок у кожному приміщенні
3	Діапазон обертання пластини	0-180 градусів
4	Основний показник	Кутова похибка локалізації
5	Додаткові показники	Кількість пакетів, якість CSI, час вимірювання
6	Умови завад	Меблі, стіни, металеві предмети, рух людей

Для кількісної оцінки точності використовується абсолютна кутова похибка. Вона визначається як модуль різниці між фактичним азимутом камери та азимутом, розрахованим системою. Чим менше значення цієї похибки, тим точніше система вказує напрямок пошуку. Проте для практичного застосування не обов’язково отримувати точні координати камери: достатньо звузити сектор ручного огляду до невеликої області.

Під час експериментів також фіксуються можливі причини помилок. До них належать низький рівень сигналу, недостатня кількість пакетів, інтенсивна багатопроменевість, наявність металевих поверхонь, несиметричне розміщення системи, сторонній рух у кімнаті та особливості антени приймача. Аналіз цих факторів потрібний для подальшого вдосконалення програмної реалізації.

4.4 Аналіз результатів моделювання та оцінка ефективності

Аналіз результатів моделювання та експериментальної перевірки показує, що метод керованої дифракції може бути використаний для практичної локалізації прихованих Wi-Fi камер. Його головна перевага полягає в тому, що система не потребує попереднього навчання для конкретної кімнати, не вимагає тривалого переміщення користувача та не залежить від дорогого спеціалізованого обладнання. Напрямок на камеру визначається за фізично інтерпретованою ознакою - ділянкою ослаблення CSI, спричиненою обертанням металевої пластини.

У порівнянні з методами, які використовують лише RSSI або трафік, запропонований підхід дає додаткову просторову інформацію. Аналіз трафіку дозволяє зрозуміти, який пристрій може бути камерою, але не дає точного напряму його розташування. Керована дифракція, навпаки, забезпечує зв’язок між геометрією поширення сигналу і кутом положення дифракційного елемента.

З рисунка 4.5 видно, що похибка локалізації змінюється залежно від положення камери і властивостей приміщення. У деяких точках похибка є меншою, у деяких - більшою. Це пояснюється неоднаковими умовами поширення сигналу, різною кількістю відбивних поверхонь, відстанню до камери та особливостями апаратної реалізації приймача.

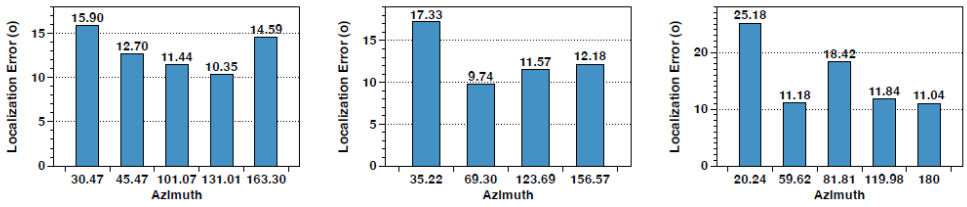


Рисунок 4.5 – Середні похибки локалізації прихованих камер у різних приміщеннях

У дослідженні DIFFLOC середня похибка азимутальної локалізації становила близько 14,82°. Для задачі пошуку прихованої камери такий результат є практично прийнятним, оскільки користувачеві потрібно не точно визначити координати

пристрою, а звузити зону огляду. Наприклад, якщо система вказує напрямок з похибкою до кількох десятків градусів, оператор може оглянути предмети у відповідному секторі: полиці, розетки, годинники, зарядні пристрої, декоративні елементи або побутову техніку.

Діаграми розподілу на рисунку 4.6 показують, що результати вимірювань мають певну варіативність. Це означає, що повторні запуски системи можуть давати близькі, але не повністю однакові значення азимуту. Така особливість є типовою для Wi-Fi середовища, оскільки канал змінюється під впливом завад, відбиттів і сторонніх рухів. Для підвищення надійності доцільно виконувати кілька послідовних вимірювань та усереднювати отримані оцінки.

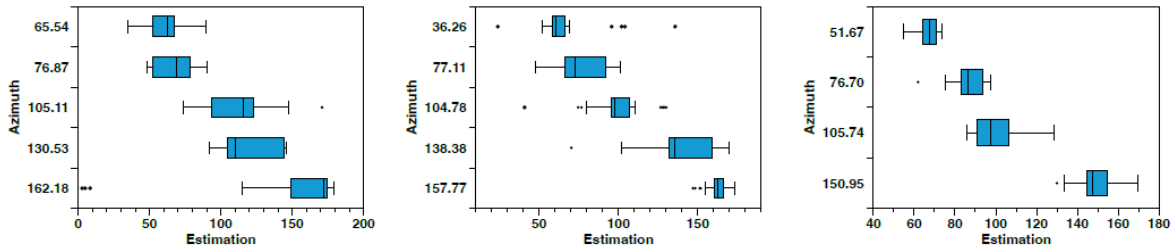


Рисунок 4.6 – Розподіл результатів локалізації для різних приміщень

На рисунку 4.7 демонструється, що похибка залежить не лише від приміщення, а й від конкретної моделі камери. Різні пристрої мають різну потужність передавання, конструкцію антени, інтенсивність трафіку та стабільність Wi-Fi з’єднання. Проте загальна працездатність методу зберігається для різних моделей, що підтверджує його універсальність.

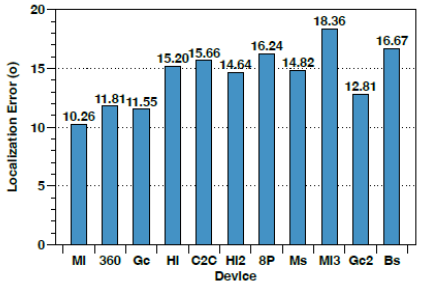


Рисунок 4.7 – Похибки локалізації для різних моделей Wi-Fi камер

Ефективність запропонованої системи доцільно оцінювати за сукупністю критеріїв. Перший критерій - точність локалізації, яка визначається середньою кутовою похибкою. Другий критерій - час виконання процедури, оскільки практичний засіб пошуку має працювати швидко. Третій критерій - кількість дій користувача. Четвертий критерій - вартість апаратної реалізації. П’ятий критерій - стабільність роботи в реальних приміщеннях. Всі оцінка ефективності кіберфізичної системи присутні на табл. 4.4.

Таблиця 4.4 – Оцінка ефективності кіберфізичної системи

Критерій ефективності	Характеристика для запропонованої системи
Точність	Оцінювання азимуту з похибкою, достатньою для звуження сектору пошуку
Швидкодія	Збір CSI виконується протягом короткого інтервалу обертання пластини
Зручність	Не потребує обходу кімнати та великої кількості дій користувача
Вартість	Базується на доступних компонентах: Raspberry Pi, Wi-Fi адаптері, двигуні та пластині
Масштабованість	Модулі збору, обробки і візуалізації можуть бути замінені або розширені
Обмеження	Залежить від якості CSI, наявності трафіку та умов багатопроменевості

До переваг системи належать низька вартість, компактність, відсутність потреби у попередньому навчанні, фізична пояснюваність результату та можливість роботи в обмеженому просторі. На відміну від методів, що потребують

проходження користувачем кількох траєкторій у кімнаті, запропонований підхід може працювати зі стаціонарного положення системи.

Разом з тим система має певні обмеження. Вона потребує наявності достатньої кількості пакетів від камери, підтримки збору CSI на апаратному рівні та відносно сприятливих умов для прояву дифракційного ослаблення. Якщо камера розташована в зоні без прямого або близького до прямого шляху сигналу, або якщо її екранує металевий предмет, точність може зменшуватися. Також можливе виникнення хибних провалів CSI через відбиття або завади.

Для підвищення ефективності доцільно передбачити повторні вимірювання, автоматичну оцінку якості сигналу, відкидання аномальних мінімумів, використання кількох піднесучих CSI і візуальне відображення довірчого сектору. У перспективі система може бути доповнена графічним інтерфейсом, автоматичним калібруванням нульового положення пластини та підтримкою кількох точок вимірювання для уточнення просторового положення камери.

Для доповнення аналізу ефективності у роботі використано скріншоти практичного запуску програмних модулів системи. Вони відображають послідовність перевірки приміщення: від задання схеми експерименту та запуску сканування Wi-Fi середовища до виявлення підозрілого пристрою і визначення кута його розташування.

На рисунку 4.8 показано схему приміщення, у якому проводилась перевірка. На плані відображено положення потенційної прихованої камери, напрямок виходу користувача з кімнати та просторові розміри контрольованої зони. Така схема дає змогу зіставити програмно визначений азимут із фактичним положенням об’єкта. Крім того, схема приміщення дозволяє врахувати вплив геометрії кімнати на поширення Wi-Fi сигналу. У реальних умовах сигнал може відбиватися від стін, меблів, дверей та інших поверхонь, що впливає на форму отриманих вимірювань. Тому порівняння результатів локалізації з планом кімнати є необхідним етапом аналізу достовірності експерименту. Якщо визначений системою напрямок збігається з областю розміщення камери, це підтверджує правильність роботи алгоритму. У випадку незначного відхилення результат також може вважатися

прийнятним, якщо він дозволяє звузити сектор ручного пошуку. Практична цінність такого підходу полягає в тому, що користувач отримує зрозумілий орієнтир для подальшої перевірки приміщення.

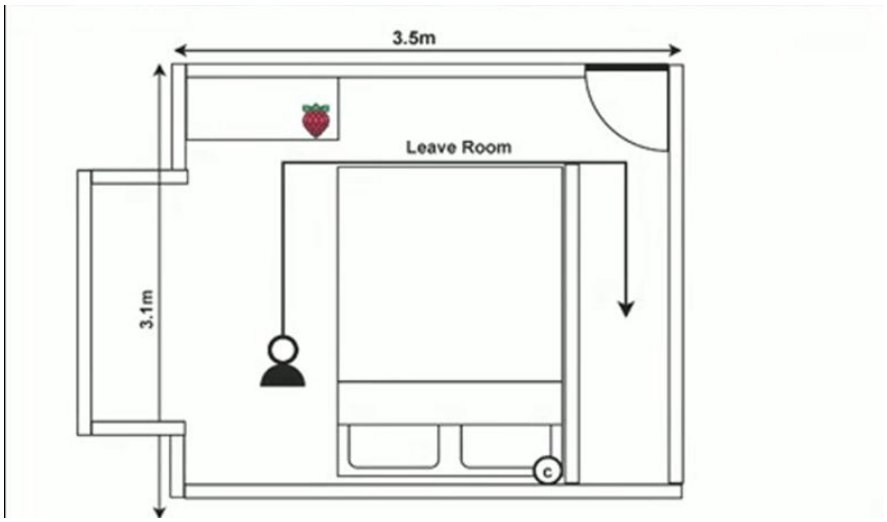


Рисунок 4.8 – Схема контрольованого приміщення для проведення експерименту з локалізації Wi-Fi камери

Рисунки 4.9–4.10 демонструють службовий етап підготовки до повторного запуску сканування. Після переривання попереднього процесу виконується переведення інтерфейсу у початковий стан і повторний запуск скрипта, що є типовою дією під час налаштування експериментального стенда. Цей етап не є основним результатом роботи системи, однак він показує послідовність дій, необхідних для стабільного проведення вимірювань. Повторний запуск сканування дозволяє перевірити, чи коректно звільнено мережевий інтерфейс після попереднього сеансу роботи. Також це дає змогу уникнути помилок, пов’язаних із зависанням процесу перехоплення пакетів або некоректним режимом роботи Wi-Fi адаптера. У процесі експерименту такі дії є важливими, оскільки забезпечують відтворюваність подальших вимірювань. Якщо інтерфейс не повернути у початковий стан, наступний запуск може дати неповні або спотворені результати. Тому службова підготовка перед повторним скануванням розглядається як

необхідна частина налаштування програмно-апаратного комплексу. Це підтверджує, що практична реалізація системи потребує не лише алгоритмів аналізу, а й правильної організації експериментального процесу.

```
    time.sleep(0.0015)
KeyboardInterrupt
Traceback (most recent call last):
  File "camsacn.py", line 215, in <module>
    main()
  File "camsacn.py", line 205, in main
    call_location_script(mac, channel)
  File "camsacn.py", line 168, in call_location_script
    subprocess.run(['python', 'locationfu.py', dangerous_d
evices, str(channel)], check=True)
  File "/usr/lib/python3.7/subprocess.py", line 474, in ru
n
    stdout, stderr = process.communicate(input, timeout=ti
meout)
  File "/usr/lib/python3.7/subprocess.py", line 931, in co
mmunicate
    self.wait()
  File "/usr/lib/python3.7/subprocess.py", line 990, in wa
it
    return self._wait(timeout=timeout)
  File "/usr/lib/python3.7/subprocess.py", line 1624, in _
wait
    (pid, sts) = self._try_wait(0)
  File "/usr/lib/python3.7/subprocess.py", line 1582, in _
try_wait
    (pid, sts) = os.waitpid(self.pid, wait_flags)
KeyboardInterrupt
(camscan_env) root@raspberrypi:/home/pi/PJ0# ip link set m
on0 down
(camscan_env) root@raspberrypi:/home/pi/PJ0# python camsac
n.py
```

Рисунок 4.9 – Стан виконання програми після переривання попереднього запуску скрипта

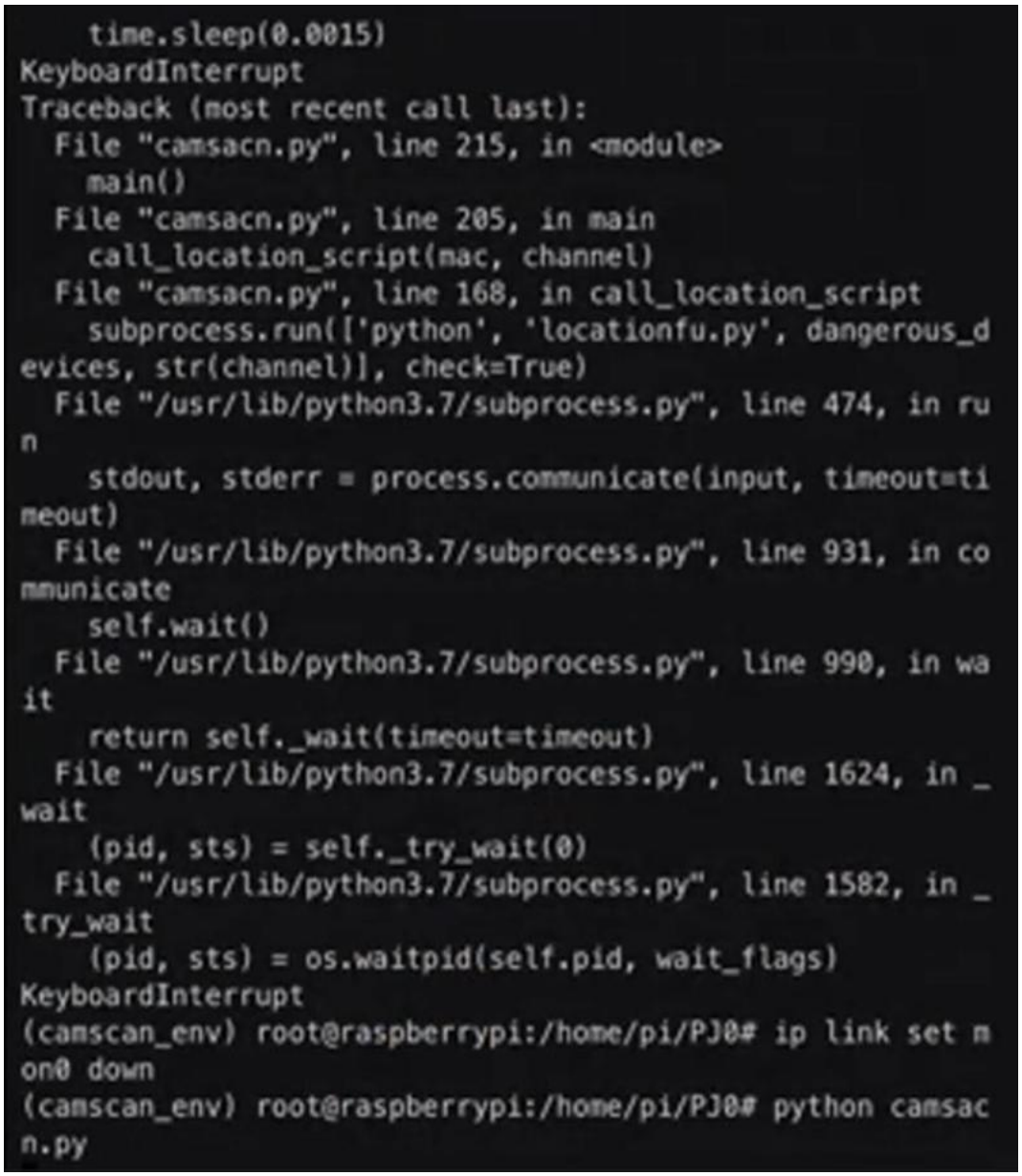


Рисунок 4.10 – Повторний запуск скрипта після скидання мережевого інтерфейсу

На рисунках 4.11–4.12 зафіксовано процес аналізу пакетів на різних каналах. Спочатку система не знаходить підозрілих пристроїв, однак під час сканування мережі purpleleaves виявляється пристрій з великою кількістю пакетів та значною середньою довжиною пакета, що відповідає ознакам активної передачі відеоданих. Такий результат свідчить про те, що алгоритм попереднього відбору не спрацьовує на всі пристрої однаково, а виділяє лише ті вузли, які мають характерну мережеву активність. Велика кількість пакетів може вказувати на постійний обмін даними

між пристроєм і мережею, що є типовим для камер, які передають відеопотік. Значна середня довжина пакета додатково підтверджує, що трафік може містити не лише службові повідомлення, а й корисні дані великого обсягу. Отже, на цьому етапі система формує список кандидатів для подальшої перевірки, не роблячи остаточного висновку про наявність прихованої камери. Це зменшує кількість пристроїв, які потрібно аналізувати на етапі локалізації, і скорочує загальний час експерименту. Таким чином, результати на рисунках 4.11–4.12 підтверджують працездатність етапу попереднього виявлення за трафіковими ознаками.

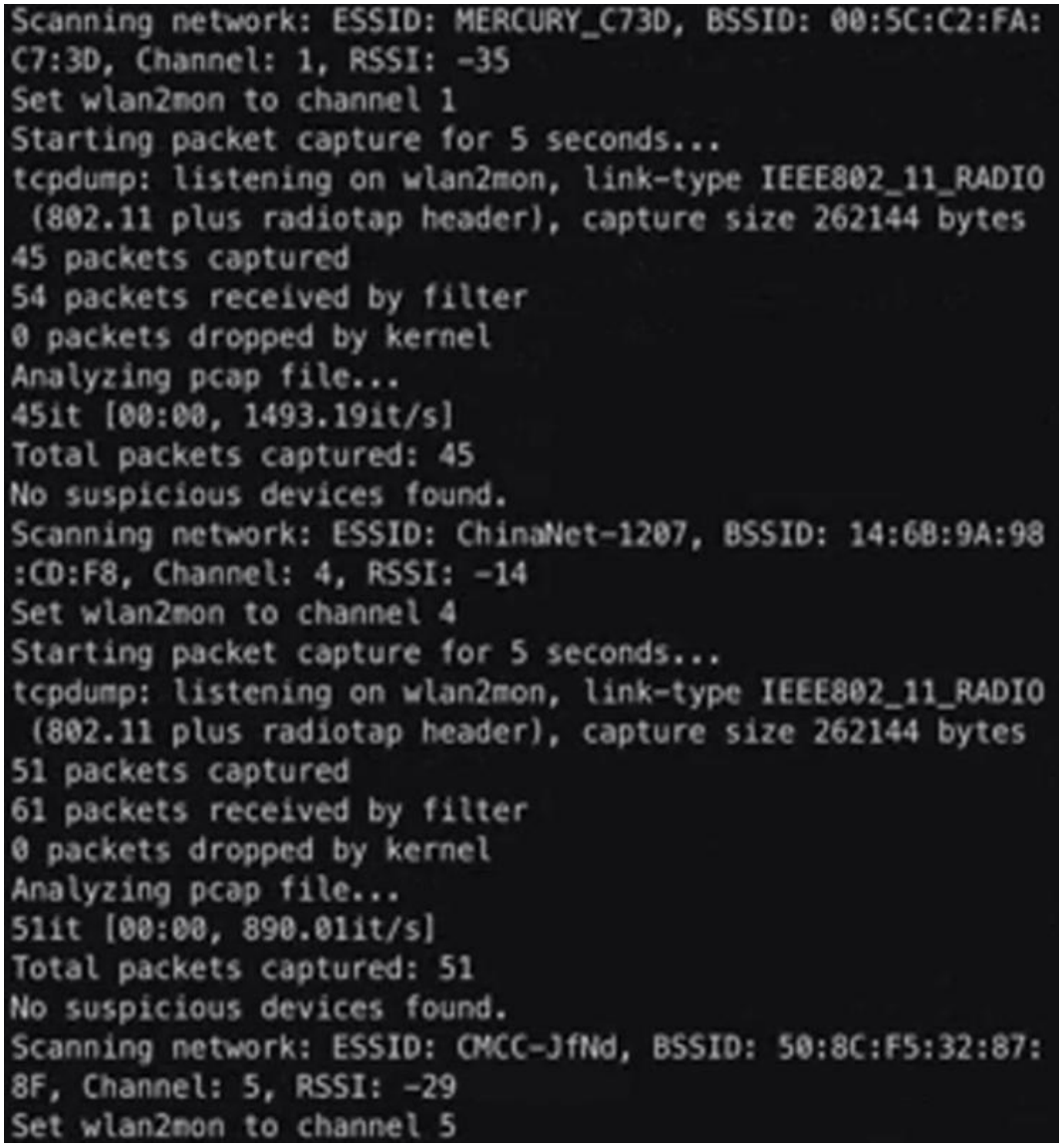


Рисунок 4.11 – Послідовне сканування Wi-Fi мереж і первинна перевірка наявності підозрілих пристроїв

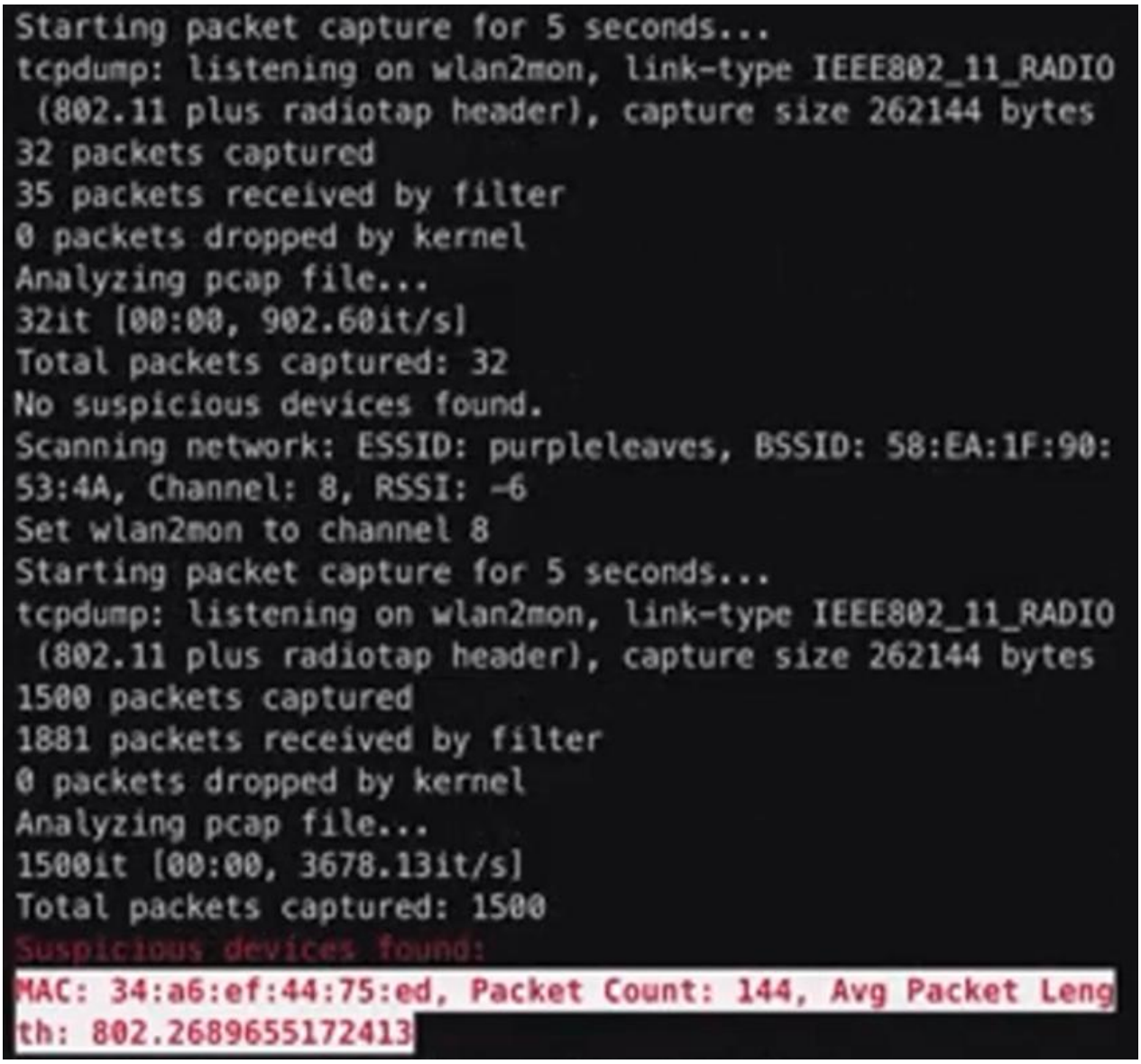


Рисунок 4.12 – Виявлення підозрілого пристрою за кількістю пакетів та середньою довжиною пакета

Рисунки 4.13–4.14 ілюструють завершальну частину експерименту. Після поглибленого аналізу MAC-адреса підозрілого пристрою передається до модуля локалізації, який налаштовує канал, запускає збір даних та визначає кут розташування небезпечного пристрою. Отримане значення 151,875° звужує сектор подальшого ручного огляду приміщення.

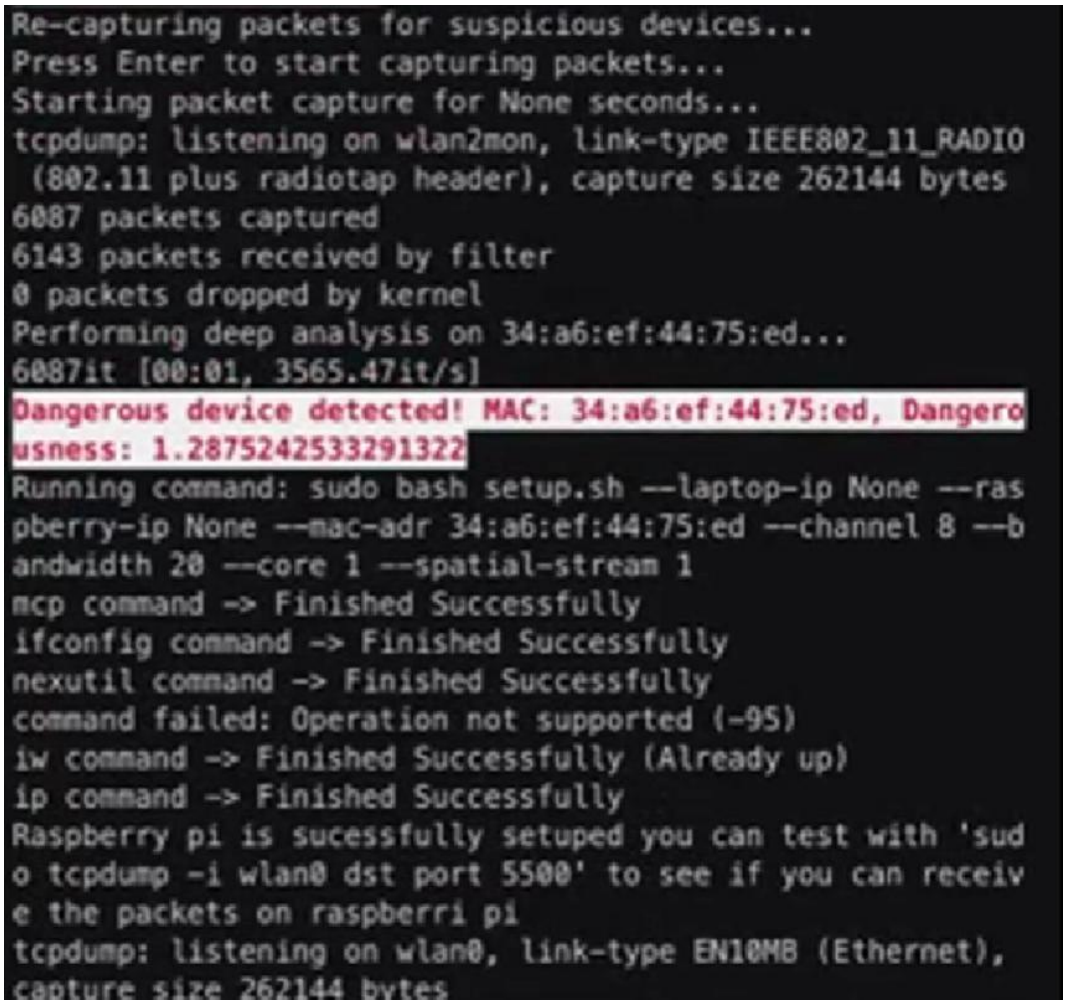


Рисунок 4.13 – Поглиблений аналіз підозрілого пристрою та запуск модуля локалізації

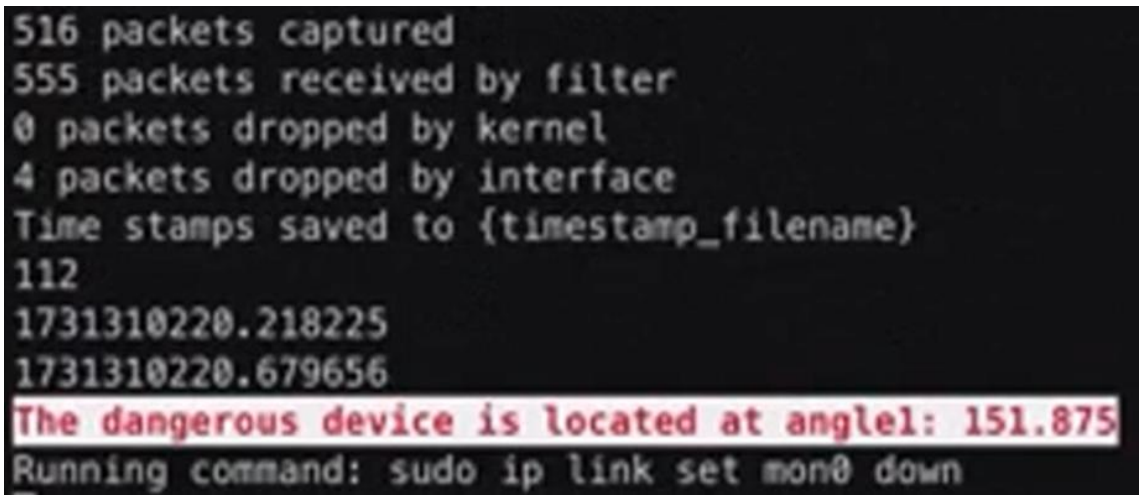


Рисунок 4.14 – Результат локалізації небезпечного пристрою з визначенням кута 151,875°

4.5 Висновки

У четвертому розділі розглянуто програмну реалізацію та експериментальне дослідження кіберфізичної системи виявлення і локалізації прихованих Wi-Fi камер у приміщеннях. Обґрунтовано вибір інструментальних засобів, до яких належать Raspberry Pi, Wi-Fi адаптер із підтримкою режиму моніторингу, програмні засоби збору CSI/RSSI-даних, кроковий двигун, драйвер керування та металева пластина.

Запропоновано архітектуру програмної моделі, яка складається з модулів сканування Wi-Fi середовища, аналізу мережевого трафіку, виявлення підозрілих пристроїв, збору CSI, керування дифракційним елементом, обробки сигналу та формування результату для користувача. Показано, що взаємодія програмної і фізичної частин утворює замкнений кіберфізичний цикл вимірювання.

Описано програмну реалізацію алгоритму, який спочатку виділяє підозрілий Wi-Fi пристрій за характеристиками трафіку, а потім визначає азимутальний напрямок на нього за допомогою аналізу дифракційного ослаблення CSI. Особливістю алгоритму є синхронізація часових міток вимірювань із кутовим положенням металевої пластини.

Сформовано план експериментального дослідження системи в різних приміщеннях і за різних положень камери. Основним показником ефективності визначено кутову похибку локалізації. Додатково враховуються кількість пакетів, якість CSI, час вимірювання, наявність багатопроменевості та вплив перешкод.

Аналіз результатів підтвердив практичну доцільність використання керованої дифракції та параметрів радіоканалу для локалізації прихованих Wi-Fi камер. Система є перспективною завдяки невисокій вартості, компактності, мінімальній участі користувача та відсутності потреби у попередньому навчанні для конкретного приміщення. Основними напрямами подальшого вдосконалення є підвищення точності, автоматичне калібрування, поліпшення стійкості до завад і розроблення зручного інтерфейсу користувача.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено кіберфізичну систему виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу. Система поєднує пасивний моніторинг Wi-Fi трафіку, аналіз CSI/RSSI-параметрів, кероване формування дифракційного впливу та програмну обробку даних для визначення азимутального напряму на підозрілий пристрій. У роботі набув подальшого розвитку метод, який дає змогу звузити сектор фізичного пошуку камери.

Також набув подальшого розвитку підхід до побудови кіберфізичних систем захисту приватності в приміщеннях. Він передбачає інтеграцію апаратних засобів збору радіоданих, модулів аналізу трафіку, алгоритмів обробки сигналів, механізму керованого впливу на радіоканал та засобів подання результатів користувачеві. Запропонований підхід орієнтований на доступні компоненти і не потребує дорогого обладнання.

Впровадження результатів роботи дозволило сформувати архітектуру переносного комплексу для перевірки житлових, офісних, готельних, навчальних і тимчасово орендованих приміщень. Практична значимість полягає у скороченні часу ручного огляду та визначенні напряму можливого розташування прихованої камери.

Поставлену мету було досягнуто шляхом розв’язання таких основних завдань:

– проаналізовано стан проблеми виявлення та локалізації прихованих Wi-Fi камер і визначено обмеження традиційних методів пошуку;

– досліджено існуючі підходи та обґрунтовано доцільність використання CSI/RSSI-характеристик і керованої дифракції електромагнітного сигналу;

– розроблено структурну та математичну модель кіберфізичної системи, у якій враховано зміну параметрів радіоканалу під час обертання металевої пластини, формування провалу амплітуди CSI та зв’язок цього провалу з кутовим положенням елемента;

– розроблено алгоритм попереднього виявлення підозрілих Wi-Fi пристроїв за MAC-адресами, кількістю пакетів, середнім розміром кадру, часткою висхідного трафіку та стабільністю передавання;

– розроблено алгоритм азимутальної локалізації, що виконує збір CSI-даних, синхронне обертання пластини, фільтрацію сигналу, пошук інтервалу максимального ослаблення та перетворення часової мітки в оцінений азимут;

– визначено вимоги до програмних та апаратно-програмних засобів, спроєктовано архітектуру комплексу і виконано програмну реалізацію основних модулів;

– проведено експериментальну перевірку, яка підтвердила працездатність запропонованого підходу та можливість використання системи для визначення напряму пошуку камери.

Аналіз результатів моделювання та експериментальних досліджень показав, що запропонована система ефективно звужує область пошуку прихованої камери. Її перевагами є низька вартість, відсутність попереднього навчання, мінімальна участь користувача та фізична пояснюваність результатів. Основними обмеженнями залишаються залежність від доступності CSI-даних, інтенсивності трафіку камери та багатопроменевості.

За темою кваліфікаційної роботи магістра опубліковано одну публікацію у матеріалах конференції ПЕРСИК 2026 (м. Харків, 23 квіт. 2026). Харків, 2026.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Cunningham R., Tan W. L. Detection and Localization of Hidden Wi-Fi Cameras. 2022 27th Asia Pacific Conference on Communications (APCC). 2022. P. 12–17. DOI: 10.1109/APCC55198.2022.9943725.

2. Zhang X. et al. DIFFLOC: WiFi Hidden Camera Localization Based on Electromagnetic Diffraction. *The 34th USENIX Security Symposium*. 2025. DOI: 10.5555/3766078.3766419.

3. Salman M., Dao N., Lee U., Noh Y. CSI:DeSpy: Enabling Effortless Spy Camera Detection via Passive Sensing of User Activities and Bitrate Variations. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 2022. Vol. 6, no. 2. Article 72. P. 1–27. DOI: 10.1145/3534593.

4. Dao D. N., Salman M., Noh Y. DeepDeSpy: A Deep Learning-Based Wireless Spy Camera Detection System. *IEEE Access*. 2021. Vol. 9. P. 145486–145497. DOI: 10.1109/ACCESS.2021.3121254.

5. Cheng Y., Ji X., Lu T., Xu W. On Detecting Hidden Wireless Cameras: A Traffic Pattern-based Approach. *IEEE Transactions on Mobile Computing*. 2020. Vol. 19, no. 4. P. 907–921. DOI: 10.1109/TMC.2019.2900919.

6. An H., Park W., Park S. Wireless Spy Camera Spotter System With Real-Time Traffic Similarity Analysis and WiFi Signal Tracing. *IEEE Access*. 2024. Vol. 12. P. 4459–4470. DOI: 10.1109/ACCESS.2024.3350175.

7. Sun W., Givehchian H., Bharadia D. Revealing Hidden IoT Devices through Passive Detection, Fingerprinting, and Localization. *Proceedings on Privacy Enhancing Technologies*. 2025. Vol. 2025, no. 1. P. 184–197. DOI: 10.56553/popets-2025-0011.

8. Ma Y., Zhou G., Wang S. WiFi Sensing with Channel State Information: A Survey. *ACM Computing Surveys*. 2019. Vol. 52, no. 3. Article 46. P. 1–36. DOI: 10.1145/3310194.

9. Wu K. et al. FILA: Fine-grained indoor localization. *IEEE INFOCOM 2012*. 2012. P. 2210–2218. DOI: 10.1109/INFCOM.2012.6195606.

10. Kotaru M. et al. SpotFi: Decimeter level localization using WiFi. *ACM SIGCOMM Computer Communication Review.* 2015. Vol. 45, no. 4. P. 269–282. DOI: 10.1145/2785956.2787487.

11. Vasisht D., Kumar S., Katabi D. Decimeter-level localization with a single WiFi access point. *13th USENIX Symposium on Networked Systems Design and Implementation.* 2016. P. 165–178. DOI: 10.5555/2930611.2930623.

12. Xiong J., Jamieson K. ArrayTrack: A fine-grained indoor location system. *10th USENIX Symposium on Networked Systems Design and Implementation*. 2013. P. 71–84. DOI: 10.5555/2482626.2482634.

13. Yang Z., Wu C., Liu Y. From RSSI to CSI: Indoor localization via channel response. *ACM Computing Surveys*. 2013. Vol. 46, no. 2. Article 25. DOI: 10.1145/2543581.2543592.

14. Ma Y., Zhou G., Wang S. WiFi sensing with channel state information: A survey. *ACM Computing Surveys*. 2019. Vol. 52, no. 3. Article 46. DOI: 10.1145/3310194.

15. Wang X. et al. DeepFi: Deep learning for indoor fingerprinting using channel state information. *2015 IEEE Wireless Communications and Networking Conference.* 2015. P. 1666–1671. DOI: 10.1109/WCNC.2015.7127718.

16. Che R. et al. Channel State Information Based Indoor Fingerprinting Localization: A Deep Learning Approach. **Sensors**. 2023. Vol. 23, no. 13. P. 5830. DOI: 10.3390/s23135830.

17. Cheng Y., Ji X., Lu T., Xu W. On detecting hidden wireless cameras: A traffic pattern-based approach. *IEEE Transactions on Mobile Computing*. 2020. Vol. 19, no. 4. P. 907–921. DOI: 10.1109/TMC.2019.2900919.

18. Dao D. N., Salman M., Noh Y. DeepDeSpy: A deep learning-based wireless spy camera detection system. *IEEE Access*. 2021. Vol. 9. P. 145486–145497. DOI: 10.1109/ACCESS.2021.3121254.

19. Salman M., Dao N., Lee U., Noh Y. CSI:DeSpy: Enabling effortless spy camera detection via passive sensing of user activities and bitrate variations. *Proceedings*

of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2022. Vol. 6, no. 2. Article 72. DOI: 10.1145/3534593.

20. Cunningham R., Tan W. L. Detection and localization of hidden Wi-Fi cameras. *2022 27th Asia Pacific Conference on Communications.* 2022. P. 12–17. DOI: 10.1109/APCC55198.2022.9943725.

21. An H., Park W., Park S. Wireless spy camera spotter system with real-time traffic similarity analysis and WiFi signal tracing. *IEEE Access.* 2024. Vol. 12. P. 4459–4470. DOI: 10.1109/ACCESS.2024.3350175.

22. Sun W., Givehchian H., Bharadia D. Revealing hidden IoT devices through passive detection, fingerprinting, and localization. *Proceedings on Privacy Enhancing Technologies.* 2025. Vol. 2025, no. 1. P. 184–197. DOI: 10.56553/popets-2025-0011.

23. Zhang X. et al. DIFFLOC: WiFi hidden camera localization based on electromagnetic diffraction. *The 34th USENIX Security Symposium*. 2025. DOI: 10.5555/3766078.3766419.

24. Zhao L. et al. A lightweight method for hidden camera detection and localization. *Information Retrieval Journal.* 2026. DOI: 10.1007/s10791-026-10114-z.

25. Keller J. B. Geometrical theory of diffraction. *Journal of the Optical Society of America*. 1962. Vol. 52, no. 2. P. 116–130. DOI: 10.1364/JOSA.52.000116.

26. Kouyoumjian R. G., Pathak P. H. A uniform geometrical theory of diffraction for an edge in a perfectly conducting surface. *Proceedings of the IEEE*. 1974. Vol. 62, no. 11. P. 1448–1461. DOI: 10.1109/PROC.1974.9381.

27. Holl P. M., Reinhard F. Holography of Wi-Fi radiation. *Physical Review Letters.* 2017. Vol. 118, no. 18. P. 183901. DOI: 10.1103/PhysRevLett.118.183901.

28. Azpilicueta L. et al. Analysis of radio wave propagation for ISM 2.4 GHz wireless sensor networks in inhomogeneous vegetation environments. *Sensors*. 2014. Vol. 14, no. 12. P. 23650–23672. DOI: 10.3390/s141223650.

29. Amzucu D. M., Ciuprina G., Vulpe A. Indoor radio propagation and interference in 2.4 GHz wireless sensor networks: Measurements and analysis. *Wireless Personal Communications.* 2014. Vol. 76. P. 759–774. DOI: 10.1007/s11277-014-1694-2.

30. He J. et al. A study on the diffraction correction prediction of electromagnetic signal propagation. *Wireless Communications and Mobile Computing*. 2021. Article 8136833. DOI: 10.1155/2021/8136833.

31. Ubom E. A. et al. Characterization of indoor propagation properties and performance evaluation for 2.4 GHz band Wi-Fi. *SSRN Electronic Journal*. 2019. DOI: 10.2139/ssrn.3391700.

32. Zhang X. et al. DIFFLOC: WiFi hidden camera localization based on electromagnetic diffraction. *The 34th USENIX Security Symposium*. 2025. DOI: 10.5555/3766078.3766419.

33. Humayed A., Lin J., Li F., Luo B. Cyber-physical systems security — A survey. *IEEE Internet of Things Journal*. 2017. Vol. 4, no. 6. P. 1802–1831. DOI: 10.1109/JIOT.2017.2703172.

34. Yaacoub J. P. A. et al. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*. 2020. Vol. 77. P. 103201. DOI: 10.1016/j.micpro.2020.103201

35. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues. *Computers in Industry*. 2018. Vol. 100. P. 212–223. DOI: 10.1016/j.compind.2018.04.017.

36. Ashibani Y., Mahmoud Q. H. Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*. 2017. Vol. 68. P. 81–97. DOI: 10.1016/j.cose.2017.04.005.

37. Giraldo J. et al. Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Design & Test.* 2017. Vol. 34, no. 4. P. 7–17. DOI: 10.1109/MDAT.2017.2709310.

38. Dudykevych V. et al. ZigBee, Wi-Fi and Bluetooth wireless sensor networks in cyber-physical systems: The “object–threat–protection” concept based on the OSI model. *Information Processing Systems.* 2019. No. 2(157). P. 114–120. DOI: 10.30748/soi.2019.157.16.

39. Gunduz M. Z., Das R. Cyber-security on smart grid: Threats and potential solutions. *Computer Networks.* 2020. Vol. 169. P. 107094. DOI: 10.1016/j.comnet.2019.107094.

40. Ali S. et al. Network challenges for cyber physical systems with tiny wireless devices: A case study on reliable pipeline condition monitoring. *Sensors*. 2015. Vol. 15, no. 4. P. 7172–7205. DOI: 10.3390/s150407172.

41. Yang Z., Wu C., Liu Y. Locating in fingerprint space: Wireless indoor localization with little human intervention. *MobiCom 2012*. 2012. P. 269–280. DOI: 10.1145/2348543.2348578.

42. Wu K. et al. FILA: Fine-grained indoor localization. *IEEE INFOCOM 2012.* 2012. P. 2210–2218. DOI: 10.1109/INFCOM.2012.6195606.

43. Kotaru M. et al. SpotFi: Decimeter level localization using WiFi. *ACM SIGCOMM Computer Communication Review*. 2015. Vol. 45, no. 4. P. 269–282. DOI: 10.1145/2785956.2787487.

44. Xiong J., Jamieson K. ArrayTrack: A fine-grained indoor location system. *10th USENIX Symposium on Networked Systems Design and Implementation*. 2013. P. 71–84. DOI: 10.5555/2482626.2482634.

45. Vasisht D., Kumar S., Katabi D. Decimeter-level localization with a single WiFi access point. *13th USENIX Symposium on Networked Systems Design and Implementation.* 2016. P. 165–178. DOI: 10.5555/2930611.2930623.

46. Hu Y. et al. Channel state information-based wireless localization by subspace projection. *EURASIP Journal on Wireless Communications and Networking.* 2023. Article 23. DOI: 10.1186/s13638-023-02303-x.

47. Li X. et al. IndoTrack: Device-free indoor human tracking with commodity Wi-Fi. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies.* 2017. Vol. 1, no. 3. Article 72. DOI: 10.1145/3130940.

48. Ma Y., Zhou G., Wang S. WiFi sensing with channel state information: A survey. *ACM Computing Surveys.* 2019. Vol. 52, no. 3. Article 46. DOI: 10.1145/3310194.

49. Yoo J. et al. Indoor localization based on Wi-Fi received signal strength indicators: Feature extraction, mobile fingerprinting, and trajectory learning. *Applied Sciences*. 2019. Vol. 9, no. 18. P. 3930. DOI: 10.3390/app9183930.

50. Yang C. et al. Survey on WiFi-based indoor positioning techniques. *IET Communications*. 2020. Vol. 14, no. 9. P. 1372–1383. DOI: 10.1049/iet-com.2019.1059.

51. Dai J. et al. A survey of latest Wi-Fi assisted indoor positioning on different platforms. 2023. Vol. 23, no. 18. P. 7961. DOI: 10.3390/s23187961.

52. Yang T. et al. A survey of recent indoor localization scenarios and methodologies. 2021. Vol. 21, no. 23. P. 8086. DOI: 10.3390/s21238086.

53. Khattak S. B. A. et al. WLAN RSS-based fingerprinting for indoor localization. 2022. Vol. 22, no. 14. P. 5236. DOI: 10.3390/s22145236.

54. Karakusak M. Z., et al. RSS-based wireless LAN indoor localization and tracking using deep architectures. 2022. Vol. 22, no. 17. P. 6431. DOI: 10.3390/s22176431.

55. Che R. et al. Channel State Information Based Indoor Fingerprinting Localization: A Deep Learning Approach. 2023. Vol. 23, no. 13. P. 5830. DOI: 10.3390/s23135830.

56. Yang Z., Wu C., Liu Y. From RSSI to CSI: Indoor localization via channel response. *ACM Computing Surveys*. 2013. Vol. 46, no. 2. Article 25. DOI: 10.1145/2543581.2543592.

57. Sivanathan A. et al. Characterizing and classifying IoT traffic in smart cities and campuses. *IEEE INFOCOM Workshops*. 2017. P. 559–564. DOI: 10.1109/INFCOMW.2017.8116438.

58. Sivanathan A. et al. Classifying IoT devices in smart environments using network traffic characteristics. *IEEE Transactions on Mobile Computing*. 2019. Vol. 18, no. 8. P. 1745–1759. DOI: 10.1109/TMC.2018.2866249.

59. Meidan Y. et al. Detection of unauthorized IoT devices using machine learning techniques. *arXiv / Wireless Communications and Mobile Computing*. 2017. DOI: 10.1002/wcm.2951.

60. Meidan Y. et al. N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing.* 2018. Vol. 17, no. 3. P. 12–22. DOI: 10.1109/MPRV.2018.03367731.

61. Miettinen M. et al. IoT Sentinel: Automated device-type identification for security enforcement in IoT. *2017 IEEE 37th International Conference on Distributed Computing Systems.* 2017. P. 2177–2184. DOI: 10.1109/ICDCS.2017.283.

62. Chowdhury R. R. et al. Network traffic analysis based IoT device identification. *Proceedings of the 2020 ACM Workshop on Big Data, IoT, and Machine Learning.* 2020. P. 79–84. DOI: 10.1145/3421537.3421545.

63. Hamad S. A. et al. IoT device identification via network-flow based fingerprinting and learning. *2019 IEEE 44th Conference on Local Computer Networks.* 2019. P. 103–111. DOI: 10.1109/LCN44214.2019.8990868.

64. Oser P. et al. Automatic fingerprinting of vulnerable BLE IoT devices with static UUIDs from mobile apps. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.* 2019. P. 1469–1483. DOI: 10.1145/3319535.3354240.

65. Miettinen M. et al. IoT Sentinel: Automated device-type identification for security enforcement in IoT. *2017 IEEE 37th International Conference on Distributed Computing Systems.* 2017. P. 2177–2184. DOI: 10.1109/ICDCS.2017.283.

66. Sivanathan A. et al. Classifying IoT devices in smart environments using network traffic characteristics. *IEEE Transactions on Mobile Computing*. 2019. Vol. 18, no. 8. P. 1745–1759. DOI: 10.1109/TMC.2018.2866249.

67. Meidan Y. et al. N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*. 2018. Vol. 17, no. 3. P. 12–22. DOI: 10.1109/MPRV.2018.03367731.

68. Chowdhury R. R. et al. Network traffic analysis based IoT device identification. *Proceedings of the 2020 ACM Workshop on Big Data, IoT, and Machine Learning.* 2020. P. 79–84. DOI: 10.1145/3421537.3421545.

69. Hamad S. A. et al. IoT device identification via network-flow based fingerprinting and learning. *2019 IEEE 44th Conference on Local Computer Networks.* 2019. P. 103–111. DOI: 10.1109/LCN44214.2019.8990868.

70. Marchal S. et al. AuDI: Toward autonomous IoT device-type identification using periodic communication. *IEEE Journal on Selected Areas in Communications.* 2019. Vol. 37, no. 6. P. 1402–1412. DOI: 10.1109/JSAC.2019.2904364.

71. Bezawada B. et al. Behavioral fingerprinting of IoT devices. *Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security.* 2018. P. 41–50. DOI: 10.1145/3266444.3266452.

72. Liu L. et al. IDENTIFY: Intelligent device identification using traffic-based fingerprinting and machine learning. *Internet of Things*. 2025. Vol. 30. P. 101407. DOI: 10.1016/j.iot.2025.101407.

73. Ma Y., Zhou G., Wang S. WiFi Sensing with Channel State Information: A Survey. *ACM Computing Surveys*. 2019. Vol. 52, no. 3. Article 46. P. 1–36. DOI: 10.1145/3310194.

74. Wu D. et al. Device-Free WiFi Human Sensing: From Pattern-Based to Model-Based Approaches. *IEEE Communications Magazine*. 2017. Vol. 55, no. 10. P. 91–97. DOI: 10.1109/MCOM.2017.1700143.

75. Wang Y. et al. E-eyes: Device-free Location-oriented Activity Identification Using Fine-grained WiFi Signatures. *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking.* 2014. P. 617–628. DOI: 10.1145/2639108.2639143.

76. Pu Q., Gupta S., Gollakota S., Patel S. Whole-home Gesture Recognition Using Wireless Signals. *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*. 2013. P. 27–38. DOI: 10.1145/2500423.2500436.

77. Wang Y., Wu K., Ni L. M. WiFall: Device-Free Fall Detection by Wireless Networks. *IEEE Transactions on Mobile Computing.* 2017. Vol. 16, no. 2. P. 581–594. DOI: 10.1109/TMC.2016.2557792.

78. Yang J. et al. SenseFi: A Library and Benchmark on Deep-Learning-Empowered WiFi Human Sensing. 2023. Vol. 4, no. 3. Article 100703. DOI: 10.1016/j.patter.2023.100703.

79. Armenta-Garcia J. A., Gonzalez-Navarro F. F., Caro-Gutierrez J. Wireless Sensing Applications with Wi-Fi Channel State Information, Preprocessing Techniques, and Detection Algorithms: A Survey. *Computer Communications*. 2024. P. 254–274. DOI: 10.1016/j.comcom.2024.06.011.

80. Miao F. et al. Wi-Fi Sensing Techniques for Human Activity Recognition: Brief Survey, Potential Challenges, and Research Directions. *ACM Computing Surveys.* 2025. Vol. 57, no. 5. Article 107. P. 1–30. DOI: 10.1145/3705893.

81. Яцків В., Ткаченко Д. Кіберфізична системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу ПерСик 2026, Харків, Україна, 23 квіт. 2026

82. Міні камера А9 з датчиком руху Wifi. URL: https://rivcont.com/mini-kamera-a9-c-datchikom-dvizheniya-wifi/ (дата звернення 15.04.2026).

83. Мікрокомп'ютер Raspberry Pi 4 Model B 2GB. URL: https://rozetka.com.ua/ua/415934619/p415934619/ (дата звернення 20.03.2026).

.

ДОДАТОК А
(обов'язковий)

Лістинг програмної реалізації кіберфізичної системи виявлення та локалізації прихованих Wi-Fi камер

Модуль config.py — модуль «Задання конфігураційних параметрів кіберфізичної системи виявлення та локалізації прихованих Wi-Fi камер у приміщенні».

```
from dataclasses import dataclass
from typing import Tuple


@dataclass
class SystemConfig:
    """
    Конфігураційні параметри кіберфізичної системи
    виявлення та локалізації прихованих Wi-Fi камер.
    """

    # Wi-Fi інтерфейс у режимі monitor mode
    monitor_interface: str = "wlan0mon"

    # Пороги для попереднього виявлення підозрілих пристроїв
    min_average_payload_size: int = 300
    min_packet_count: int = 150

    # Тривалість пасивного захоплення Wi-Fi трафіку, с
    traffic_capture_time: int = 30

    # Файл з CSI-даними
    csi_csv_file: str = "csi_capture.csv"

    # Файл із часовими мітками та кутами повороту пластини
    motor_log_file: str = "motor_angles.csv"

    # Параметри крокового двигуна
    step_delay: float = 0.002
    steps_per_revolution: int = 4096

    # Сектор обертання металевої пластини
    start_angle: float = 0.0
    end_angle: float = 180.0
    angle_step: float = 1.0

    # GPIO-піни Raspberry Pi для ULN2003
    motor_pins: Tuple[int, int, int, int] = (17, 18, 27, 22)
```

```
    # Параметри цифрової обробки CSI
    smoothing_window: int = 7
    attenuation_percentile: float = 0.15
```

Модуль models.py — модуль «Опис структур даних для збереження параметрів Wi-Fi пристроїв, CSI-відліків, підозрілих об’єктів та кутів повороту металевої пластини».

```
from dataclasses import dataclass
from typing import Optional


@dataclass
class DeviceTrafficStats:
    """
    Статистика трафіку окремого Wi-Fi пристрою.
    """

    mac: str
    packet_count: int
    total_payload_size: int
    channel: Optional[int] = None

    @property
    def average_payload_size(self) -> float:
        if self.packet_count == 0:
            return 0.0
        return self.total_payload_size / self.packet_count


@dataclass
class SuspiciousDevice:
    """
    Опис пристрою, який має ознаки Wi-Fi камери.
    """

    mac: str
    channel: Optional[int]
    packet_count: int
    average_payload_size: float


@dataclass
class CsiSample:
    """
    Один відлік CSI-даних.
    """

    timestamp: float
```

```
    amplitude: float


@dataclass
class MotorAngleSample:
    """
    Один відлік положення металевої пластини.
    """

    timestamp: float
    angle: float
```

Модуль traffic_analyzer.py — модуль «Пасивний аналіз Wi-Fi трафіку для виявлення пристроїв з ознаками передавання відеопотоку та формування списку підозрілих Wi-Fi камер».

```
from typing import Dict, List, Optional

from config import SystemConfig
from models import DeviceTrafficStats, SuspiciousDevice

try:
    from scapy.all import sniff, Dot11, RadioTap
except ImportError:
    sniff = None
    Dot11 = None
    RadioTap = None


class WiFiTrafficAnalyzer:
    """
    Модуль пасивного аналізу Wi-Fi трафіку.

    Його завдання:
    - перехоплювати 802.11 пакети;
    - відбирати Data-кадри;
    - групувати пакети за MAC-адресами;
    - знаходити пристрої з ознаками відеопотоку.
    """

    def __init__(self, config: SystemConfig):
        self.config = config
        self.devices: Dict[str, DeviceTrafficStats] = {}

    def _extract_channel(self, packet) -> Optional[int]:
        """
        Отримання номера Wi-Fi каналу з Radiotap-заголовка.
        """
        try:
            if packet.haslayer(RadioTap):
```

```
                freq = packet[RadioTap].ChannelFrequency
                return self._frequency_to_channel(freq)
        except Exception:
            return None

        return None

    @staticmethod
    def _frequency_to_channel(freq: int) -> Optional[int]:
        """
        Перетворення частоти Wi-Fi у номер каналу.
        """
        if 2412 <= freq <= 2472:
            return int((freq - 2407) / 5)

        if freq == 2484:
            return 14

        if 5000 <= freq <= 5900:
            return int((freq - 5000) / 5)

        return None

    def _packet_handler(self, packet) -> None:
        """
        Обробка одного перехопленого Wi-Fi пакета.
        """
        if not packet.haslayer(Dot11):
            return

        dot11 = packet[Dot11]

        # type=2 відповідає Data frame у стандарті 802.11
        if dot11.type != 2:
            return

        source_mac = dot11.addr2

        if source_mac is None:
            return

        payload_size = len(bytes(packet.payload))
        channel = self._extract_channel(packet)

        if source_mac not in self.devices:
            self.devices[source_mac] = DeviceTrafficStats(
                mac=source_mac,
                packet_count=0,
                total_payload_size=0,
                channel=channel
            )

        self.devices[source_mac].packet_count += 1
```

```
        self.devices[source_mac].total_payload_size += payload_size

        if channel is not None:
            self.devices[source_mac].channel = channel

    def capture_traffic(self) -> None:
        """
        Запуск пасивного захоплення Wi-Fi трафіку.
        """
        if sniff is None:
            raise RuntimeError(
                "Бібліотека scapy не встановлена. "
                "Встановіть її командою: pip install scapy"
            )

        print("[INFO] Початок пасивного захоплення Wi-Fi трафіку")
        print(f"[INFO] Інтерфейс: {self.config.monitor_interface}")
        print(f"[INFO] Тривалість:
{self.config.traffic_capture_time} c")

        sniff(
            iface=self.config.monitor_interface,
            prn=self._packet_handler,
            timeout=self.config.traffic_capture_time,
            store=False
        )

        print("[INFO] Захоплення трафіку завершено")

    def find_suspicious_devices(self) -> List[SuspiciousDevice]:
        """
        Пошук пристроїв, які мають ознаки Wi-Fi камери.

        Ознаки:
        - велика кількість Data-кадрів;
        - великий середній розмір корисного навантаження.
        """
        suspicious_devices: List[SuspiciousDevice] = []

        for mac, stats in self.devices.items():
            if (
                stats.packet_count >= self.config.min_packet_count
                and stats.average_payload_size >=
self.config.min_average_payload_size
            ):
                suspicious_devices.append(
                    SuspiciousDevice(
                        mac=mac,
                        channel=stats.channel,
                        packet_count=stats.packet_count,

average_payload_size=stats.average_payload_size
                    )
```

```
                )

        suspicious_devices.sort(
            key=lambda device: (
                device.packet_count,
                device.average_payload_size
            ),
            reverse=True
        )

        return suspicious_devices

    def print_report(self, suspicious_devices:
List[SuspiciousDevice]) -> None:
        """
        Виведення звіту про знайдені Wi-Fi пристрої.
        """
        print("\n========== ЗВІТ ПРО WI-FI ПРИСТРОЇ ==========")

        if not self.devices:
            print("Пакети не були виявлені.")
            return

        for mac, stats in self.devices.items():
            print(
                f"MAC: {mac:17s} | "
                f"Канал: {str(stats.channel):>4s} | "
                f"Пакетів: {stats.packet_count:5d} | "
                f"Середній розмір: {stats.average_payload_size:8.2f}
байт"
            )

        print("\n========== ПІДОЗРІЛІ ПРИСТРОЇ ==========")

        if not suspicious_devices:
            print("Підозрілих пристроїв за заданими порогами не
виявлено.")
            return

        for index, device in enumerate(suspicious_devices, start=1):
            print(
                f"{index}. MAC: {device.mac}, "
                f"канал: {device.channel}, "
                f"пакетів: {device.packet_count}, "
                f"середній розмір: {device.average_payload_size:.2f}
байт"
            )
```

Модуль motor_controller.py — модуль «Керування кроковим двигуном для обертання металевої пластини та створення контрольованого дифракційного ослаблення радіосигналу».

```
import csv
import time
from typing import List, Tuple

from config import SystemConfig
from models import MotorAngleSample

try:
    import RPi.GPIO as GPIO
except ImportError:
    GPIO = None


class StepperMotorController:
    """
    Модуль керування кроковим двигуном.

    Двигун обертає металеву пластину навколо Wi-Fi приймача.
    Під час обертання фіксуються часові мітки та кути повороту.
    """

    HALF_STEP_SEQUENCE = [
        (1, 0, 0, 0),
        (1, 1, 0, 0),
        (0, 1, 0, 0),
        (0, 1, 1, 0),
        (0, 0, 1, 0),
        (0, 0, 1, 1),
        (0, 0, 0, 1),
        (1, 0, 0, 1),
    ]

    def __init__(self, config: SystemConfig, simulation: bool =
False):
        self.config = config
        self.simulation = simulation or GPIO is None

        if self.simulation:
            print("[WARN] GPIO недоступний. Увімкнено режим
симуляції.")
        else:
            GPIO.setmode(GPIO.BCM)

            for pin in self.config.motor_pins:
                GPIO.setup(pin, GPIO.OUT)
                GPIO.output(pin, 0)

    def _set_pins(self, values: Tuple[int, int, int, int]) -> None:
        """
        Встановлення стану GPIO-пінів.
        """
        if self.simulation:
```

```
            return

        for pin, value in zip(self.config.motor_pins, values):
            GPIO.output(pin, value)

    def _single_step(self, direction: int = 1) -> None:
        """
        Виконання одного кроку двигуна.
        """
        sequence = self.HALF_STEP_SEQUENCE

        if direction < 0:
            sequence = list(reversed(sequence))

        for pattern in sequence:
            self._set_pins(pattern)
            time.sleep(self.config.step_delay)

    def rotate_to_angle_range(self) -> List[MotorAngleSample]:
        """
        Обертання металевої пластини у заданому секторі.
        """
        angle_samples: List[MotorAngleSample] = []

        current_angle = self.config.start_angle
        steps_per_degree = self.config.steps_per_revolution / 360.0

        steps_for_angle_step = max(
            1,
            int(steps_per_degree * self.config.angle_step)
        )

        print("\n[INFO] Початок повороту металевої пластини")
        print(
            f"[INFO] Сектор: {self.config.start_angle}° - "
            f"{self.config.end_angle}°"
        )

        while current_angle <= self.config.end_angle:
            timestamp = time.time()

            angle_samples.append(
                MotorAngleSample(
                    timestamp=timestamp,
                    angle=current_angle
                )
            )

            print(f"[MOTOR] t={timestamp:.3f},
angle={current_angle:.2f}°")

            for _ in range(steps_for_angle_step):
                self._single_step(direction=1)
```

```
            current_angle += self.config.angle_step

        self._release_motor()
        self._save_motor_log(angle_samples)

        print("[INFO] Поворот металевої пластини завершено")

        return angle_samples

    def _release_motor(self) -> None:
        """
        Вимкнення обмоток двигуна.
        """
        self._set_pins((0, 0, 0, 0))

    def _save_motor_log(self, samples: List[MotorAngleSample]) ->
None:
        """
        Збереження часових міток і кутів у CSV-файл.
        """
        with open(
            self.config.motor_log_file,
            "w",
            newline="",
            encoding="utf-8"
        ) as file:
            writer = csv.writer(file)
            writer.writerow(["timestamp", "angle"])

            for sample in samples:
                writer.writerow([sample.timestamp, sample.angle])

        print(f"[INFO] Лог кутів збережено:
{self.config.motor_log_file}")

    def cleanup(self) -> None:
        """
        Завершення роботи з GPIO.
        """
        if not self.simulation:
            self._release_motor()
            GPIO.cleanup()
```

Модуль csi_processor.py — модуль «Обробка CSI-даних для виявлення області максимального ослаблення сигналу та визначення азимутального напрямку на приховану Wi-Fi камеру».

```
import csv
import math
```

```
import statistics
from typing import List, Optional

from config import SystemConfig
from models import CsiSample, MotorAngleSample


class CsiProcessor:
    """
    Модуль обробки CSI-даних.

    Основне завдання модуля:
    - завантажити CSI-амплітуди;
    - згладити сигнал;
    - знайти область дифракційного ослаблення;
    - визначити середину провалу;
    - зіставити її з кутом повороту металевої пластини.
    """

    def __init__(self, config: SystemConfig):
        self.config = config

    def load_csi_from_csv(self, filename: Optional[str] = None) ->
List[CsiSample]:
        """
        Завантаження CSI-даних із CSV-файлу.

        Очікуваний формат:
            timestamp, amplitude
        """
        filename = filename or self.config.csi_csv_file
        samples: List[CsiSample] = []

        with open(filename, "r", encoding="utf-8") as file:
            reader = csv.DictReader(file)

            for row in reader:
                samples.append(
                    CsiSample(
                        timestamp=float(row["timestamp"]),
                        amplitude=float(row["amplitude"])
                    )
                )

        if not samples:
            raise RuntimeError("Файл CSI не містить даних.")

        print(f"[INFO] Завантажено {len(samples)} CSI-відліків")

        return samples

    def smooth_signal(self, samples: List[CsiSample]) ->
List[CsiSample]:
```

```
        """
        Згладжування CSI-сигналу ковзним середнім.
        """
        window = self.config.smoothing_window

        if window <= 1:
            return samples

        smoothed: List[CsiSample] = []
        amplitudes = [sample.amplitude for sample in samples]

        for i, sample in enumerate(samples):
            left = max(0, i - window // 2)
            right = min(len(samples), i + window // 2 + 1)

            local_mean = statistics.mean(amplitudes[left:right])

            smoothed.append(
                CsiSample(
                    timestamp=sample.timestamp,
                    amplitude=local_mean
                )
            )

        return smoothed

    def normalize_signal(self, samples: List[CsiSample]) ->
List[CsiSample]:
        """
        Нормалізація CSI-амплітуди до діапазону 0...1.
        """
        amplitudes = [sample.amplitude for sample in samples]

        min_amp = min(amplitudes)
        max_amp = max(amplitudes)

        if math.isclose(max_amp, min_amp):
            return [
                CsiSample(sample.timestamp, 1.0)
                for sample in samples
            ]

        normalized: List[CsiSample] = []

        for sample in samples:
            value = (sample.amplitude - min_amp) / (max_amp -
min_amp)

            normalized.append(
                CsiSample(
                    timestamp=sample.timestamp,
                    amplitude=value
                )
```

```
            )

        return normalized

    def find_attenuation_midpoint(self, samples: List[CsiSample]) ->
float:
        """
        Пошук середини області максимального ослаблення CSI.

        У запропонованій системі вважається, що саме середина
        дифракційного провалу відповідає напрямку на Wi-Fi камеру.
        """
        amplitudes = sorted(sample.amplitude for sample in samples)

        threshold_index = int(
            len(amplitudes) * self.config.attenuation_percentile
        )

        threshold_index = max(
            0,
            min(threshold_index, len(amplitudes) - 1)
        )

        threshold = amplitudes[threshold_index]

        attenuation_times = [
            sample.timestamp
            for sample in samples
            if sample.amplitude <= threshold
        ]

        if not attenuation_times:
            raise RuntimeError("Не знайдено області ослаблення
CSI.")

        start_time = min(attenuation_times)
        end_time = max(attenuation_times)
        midpoint_time = (start_time + end_time) / 2.0

        print("\n========== АНАЛІЗ CSI ==========")
        print(f"Поріг ослаблення: {threshold:.4f}")
        print(f"Початок ослаблення: {start_time:.3f}")
        print(f"Кінець ослаблення: {end_time:.3f}")
        print(f"Середина ослаблення: {midpoint_time:.3f}")

        return midpoint_time

    def load_motor_angles(
        self,
        filename: Optional[str] = None
    ) -> List[MotorAngleSample]:
        """
        Завантаження журналу кутів повороту металевої пластини.
```

```
        """
        filename = filename or self.config.motor_log_file
        samples: List[MotorAngleSample] = []

        with open(filename, "r", encoding="utf-8") as file:
            reader = csv.DictReader(file)

            for row in reader:
                samples.append(
                    MotorAngleSample(
                        timestamp=float(row["timestamp"]),
                        angle=float(row["angle"])
                    )
                )

        if not samples:
            raise RuntimeError("Файл кутів двигуна не містить
даних.")

        return samples

    def interpolate_angle(
        self,
        motor_samples: List[MotorAngleSample],
        target_time: float
    ) -> float:
        """
        Визначення кута пластини за часовою міткою.
        """
        motor_samples = sorted(
            motor_samples,
            key=lambda sample: sample.timestamp
        )

        if target_time <= motor_samples[0].timestamp:
            return motor_samples[0].angle

        if target_time >= motor_samples[-1].timestamp:
            return motor_samples[-1].angle

        for i in range(len(motor_samples) - 1):
            left = motor_samples[i]
            right = motor_samples[i + 1]

            if left.timestamp <= target_time <= right.timestamp:
                dt = right.timestamp - left.timestamp

                if math.isclose(dt, 0.0):
                    return left.angle

                ratio = (target_time - left.timestamp) / dt

                return left.angle + ratio * (right.angle -
```

```
left.angle)

        return motor_samples[-1].angle

    def estimate_azimuth(self) -> float:
        """
        Повний цикл оцінювання азимуту прихованої Wi-Fi камери.
        """
        raw_csi = self.load_csi_from_csv()
        smoothed_csi = self.smooth_signal(raw_csi)
        normalized_csi = self.normalize_signal(smoothed_csi)

        midpoint_time =
self.find_attenuation_midpoint(normalized_csi)

        motor_samples = self.load_motor_angles()
        azimuth = self.interpolate_angle(motor_samples,
midpoint_time)

        print("\n========== РЕЗУЛЬТАТ ЛОКАЛІЗАЦІЇ ==========")
        print(f"Оцінений азимут прихованої Wi-Fi камери:
{azimuth:.2f}°")

        return azimuth
```

Модуль test_data_generator.py — модуль «Генерація тестових CSI-даних і журналу кутів повороту для перевірки алгоритму локалізації без використання реального апаратного обладнання».

```
import csv
import math
import time

from config import SystemConfig


class TestDataGenerator:
    """
    Модуль генерації тестових CSI-даних.

    Він дозволяє перевірити алгоритм локалізації без реального
    Raspberry Pi, Wi-Fi камери, nexmon_csi та крокового двигуна.
    """

    @staticmethod
    def generate_test_csi(
        config: SystemConfig,
        true_azimuth: float = 75.0
    ) -> None:
        """
```

```
        Генерує:
        - файл motor_angles.csv з кутами повороту пластини;
        - файл csi_capture.csv з імітованим CSI-провалом.
        """
        start_time = time.time()

        with open(
            config.motor_log_file,
            "w",
            newline="",
            encoding="utf-8"
        ) as motor_csv:
            writer = csv.writer(motor_csv)
            writer.writerow(["timestamp", "angle"])

            angle = config.start_angle
            index = 0

            while angle <= config.end_angle:
                timestamp = start_time + index * 0.05
                writer.writerow([timestamp, angle])

                angle += config.angle_step
                index += 1

        with open(
            config.csi_csv_file,
            "w",
            newline="",
            encoding="utf-8"
        ) as csi_csv:
            writer = csv.writer(csi_csv)
            writer.writerow(["timestamp", "amplitude"])

            angle = config.start_angle
            index = 0

            while angle <= config.end_angle:
                timestamp = start_time + index * 0.05

                # Базовий рівень сигналу
                amplitude = 1.0

                # Імітація дифракційного провалу біля кута
true_azimuth
                attenuation = math.exp(
                    -((angle - true_azimuth) ** 2) / (2 * 8.0 ** 2)
                )

                amplitude -= 0.45 * attenuation

                # Додавання невеликої шумової складової
                amplitude += 0.03 * math.sin(angle / 5.0)
```

```
                writer.writerow([timestamp, amplitude])

                angle += config.angle_step
                index += 1

        print("[INFO] Згенеровано тестові дані")
        print(f"[INFO] Файл CSI: {config.csi_csv_file}")
        print(f"[INFO] Файл кутів: {config.motor_log_file}")
        print(f"[INFO] Заданий азимут: {true_azimuth:.2f}°")
```

Модуль camera_system.py — модуль «Інтеграція етапів виявлення підозрілого Wi-Fi пристрою, керування дифракційним елементом, аналізу CSI та формування результату локалізації».

```
from config import SystemConfig
from traffic_analyzer import WiFiTrafficAnalyzer
from motor_controller import StepperMotorController
from csi_processor import CsiProcessor


class HiddenWiFiCameraLocalizationSystem:
    """
    Головний модуль системи.

    Він об'єднує:
    - аналіз Wi-Fi трафіку;
    - вибір підозрілого пристрою;
    - керування металевою пластиною;
    - аналіз CSI;
    - оцінювання азимуту прихованої камери.
    """

    def __init__(self, config: SystemConfig):
        self.config = config
        self.traffic_analyzer = WiFiTrafficAnalyzer(config)
        self.csi_processor = CsiProcessor(config)

    def detection_stage(self):
        """
        Етап виявлення підозрілих Wi-Fi пристроїв.
        """
        self.traffic_analyzer.capture_traffic()

        suspicious_devices =
self.traffic_analyzer.find_suspicious_devices()

        self.traffic_analyzer.print_report(suspicious_devices)

        return suspicious_devices
```

```
    def localization_stage(self, simulation: bool = False) -> float:
        """
        Етап локалізації прихованої Wi-Fi камери.
        """
        motor = StepperMotorController(
            config=self.config,
            simulation=simulation
        )

        try:
            motor.rotate_to_angle_range()
        finally:
            motor.cleanup()

        azimuth = self.csi_processor.estimate_azimuth()

        return azimuth

    def run_full_cycle(self, simulation: bool = False) -> None:
        """
        Повний цикл роботи системи:
        1. Виявлення підозрілого Wi-Fi пристрою.
        2. Визначення MAC-адреси та каналу.
        3. Поворот металевої пластини.
        4. Аналіз CSI.
        5. Виведення напрямку на камеру.
        """
        print("================================================")
        print(" КІБЕРФІЗИЧНА СИСТЕМА ПОШУКУ WI-FI КАМЕР")
        print("================================================")

        suspicious_devices = self.detection_stage()

        if not suspicious_devices:
            print("\n[RESULT] Пристроїв з ознаками відеопотоку не
виявлено.")
            return

        target = suspicious_devices[0]

        print("\n[INFO] Для локалізації обрано найбільш підозрілий
пристрій:")
        print(f"MAC-адреса: {target.mac}")
        print(f"Wi-Fi канал: {target.channel}")
        print(f"Кількість пакетів: {target.packet_count}")
        print(f"Середній розмір пакета:
{target.average_payload_size:.2f} байт")

        azimuth = self.localization_stage(simulation=simulation)

        print("\n[RESULT] Підсумковий результат:")
        print(f"Ймовірна прихована Wi-Fi камера: {target.mac}")
```

```
        print(f"Орієнтовний напрямок пошуку: {azimuth:.2f}°")
        print(
            "Рекомендація: оглянути предмети у вказаному секторі, "
            "починаючи з найближчих до системи об'єктів."
        )
```

Модуль main.py — модуль «Організація запуску програмного забезпечення та вибору режиму роботи кіберфізичної системи через командний рядок».

```
import argparse

from config import SystemConfig
from camera_system import HiddenWiFiCameraLocalizationSystem
from test_data_generator import TestDataGenerator


def main() -> None:
    """
    Точка входу в програму.
    """

    parser = argparse.ArgumentParser(
        description=(
            "Кіберфізична система виявлення та локалізації "
            "прихованих Wi-Fi камер"
        )
    )

    parser.add_argument(
        "--mode",
        choices=["detect", "localize", "full", "test"],
        default="test",
        help="Режим роботи програми"
    )

    parser.add_argument(
        "--iface",
        default="wlan0mon",
        help="Wi-Fi інтерфейс у monitor mode"
    )

    parser.add_argument(
        "--csi",
        default="csi_capture.csv",
        help="CSV-файл з CSI-даними"
    )

    parser.add_argument(
        "--motor-log",
        default="motor_angles.csv",
        help="CSV-файл із кутами повороту металевої пластини"
```

```
)

parser.add_argument(
    "--simulation",
    action="store_true",
    help="Запуск без реального GPIO та двигуна"
)

parser.add_argument(
    "--true-azimuth",
    type=float,
    default=75.0,
    help="Істинний азимут для тестової генерації CSI"
)

args = parser.parse_args()

config = SystemConfig(
    monitor_interface=args.iface,
    csi_csv_file=args.csi,
    motor_log_file=args.motor_log
)

system = HiddenWiFiCameraLocalizationSystem(config)

if args.mode == "test":
    TestDataGenerator.generate_test_csi(
        config=config,
        true_azimuth=args.true_azimuth
    )

    estimated_azimuth = system.csi_processor.estimate_azimuth()

    print("\n[TEST] Перевірка алгоритму завершена")
    print(f"[TEST] Заданий азимут: {args.true_azimuth:.2f}°")
    print(f"[TEST] Оцінений азимут: {estimated_azimuth:.2f}°")
    print(
        f"[TEST] Абсолютна похибка: "
        f"{abs(args.true_azimuth - estimated_azimuth):.2f}°"
    )

elif args.mode == "detect":
    system.detection_stage()

elif args.mode == "localize":
    system.localization_stage(
        simulation=args.simulation
    )

elif args.mode == "full":
    system.run_full_cycle(
        simulation=args.simulation
    )
```

```
if __name__ == "__main__":
    main()
```

ДОДАТОК Б
(обов'язковий)

Публікація

УДК 004.056:004.7:621.396

КІБЕРФІЗИЧНА СИСТЕМА ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ПРИХОВАНИХ WI-FI КАМЕР У ПРИМІЩЕННЯХ НА ОСНОВІ АНАЛІЗУ ПАРАМЕТРІВ РАДІОКАНАЛУ

Ткаченко Д.Д., студент гр. КІ2м-24
Науковий керівник: д. т. н., професор Яцків В.В.
Хмельницький національний університет

Актуальність. Поширення бездротових камер спостереження та мініатюрних IoT-пристроїв посилює ризики прихованого відеоспостереження у квартирах, готельних номерах, офісах і короткостроково орендованих приміщеннях. Традиційні способи пошуку камер, що спираються на виявлення відблисків об'єктива, теплового випромінювання або ручне обстеження кімнати, часто потребують спеціального обладнання, значних зусиль користувача і вільного простору.

Метою роботи є узагальнення принципів побудови кіберфізичної системи виявлення та локалізації прихованих Wi-Fi камер у приміщенні на основі аналізу параметрів радіоканалу та оцінка можливостей підходу DIFFLOC, який використовує явище електромагнітної дифракції.

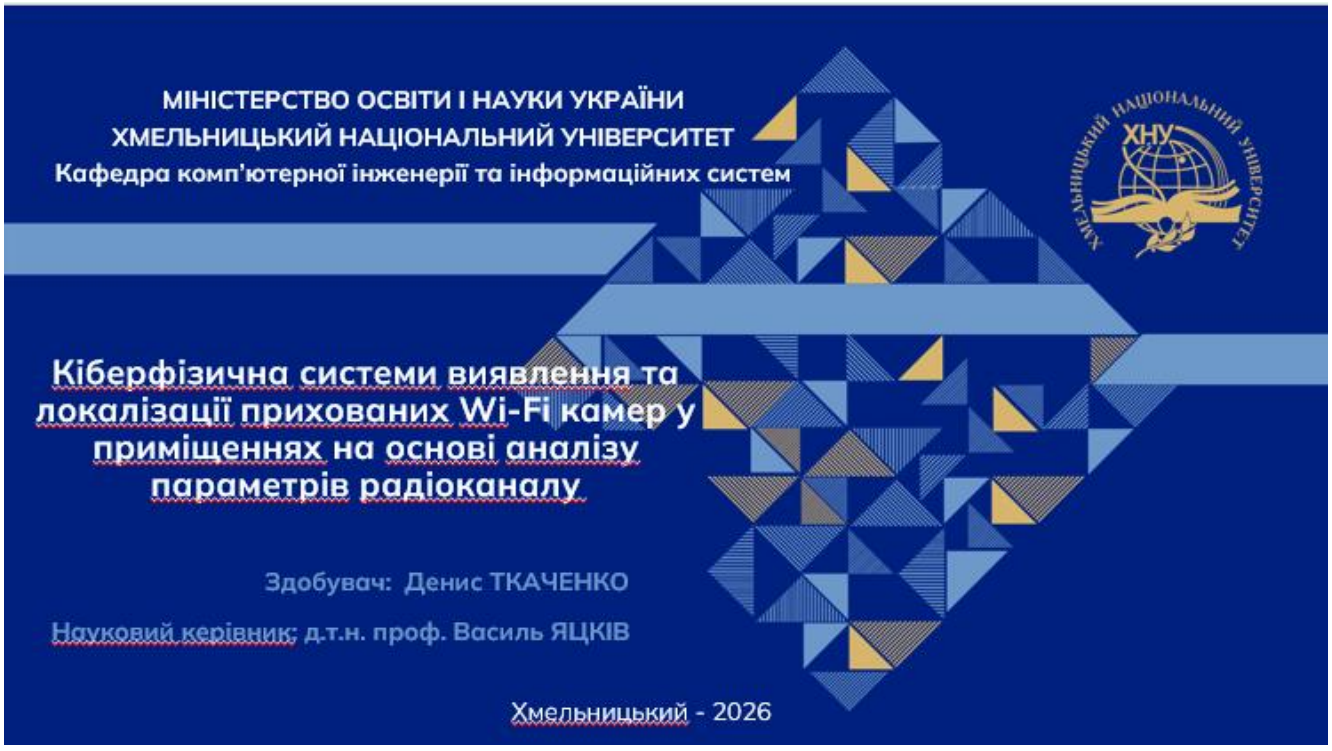
Аналіз рішень. Сучасні методи локалізації прихованих камер застосовують аналіз трафіку, RSSI та CSI, однак більшість із них вимагає попереднього навчання моделі, задання параметрів середовища або переміщення користувача вздовж периметра кімнати. У DIFFLOC біля пасивного приймача Wi-Fi обертається невелика металева пластина, яка створює кероване дифракційне затінення та формує характерне ослаблення сигналу в CSI.

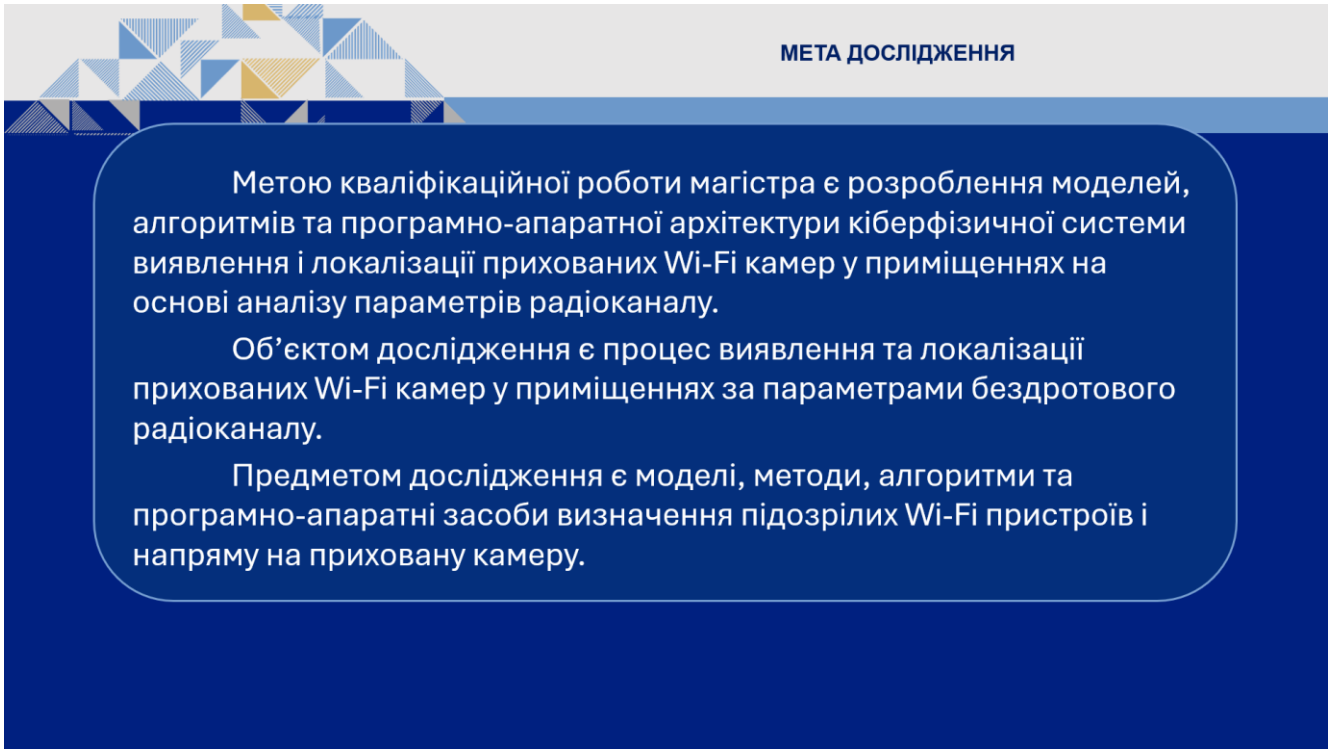
Результати. Запропонована система поєднує виявлення підозрілих пристроїв за параметрами вихідного трафіку та локалізацію камери за азимутом. На етапі виявлення аналізуються MAC-адреси, канал 802.11 і зміни пропускної здатності після виходу користувача з кімнати. На етапі локалізації Raspberry Pi у режимі пасивного моніторингу збирає CSI, а кроковий двигун обертає металеву пластину навколо приймача.

Висновки. Підхід DIFFLOC підтверджує можливість побудови недорогої кіберфізичної системи локалізації прихованих Wi-Fi камер без попереднього навчання моделі та без дорогих сенсорів. Подальші дослідження доцільно спрямувати на створення портативних засобів захисту приватності.

ДОДАТОК В
(обов’язковий)

Презентація





ЗАДАЧІ ДОСЛІДЖЕННЯ

Поставлена мета досягається розв’язанням таких основних завдань

- проаналізувати стан проблеми прихованого відеоспостереження та обмеження традиційних засобів пошуку;
- порівняти оптичні, теплові, RSSI-, CSI- та трафікові підходи до виявлення прихованих камер;
- обґрунтувати використання CSI/RSSI та керованої дифракції електромагнітного сигналу;
- розробити структурну й математичну модель кіберфізичної системи;
- розробити алгоритми попереднього виявлення та азимутальної локалізації;
- реалізувати програмно-апаратний прототип і провести експериментальну перевірку.

НАУКОВА НОВИЗНА ТА ПРАКТИЧНА ЦІННІСТЬ ОТРИМАНИХ РЕЗУЛЬТАТІВ

- набув подальшого розвитку метод виявлення та локалізації прихованих Wi-Fi камер, який поєднує пасивний моніторинг Wi-Fi трафіку з аналізом змін характеристик радіосигналу;

- набув подальшого розвитку підхід до побудови кіберфізичних систем захисту приватності, що поєднує апаратний збір радіоданих, аналіз трафіку та алгоритми локалізації прихованих пристроїв.

НАУКОВА НОВИЗНА ТА ПРАКТИЧНА ЦІННІСТЬ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Практична цінність роботи полягає у можливості використання запропонованого методу для виявлення та локалізації прихованих Wi-Fi камер у приміщеннях без необхідності фізичного доступу до підозрілих пристроїв. Розроблена кіберфізична система може бути застосована для підвищення рівня приватності та інформаційної безпеки в офісах, готелях, навчальних аудиторіях, житлових приміщеннях та інших просторах, де існує ризик несанкціонованого відеоспостереження.

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ

Актуальність роботи полягає у зростанні ризиків несанкціонованого відеоспостереження в приміщеннях через поширення компактних прихованих Wi-Fi камер та інших бездротових пристроїв.

Тому розроблення кіберфізичної системи для їх виявлення і локалізації на основі аналізу параметрів радіоканалу є важливим для підвищення рівня приватності, інформаційної безпеки та захисту персональних даних.

АНАЛІЗ ВІДОМИХ МЕТОДІВ

Аналіз відомих методів показав, що для виявлення прихованих камер найчастіше використовують візуальний огляд, пошук відбиття від об'єктива, аналіз мережевого трафіку, радіочастотне сканування та спеціалізовані детектори випромінювання.

Встановлено, що традиційні підходи мають певні обмеження, оскільки не завжди дозволяють точно визначити місце розташування пристрою, особливо якщо камера замаскована або працює у звичайній Wi-Fi мережі.

Тому перспективним є використання комбінованого підходу, який поєднує аналіз бездротового трафіку, параметрів радіоканалу та алгоритмів локалізації для підвищення точності виявлення прихованих пристроїв.

Принцип роботи кіберфізичної системи

1. Виявлення підозрілих пристроїв
- сканування мережі
- MAC-адреси
- канал 802.11
- аналіз вихідного трафіку

→

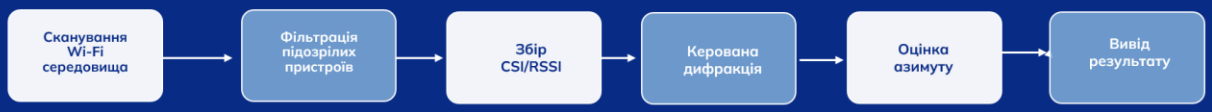
2. Локалізація (DIFFLOC)
- пасивний збір CSI
- обертання металевої пластини
- дифракційне затінення
- оцінка азимуту

→

3. Пошук камери за напрямком
- визначення азимуту
- перевірка об'єктів на лінії огляду
- підтвердження місця розміщення

Перевага підходу: відсутність попереднього навчання моделі та використання недорогих компонентів.

МОДЕЛЬ ПРОЦЕСУ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ПРИХОВАНИХ WI-FI КАМЕР



Структурна модель поєднує фізичне середовище, приховану Wi-Fi камеру, пасивний приймач, керований дифракційний модуль та програмну обробку даних.

МЕТОД ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ПРИХОВАНИХ WI-FI КАМЕР

- 1. Пасивне сканування бездротового середовища та групування пакетів за MAC-адресами.
- 2. Виявлення пристроїв, які стабільно передають значний обсяг даних і схожі на джерело відеопотоку.
- 3. Збір CSI/RSSI на відповідному каналі та синхронізація вимірювань з часовими мітками.
- 4. Обертання металевої пластини для створення контрольованого дифракційного впливу на радіоканал.

МЕТОД ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ПРИХОВАНИХ WI-FI КАМЕР

- 5. Фільтрація шуму та згладжування часових рядів амплітуди CSI.
- 6. Пошук локальних мінімумів, які відповідають проходженню пластини через зону Френеля.
- 7. Зіставлення мінімуму CSI з кутом повороту крокового двигуна.
- 8. Формування азимутального напряму на потенційну приховану Wi-Fi камеру.

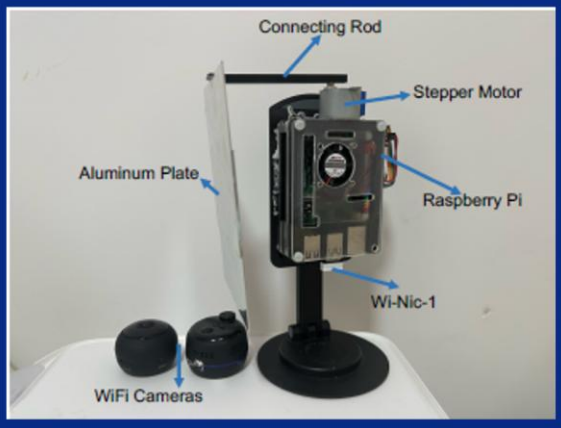
МЕТОД ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ПРИХОВАНИХ WI-FI КАМЕР

Схема методу

РЕАЛІЗАЦІЯ МЕТОДУ

- центральний вузол системи – Raspberry Pi з Linux, Python, monitor mode та засобами обробки Wi-Fi даних;
- апаратні компоненти: Wi-Fi адаптер, кроковий двигун, драйвер ULN2003, металева пластина та опорний механізм;
- програмні модулі: сканування каналів, перехоплення пакетів, фільтрація трафіку, збір CSI, керування двигуном, синхронізація та розрахунок азимуту;
- результатом роботи є список підозрілих пристроїв і напрямок пошуку прихованої камери.

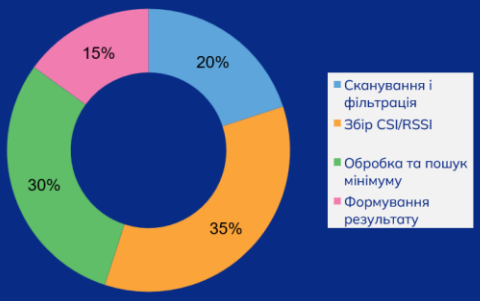
РЕАЛІЗАЦІЯ МЕТОДУ



Приклад прототипу системи з дифракційним елементом

РЕАЛІЗАЦІЯ МЕТОДУ

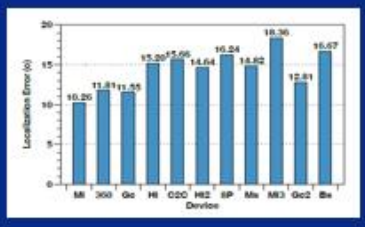
Розподіл обчислювального часу для методу



Найбільшу частку займає збір і обробка канальних параметрів, оскільки саме ці дані формують основу локалізації.

ЕКСПЕРИМЕНТИ

Результати роботи методу при різних параметрах системи




```
516 packets captured
555 packets received by filter
0 packets dropped by kernel
4 packets dropped by interface
Time stamps saved to {timestamp_filename}
112
1731310220.218225
1731310220.679656
The dangerous device is located at angle1: 151.875
Running command: sudo ip link set mon0 down
```

Експериментальні графіки та консольні результати підтверджують працездатність програмної моделі: система виконує збір пакетів, аналізує параметри радіоканалу та видає оцінку напрямку на прихований пристрій.

ВИСНОВКИ

- проаналізовано сучасні методи виявлення та локалізації прихованих Wi-Fi камер і визначено їх основні обмеження;
- обґрунтовано використання CSI/RSSI-параметрів і керованої дифракції для оцінювання напряму на джерело сигналу;
- розроблено архітектуру кіберфізичної системи, алгоритми виявлення підозрілих пристроїв і азимутальної локалізації;
- реалізовано програмно-апаратну модель системи та проведено експериментальну перевірку;
- запропонована система може використовуватися як основа переносного засобу підвищення приватності у приміщеннях.

ПУБЛІКАЦІЇ

- Яцків В., Ткаченко Д. Кіберфізична системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу ПерСик 2026, Харків, Україна, 23 квіт. 2026.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Денис ТКАЧЕНКО

Тема: Кіберфізична системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень – ; кількість сторінок записки 78

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано систему профілювання вразливостей при керуванні розумним будинком

2. Висновок про відповідність роботи дипломному завданню Кваліфікаційна робота магістра відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено огляд проаналізовано проблему прихованих Wi-Fi камер, сучасні методи їх виявлення та обґрунтовано актуальність використання параметрів радіоканалу. Досліджено відомі рішення та засоби в цій сфері. У другому розділі розроблено модель кіберфізичної системи та обґрунтовано використання CSI/RSSI-параметрів і керованої дифракції для локалізації камери. У третьому розділі запропоновано алгоритми виявлення підозрілих Wi-Fi пристроїв, азимутальної локалізації та архітектуру програмно-апаратного комплексу. У четвертому розділі виконано програмну реалізацію системи, проведено експериментальні дослідження та оцінено ефективність запропонованого рішення.

4. Позитивні сторони роботи: Запропонований метод відповідає поставленій задачі, виражена наукова новизна та практична цінність, розроблений метод добре масштабується та є гнучким.

5. Негативні сторони роботи: Запропонована кіберфізична система потребує додаткової перевірки в більшій кількості реальних приміщень із різними умовами

поширення Wi-Fi сигналу для точнішого оцінювання її ефективності та стійкості.

6. Оцінка графічного оформлення та пояснювальної записки роботи: –

7. Відгук про роботу в цілому: В загальному робота виконана на належному рівні.

8. Інші зауваження: –

9. Оцінка кваліфікаційної роботи магістра:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки «добре» 80.00 (В)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Мартинюк Валерій Володимирович, пр.вр. каф. АКІТ та Р, д.т.н., проф.

"1" 05 2026р.

Зав. кафедри КІС
д-р. філософії Ользі ПАВЛОВІЙ

Денис ТКАЧЕНКО
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-24-2

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

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

1 травня 2026 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Кіберфізична системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу
Автор Денис ТКАЧЕНКО
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: д.т.н., професор Василь ЯЦКІВ

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

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

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 8,6% та системою Anti-Plagiarism складає 1%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

19.05.2026

Завідувач кафедри — Підпис — Ольга ПАВЛОВА (Ім'я, ПРІЗВИЩЕ)

Гарант освітньої програми — Підпис — Олег САВЕНКО (Ім'я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи — Підпис — Василь ЯЦКІВ (Ім'я, ПРІЗВИЩЕ)

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: Денис ТКАЧЕНКО

Співавтор:

Назва: Кіберфізична системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу

Експерт: Василь ЯЦКІВ

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:8.6%

Коефіцієнт подібності 2:2.94%

Мікропробіли: 3

Заміна букв: 7

Інтервали: 0

Білі знаки: 6

Дата створення звіту: 2026-05-19 14:52:29.0

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:

2026-05-19

Дата

Доцент Андрій Нічепорук

експерт

Tue May 19 13:11:08 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

	Документ		Сумарний збіг по Базі Даних	
ID: 271691 Назва: МКР Кіберфізична системи виявлення та локалізації прихованих Wi-Fi камер у приміщеннях на основі аналізу параметрів радіоканалу Додано в БД: 2026-05-19 Автора: Денис ТКАЧЕНКО Керівники: Василь ЯЦКІВ Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	123938	1083	3749 (3%)	45 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми