**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»**

**Навчально-науковий інститут телекомунікаційних систем**

**Кафедра інформаційних технологій в телекомунікаціях**

**«До захисту допущено»**
В.О. завідувача кафедрою
_____ Валерій ПРАВИЛО
«___»_____2026 р.

**Дипломна робота**
на здобуття ступеня бакалавра
за освітньо-професійною програмою «Інформаційно-комунікаційні технології»
спеціальності 172 Телекомунікації та радіотехніка

на тему: Метод безпечної передачі приватних даних на близькій відстані

Виконала: студентка IV курсу, групи ТІ-22
Іщенко Марія Олександрівна _____
(підпис)

Науковий керівник: старший викладач кафедри ІТТ НН ІТС
кандидат технічних наук Педан Станіслав Ігорович ____
(підпис)

Рецензент: доцент кафедри Інформаційної безпеки НН ФТІ
Прогонов Дмитро Олександрович _____
(підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студентка _____

Київ - 2026 року

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

**Навчально-науковий інститут телекомунікаційних систем**

**Кафедра інформаційних технологій в телекомунікаціях**

Рівень вищої освіти – перший (бакалаврський)
Освітньо-професійна програма «Інформаційно-комунікаційні технології»
спеціальності 172 Телекомунікації та радіотехніка

**ЗАТВЕРДЖУЮ**
В.О. завідувача кафедри
_____ Валерій ПРАВИЛО
«_____»_____2026 р.

**ЗАВДАННЯ**
**на дипломну роботу студентці**
Іщенко Марії Олександрівні

1. Тема роботи: «Метод безпечної передачі приватних даних на близькій відстані», науковий керівник роботи Педан Станіслав Ігорович, старший викладач кафедри ІТТ НН ІТС, кандидат технічних наук - затверджені наказом по університету від 26.05.2026 р. № 1912-с

.

2. Строк подання студенткою роботи 06 червня 2026 р.

3. Вихідні дані до роботи: науково-технічна література, матеріали мережі Інтернет, мобільні пристрої з підтримкою безпроводових технологій (Bluetooth, Wi-Fi), програмні засоби для аналізу параметрів сигналу, результати власних досліджень та експериментів.

4. Зміст пояснювальної записки дипломної роботи

- Аналіз безпроводових технологій передавання даних та їх застосування
- Проблеми безпеки під час передавання приватних даних та випадкове передавання інформації
- Огляд існуючих методів забезпечення безпеки передавання даних
- Метод безпечної передачі приватних даних на близькій відстані
- Оцінка ефективності запропонованого методу

- Загальні висновки

5. Перелік графічного (ілюстративного) матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо)

- Зміст дипломної роботи;
- Мета роботи;
- 1.1 Безпроводові технології передавання даних
- Проблема випадкової передачі приватних даних
- Огляд існуючих методів захисту
- Схема взаємодії пристроїв (Trusted Zone)
- Метод безпечного передавання даних
- Алгоритм роботи методу
- Дослідження залежності RSSI від відстані між пристроями
- Діаграми результатів досліджень
- Висновки.

6. Дата видачі завдання : «20» січня 2026 р.

Календарний план

| № з/п | Назва етапів виконання дипломної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Аналіз безпроводових технологій передачі даних | 15.04-21.04 | виконано |
| 2 | Дослідження проблеми безпеки та випадкової передачі приватних даних | 22.04-28.04 | виконано |
| 3 | Аналіз існуючих методів забезпечення безпеки передачі даних | 29.04-05.05 | виконано |
| 4 | Розробка методу безпечної передачі приватних даних на близькій відстані | 06.05-12.05 | виконано |
| 5 | Оцінка ефективності запропонованого методу та проведення досліджень | 13.05-19.05 | виконано |

Студентка _____ Марія ІЩЕНКО

Науковий керівник роботи _____ Станіслав ПЕДАН

# РЕФЕРАТ

Дипломна робота «Метод безпечної передачі приватних даних на близькій відстані» містить 75 сторінок тексту, 10 рисунків та 12 таблиць, а також використовує 15 літературних джерел посилання.

Дипломна робота присвячена задачі безпечного локального обміну приватними файлами між мобільними та IoT-пристроями. Пояснювальна записка містить теоретичний аналіз, опис запропонованого методу, таблиці, рисунки та перелік використаних джерел.

У роботі розглянуто типові випадки, коли приватний файл може потрапити не тому отримувачу: через однакові або схожі назви пристроїв, перевантажений список доступних з’єднань чи поспішне підтвердження дії користувачем. Для зменшення такого ризику запропоновано комбінований метод, у якому перед передаванням перевіряються клас приватності файлу, близькість отримувача за RSSI, можливе NFC/UWB-підтвердження та відповідність пристрою умовам Trusted Zone.

Об’єктом дослідження є процес безпроводового передавання даних між мобільними та IoT-пристроями в умовах локальної взаємодії користувачів.

Предметом дослідження є підходи до контролю безпечності передавання приватних даних із використанням характеристик безпроводового сигналу, довіреності пристрою та фізичної близькості отримувача.

Мета роботи полягає у підвищенні безпеки локального передавання приватних даних завдяки попередній перевірці отримувача, рівня приватності файлу й допустимої відстані між пристроями.

Наукова новизна дослідження:

Запропоновано контекстний підхід до контролю передавання, за якого рішення про дозвіл, додаткове підтвердження або блокування залежить від класу приватності файлу, параметрів близькості та статусу довіри до отримувача.

Розроблено модель Trusted Zone, яка об’єднує RSSI-оцінювання, NFC/UWB-підтвердження та перевірку довіреності отримувача в єдину процедуру прийняття рішення.

Ключові слова: БЕЗПЕКА, БЕЗПРОВОДОВІ ТЕХНОЛОГІЇ, ПЕРЕДАВАННЯ ДАНИХ, RSSI, ПРИВАТНІСТЬ, BLUETOOTH, WI-FI, ЗОНА ДОВІРИ.

## ABSTRACT

The thesis “Method for Secure Transmission of Private Data over Short Distances” consists of 75 pages, 10 figures, and 12 tables, and includes 15 references.

The bachelor thesis addresses the practical problem of secure local exchange of private files between mobile and IoT devices. The explanatory note includes theoretical analysis, a description of the proposed method, figures, tables and references.

The paper examines situations where a private file can be sent to an unintended receiver because device names are similar, many wireless devices are visible at the same time, or the user confirms the action too quickly. To reduce this risk, a combined method is proposed. Before transmission, it checks the file privacy class, receiver proximity based on RSSI, possible NFC/UWB confirmation and compliance with the Trusted Zone conditions.

The object of the study is wireless data transmission between mobile and IoT devices during local user interaction.

The subject of the study is methods for controlling the safety of private data transmission using wireless signal parameters, receiver trust status and physical proximity.

The purpose of the study is to improve the security of local private data transmission by checking the receiver, the file privacy class and the allowed distance between devices before the transfer starts.

Scientific novelty of the work:

A context-based transmission control approach is proposed, where the decision to allow, additionally confirm or block a transfer depends on the file privacy class, proximity parameters and receiver trust status.

A Trusted Zone model is developed by combining RSSI evaluation, NFC/UWB confirmation and receiver trust verification into a single decision procedure.

Keywords: SECURITY, WIRELESS TECHNOLOGIES, DATA TRANSMISSION, RSSI, PRIVACY, BLUETOOTH, WI-FI, TRUSTED ZONE.

# ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ..... 8
ВСТУП ..... 9
1. АНАЛІЗ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ ТА ПРОБЛЕМ БЕЗПЕКИ ..... 11
1.1 Безпроводові технології передавання даних ..... 11
1.2 Проблема випадкової передачі приватних даних ..... 13
1.3 Аналіз існуючих методів забезпечення безпеки ..... 15
1.4 Висновки за розділом 1 ..... 18
2. ОСНОВНІ ЗАГРОЗИ БЕЗПЕКИ ПРИ ПЕРЕДАЧІ ДАНИХ ..... 20
2.1 Детальний аналіз проблеми випадкової передачі приватних даних ..... 20
2.2 Методи виявлення випадкового передавання даних ..... 22
2.3 Методи запобігання випадковій передачі приватних даних ..... 24
2.4 Висновки за розділом 2 ..... 27
3. ОГЛЯД МЕТОДІВ ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ ..... 28
3.1 Методи шифрування та автентифікації ..... 28
3.2 Використання безпроводових технологій ..... 31
3.3 Обмеження існуючих рішень ..... 36
3.4 Висновки за розділом 3 ..... 39
4. МЕТОД БЕЗПЕЧНОЇ ПЕРЕДАЧІ ПРИВАТНИХ ДАНИХ НА БЛИЗЬКІЙ ВІДСТАНІ ..... 42
4.1 Загальна концепція методу ..... 48
4.2 Використання RSSI для визначення відстані ..... 53
4.3 Формування зони довіри (Trusted Zone) ..... 58
4.4 Алгоритм роботи методу ..... 64
4.5 Оцінка ефективності ..... 64
4.6 Висновки за розділом 4 ..... 72
ЗАГАЛЬНІ ВИСНОВКИ ..... 74
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ..... 76

# ПЕРЕЛІК СКОРОЧЕНЬ

BLE (Bluetooth Low Energy) - безпроводова технологія з низьким енергоспоживанням для передавання даних на короткі відстані

NFC (Near Field Communication) - технологія безконтактного зв’язку на дуже малих відстанях

Wi-Fi (Wireless Fidelity) - технологія безпроводового передавання даних у локальних мережах

RSSI (Received Signal Strength Indicator) - індикатор сили прийнятого сигналу, використовується для оцінки відстані між пристроями

MITM (Man-in-the-Middle) - атака «людина посередині», при якій зловмисник перехоплює та змінює передані дані

AES (Advanced Encryption Standard) - стандарт симетричного шифрування даних

RSA (Rivest-Shamir-Adleman) - криптографічний алгоритм асиметричного шифрування

ECC (Elliptic Curve Cryptography) - криптографія на основі еліптичних кривих

TLS (Transport Layer Security) - протокол захисту даних на транспортному рівні

HTTPS (HyperText Transfer Protocol Secure) - захищений протокол передачі гіпертексту

MAC (Media Access Control) - механізм керування доступом до середовища передавання даних

PHY (Physical Layer) - фізичний рівень моделі OSI, на якому відбувається передача сигналу

PIN (Personal Identification Number) - персональний ідентифікаційний код для автентифікації

OTP (One-Time Password) - одноразовий пароль для підтвердження дій користувача

API (Application Programming Interface) - програмний інтерфейс взаємодії між системами

OS (Operating System) - операційна система пристрою

QoS (Quality of Service) - параметр якості передавання даних у мережі

# ВСТУП

Для досягнення мети роботи розглянуто кілька взаємопов’язаних задач. Спочатку проаналізовано безпроводові технології, які найчастіше застосовуються для локального обміну даними між пристроями, зокрема Bluetooth, Wi-Fi Direct та NFC. Такий огляд потрібний для того, щоб порівняти їхні можливості, обмеження та роль у сценаріях передавання приватної інформації [2, 4-6].

Окремо досліджено проблему випадкової передачі приватної інформації. Вона виникає не лише через технічні особливості безпроводового середовища, а й через спосіб взаємодії користувача з інтерфейсом: вибір зі списку пристроїв, схожі назви отримувачів, автоматичні підказки системи та поспішне підтвердження операції.

Важливим напрямом роботи є проведення аналізу існуючих методів забезпечення безпеки передавання даних, включаючи криптографічні механізми, методи автентифікації та контролю доступу. У межах цього етапу здійснюється оцінка їх ефективності з погляду захисту інформації від несанкціонованого доступу, а також виявлення обмежень і недоліків, пов’язаних із відсутністю механізмів контролю правильності вибору отримувача та врахування фізичного контексту взаємодії між пристроями [8, 15].

На основі отриманих результатів передбачається розробка методу безпечного передавання даних, який враховує просторову близькість пристроїв та дозволяє обмежити передачу приватної інформації лише у межах визначеної довіреної зони. Запропонований підхід базується на аналізі параметрів безпроводового сигналу, зокрема рівня RSSI, що дозволяє оцінити відстань між пристроями та підвищити точність визначення цільового отримувача.

Завершальним етапом роботи є оцінка ефективності запропонованого методу шляхом аналізу його здатності зменшувати ризик випадкового передавання даних, а також визначення практичної доцільності його використання у сучасних мобільних системах. Це дозволяє підтвердити

актуальність розробленого підходу та обґрунтувати можливість його подальшого застосування у реальних умовах.

# 1. АНАЛІЗ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ ТА ПРОБЛЕМ БЕЗПЕКИ

## 1.1 Безпроводові технології передавання даних

Безпроводові технології передавання даних нині займають важливе місце у сфері інформаційно-комунікаційних систем. Їх активний розвиток безпосередньо пов’язаний із поширенням мобільних пристроїв, а також зі зростанням потреби у швидкому та зручному обміні інформацією між користувачами. Якщо раніше передавання даних переважно здійснювалась за допомогою кабельних з’єднань, то зараз більшість взаємодій між пристроями відбувається саме через безпроводові технології [9-11].

Основною особливістю таких технологій є те, що передавання інформації відбувається за допомогою електромагнітних хвиль, які поширюються у навколишньому середовищі. Це дозволяє пристроям взаємодіяти між собою без фізичного підключення, що підвищує мобільність користувачів і спрощує сам процес обміну даними. Наприклад, для передачі файлу між двома смартфонами більше не потрібно використовувати кабель або додаткове обладнання - достатньо лише активувати відповідну функцію.

Водночас така зручність має і зворотну сторону. Оскільки сигнал поширюється у відкритому просторі, він потенційно доступний для всіх пристроїв, які знаходяться у зоні його дії. Це означає, що передавання даних не обмежується лише двома конкретними пристроями, а фактично відбувається у середовищі, де можуть бути присутні й інші користувачі. Саме ця особливість і створює передумови для виникнення різного роду проблем, пов’язаних із безпекою.

На практиці у мобільних пристроях найчастіше використовуються такі безпроводові технології, як Bluetooth, Wi-Fi Direct та NFC. Кожна з них має свої особливості та використовується залежно від конкретних задач [2, 4, 5].

Bluetooth є однією з найпоширеніших технологій, яка використовується для передавання даних на невеликі відстані. Вона відома своєю простотою та універсальністю, оскільки підтримується практично всіма сучасними пристроями. За допомогою Bluetooth користувачі можуть передавати файли,

підключати навушники, колонки, клавіатури та інші пристрої. При цьому процес підключення зазвичай включає пошук доступних пристроїв, вибір потрібного зі списку та підтвердження з’єднання [2, 3].

Саме на цьому етапі і виникають певні складнощі. Користувач бачить список пристроїв, які знаходяться у зоні дії сигналу, і повинен самостійно обрати потрібний. Якщо у цьому списку є декілька пристроїв із подібними назвами, або якщо користувач не впевнений у правильності вибору, зростає ймовірність помилки.

Wi-Fi Direct є більш швидкою технологією, яка дозволяє передавати великі обсяги даних без використання маршрутизатора. Вона часто використовується для передачі відео, фотографій або великих файлів між пристроями. На відміну від Bluetooth, ця технологія має більший радіус дії, що означає, що у зоні доступності може знаходитися значно більше пристроїв. З одного боку, це зручно, оскільки дозволяє підключатися на більшій відстані, але з іншого - ускладнює процес вибору потрібного отримувача [5, 7, 14].

NFC, у свою чергу, працює на дуже малих відстанях і використовується, наприклад, для безконтактних платежів або швидкого з’єднання між пристроями. Завдяки тому, що для взаємодії необхідно фактично торкнутися пристроїв, ця технологія вважається більш безпечною. Проте навіть у цьому випадку не можна повністю виключити можливість помилки, особливо у ситуаціях, коли поруч знаходиться кілька пристроїв [4, 13].

Ще однією важливою особливістю безпроводових технологій є те, що якість сигналу змінюється залежно від відстані між пристроями та умов навколишнього середовища. Наприклад, стіни, меблі або інші об’єкти можуть послаблювати сигнал, а також впливати на його стабільність. У результаті реальна зона дії сигналу може відрізнятися від очікуваної [10-12].

Також потрібно враховувати, що у сучасних умовах кількість безпроводових пристроїв постійно зростає. У публічних місцях, таких як кафе, транспорт або офіси, одночасно може знаходитися велика кількість активних

пристроїв. Усі вони можуть бути відображені у списку доступних, що ускладнює процес вибору.

У підсумку, безпроводові технології передавання даних значно спрощують взаємодію між пристроями та підвищують зручність користування сучасними цифровими системами. Однак їхні особливості, зокрема відкритість середовища передачі, залежність сигналу від відстані та велика кількість пристроїв у зоні дії, створюють передумови для виникнення проблем, пов’язаних із безпекою передавання інформації. Саме ці фактори необхідно враховувати під час подальшого аналізі та розробці методів підвищення безпеки.

### 1.2 Проблема випадкової передачі приватних даних

Проблема випадкової передачі приватних даних у безпроводових мережах на сьогодні є актуальною, хоча часто недооцінюється користувачами. На відміну від типових загроз інформаційній безпеці, таких як злам системи або перехоплення даних, у цьому випадку мова йде про ситуації, коли інформація передається не тому отримувачу не через атаку, а через помилку. Саме тому така проблема є менш очевидною, але при цьому може мати серйозні наслідки.

У більшості випадків передавання даних між пристроями здійснюється за допомогою інтерфейсу, який відображає список доступних пристроїв. Користувач обирає потрібний пристрій і ініціює передачу. З першого погляду цей процес виглядає досить простим, однак у реальних умовах він може бути значно складнішим. Особливо це стосується ситуацій, коли навколо знаходиться велика кількість інших пристроїв.

У публічних місцях, таких як кафе, транспорт або навчальні заклади, одночасно може працювати багато смартфонів, ноутбуків та інших пристроїв із активованими безпроводовими модулями. У результаті список доступних пристроїв може містити десятки позицій. Користувач змушений швидко зорієнтуватися серед цього списку та обрати потрібний варіант, що не завжди є простою задачею.

Основною проблемою у цьому випадку є те, що вибір пристрою зазвичай здійснюється на основі його назви. При цьому назва не завжди є унікальною.

Наприклад, багато користувачів залишають стандартні назви пристроїв, які містять лише модель телефону або загальне ім’я. У таких умовах може виникнути ситуація, коли кілька пристроїв мають однакову або дуже схожу назву. Це ускладнює процес ідентифікації та підвищує ймовірність помилки.

Крім того, інтерфейс більшості систем не надає додаткової інформації, яка могла б допомогти користувачу зробити правильний вибір. Наприклад, зазвичай не відображається відстань до пристрою або рівень сигналу, хоча ці параметри могли б бути корисними. У результаті користувач змушений приймати рішення, маючи обмежену кількість даних [10-12].

Ще одним фактором, який впливає на виникнення проблеми, є динамічність безпроводового середовища. Пристрої можуть з’являтися та зникати зі списку доступних у залежності від того, як переміщуються користувачі або змінюються умови сигналу. Це може призводити до плутанини, особливо якщо користувач не одразу виконує передачу, а повертається до вибору через деякий час.

Також потрібно враховувати автоматичні механізми, які використовуються у деяких технологіях. Наприклад, система може пропонувати підключення до пристрою, з яким раніше вже встановлювався зв’язок, або до найближчого пристрою. З одного боку, це підвищує зручність, але з іншого - може призводити до ситуацій, коли користувач не повністю контролює процес вибору.

Окремо слід виділити роль людського фактора. У більшості випадків користувачі не приділяють достатньої уваги перевірці отримувача, особливо якщо передавання даних здається простою та звичною операцією. Часто рішення приймається швидко, без детального аналізу, що збільшує ризик помилки. Це особливо актуально у ситуаціях, коли користувач поспішає або виконує кілька дій одночасно.

Наслідки випадкового передавання даних можуть бути суттєвими. Якщо передається звичайний файл без важливої інформації, помилка може не мати значних наслідків. Однак у випадку передачі конфіденційних даних ситуація

змінюється. До таких даних можуть належати особисті фотографії, документи, дані облікових записів або фінансова інформація. Потрапляння таких даних до сторонніх осіб може призвести до порушення конфіденційності, а в окремих випадках - до фінансових або репутаційних втрат [8, 15].

У підсумку, проблема випадкової передачі приватних даних є реальною і виникає у повсякденному використанні безпроводових технологій. Вона пов’язана не лише з технічними особливостями системи, але й з поведінкою користувача. Саме поєднання цих факторів робить її складною для вирішення і потребує більш глибокого підходу до забезпечення безпеки передавання інформації.

### 1.3 Аналіз існуючих методів забезпечення безпеки

У сучасних безпроводових мережах питання безпеки передавання даних вирішується за допомогою комплексу методів, які спрямовані на захист інформації від несанкціонованого доступу, перехоплення або модифікації. Враховуючи відкритий характер середовища передачі, ці методи є необхідними для забезпечення базового рівня захисту, оскільки будь-який сигнал, що передається у повітрі, потенційно може бути прийнятий стороннім пристроєм. Саме тому у більшості сучасних технологій безпроводового зв’язку реалізовано механізми, які дозволяють знизити ризики, пов’язані із такими загрозами [8, 15].

Одним із основних підходів до забезпечення безпеки є шифрування даних. Його використання передбачає перетворення інформації у вигляд, який є недоступним для розуміння без відповідного ключа. Таким чином, навіть якщо дані будуть перехоплені під час передавання, сторонній користувач не зможе їх використати. У сучасних безпроводових технологіях застосовуються досить надійні алгоритми шифрування, які забезпечують високий рівень захисту. Наприклад, у Bluetooth та Wi-Fi використовуються стандартизовані криптографічні механізми, що дозволяють захистити інформацію під час передавання між пристроями [8, 15].

Разом із шифруванням широко використовується автентифікація. Її основна задача полягає у підтвердженні того, що пристрій, з яким

встановлюється з’єднання, є дійсно тим, за кого себе видає. У практичному використанні це може виглядати як введення PIN-коду, підтвердження на екрані або погодження певних параметрів з’єднання. Автентифікація дозволяє уникнути ситуацій, коли користувач випадково підключається до стороннього або підробленого пристрою, що є важливим елементом захисту [8, 15].

Ще одним поширеним підходом є контроль доступу. Він передбачає обмеження можливості взаємодії між пристроями на основі певних правил. Наприклад, пристрій може дозволяти підключення лише до тих об’єктів, з якими вже було встановлено з’єднання раніше, або до тих, що входять до списку довірених. Такий підхід дозволяє зменшити кількість потенційних підключень і, відповідно, знизити ризик небажаної взаємодії.

У деяких випадках використовуються також додаткові механізми, такі як підтвердження дій користувачем. Наприклад, перед встановленням з’єднання система може вимагати підтвердження у вигляді натискання кнопки або погодження запиту. Це дозволяє уникнути автоматичних підключень без відома користувача та підвищує контроль над процесом взаємодії.

Незважаючи на ефективність зазначених методів, вони мають низку обмежень, які стають особливо помітними при розгляді проблеми випадкового передавання даних. Основна їхня особливість полягає в тому, що вони спрямовані на захист інформації від зовнішніх загроз, але практично не враховують правильність вибору отримувача.

Іншими словами, система може гарантувати, що передані дані не будуть перехоплені сторонніми особами під час передавання, однак вона не гарантує, що ці дані будуть передані саме тому пристрою, якому вони призначені. Якщо користувач помилково обирає неправильний пристрій зі списку доступних, система не розглядає це як помилку і виконує передачу у звичайному режимі.

Це є принципово важливим моментом, оскільки з технічної точки зору така передача вважається коректною. Усі механізми безпеки працюють належним чином: дані зашифровані, пристрій автентифікований, доступ дозволений. Проте

з погляду користувача відбувається витік інформації, оскільки вона потрапляє до стороннього отримувача.

Ще одним суттєвим обмеженням є те, що існуючі методи не враховують фізичний контекст взаємодії між пристроями. Зокрема, система не аналізує відстань між пристроями або рівень сигналу, хоча ці параметри могли б бути використані для оцінки того, наскільки ймовірно, що обраний пристрій є цільовим. У результаті пристрій, який знаходиться на значній відстані, може бути обраний так само, як і той, що знаходиться безпосередньо поруч.

Крім того, більшість існуючих підходів не враховують тип або рівень важливості переданих даних. Передача звичайного файлу та передача конфіденційної інформації здійснюється за однаковими правилами, хоча рівень ризику у цих випадках суттєво відрізняється. Це означає, що система не адаптує свою поведінку залежно від контексту і не застосовує додаткові заходи безпеки у випадках, коли це дійсно необхідно.

Також важливо враховувати, що сучасні безпроводові технології часто орієнтовані на максимальну зручність використання. Це означає, що багато процесів автоматизовано або спрощено настільки, що користувач практично не контролює їх виконання. З одного боку, це підвищує комфорт, але з іншого - зменшує рівень усвідомлення того, що саме відбувається під час передавання даних.

У результаті можна зробити висновок, що існуючі методи забезпечення безпеки є ефективними у боротьбі з традиційними загрозами, такими як перехоплення або несанкціонований доступ. Однак вони не вирішують проблему випадкового передавання даних, оскільки не враховують ключовий фактор - правильність вибору отримувача.

У підсумку, виникає необхідність розробки нових підходів до забезпечення безпеки, які доповнюють існуючі методи та враховують додаткові параметри взаємодії між пристроями. Зокрема, перспективним є використання фізичних характеристик сигналу, таких як його рівень або зміни у часі, для оцінки відстані між пристроями та обмеження передавання даних у межах певної

зони. Це дозволить підвищити точність визначення отримувача і зменшити ризик випадкового передавання інформації.

### 1.4 Висновки за розділом 1

У цьому розділі було розглянуто особливості безпроводових технологій передавання даних та проаналізовано пов’язані з ними проблеми інформаційної безпеки. Встановлено, що такі технології, як Bluetooth, Wi-Fi Direct та NFC, широко застосовуються завдяки своїй зручності, доступності та універсальності, забезпечуючи швидкий обмін інформацією між пристроями без використання фізичних каналів зв’язку.

Разом із тим визначено, що відкритий характер безпроводового середовища створює передумови для виникнення загроз безпеці, оскільки сигнал може бути доступний усім пристроям у зоні дії. Це принципово відрізняє безпроводові технології від провідних та потребує додаткових механізмів захисту.

У ході аналізу встановлено, що однією з ключових проблем є випадкова передача приватних даних нецільовому отримувачу. Ця проблема виникає внаслідок поєднання технічних особливостей системи та людського фактора, зокрема через складність вибору пристрою зі списку доступних, особливо в умовах публічного середовища.

Також визначено, що користувачі орієнтуються переважно на назву пристрою, яка не завжди є унікальною, а інтерфейси більшості систем не надають достатньої інформації для точної ідентифікації отримувача. Це підвищує ймовірність помилкового вибору та, відповідно, витоку інформації.

Аналіз існуючих методів безпеки показав, що шифрування, автентифікація та контроль доступу ефективно захищають дані від перехоплення, однак не враховують правильність вибору отримувача. Крім того, ці підходи не використовують фізичні параметри взаємодії, такі як відстань між пристроями або рівень сигналу.

Отже, існуючі рішення не повністю вирішують проблему випадкового передавання даних, що обґрунтовує необхідність розробки нових підходів, які

враховують фізичний контекст взаємодії та дозволяють обмежити передавання інформації у межах безпечної зони.

# 2. ОСНОВНІ ЗАГРОЗИ БЕЗПЕКИ ПРИ ПЕРЕДАЧІ ДАНИХ

## 2.1 Детальний аналіз проблеми випадкової передачі приватних даних

У сучасних інформаційно-комунікаційних системах безпроводові технології передавання даних стали невід'ємною частиною повсякденного життя користувачів. Використання Bluetooth, Wi-Fi Direct та інших протоколів дозволяє швидко обмінюватися інформацією між мобільними пристроями без необхідності використання фізичних каналів зв'язку. Однак разом із підвищенням зручності використання таких технологій виникають нові загрози безпеці, однією з яких є проблема випадкової передачі приватних даних [9-11].

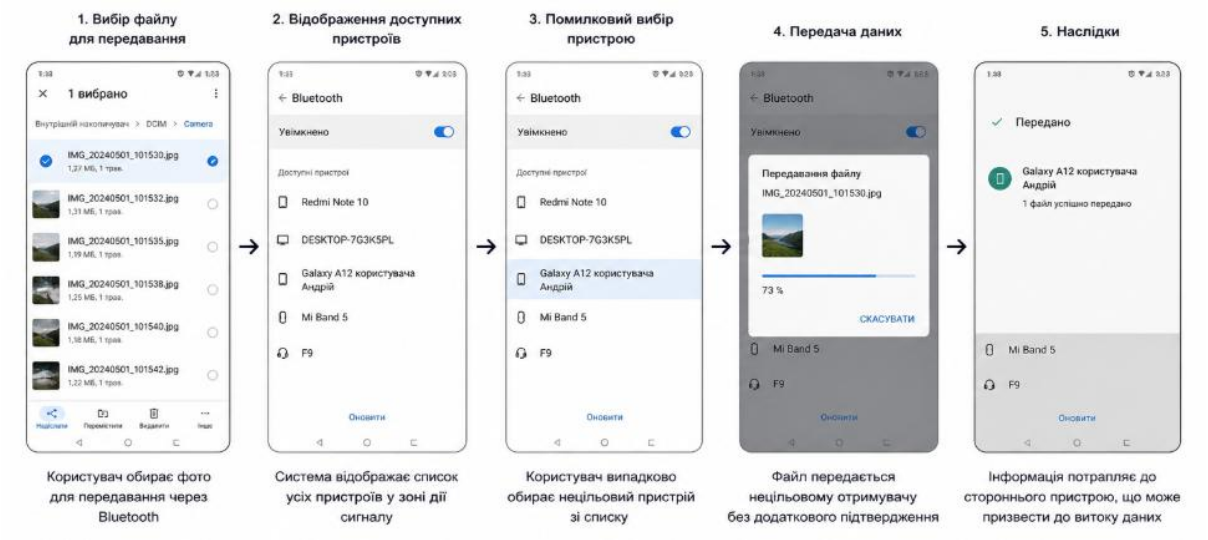


Рисунок 2.1 - Приклад сценарію випадкової передачі приватних даних у безпроводовому середовищі

На відміну від традиційних атак, зокрема атак типу «людина посередині», випадкове передавання інформації не передбачає наявності зловмисника як активного учасника процесу. У даному випадку витік інформації відбувається внаслідок помилки користувача або недосконалості механізмів взаємодії між пристроями. Це робить проблему менш очевидною, проте її наслідки можуть бути не менш критичними.

Сутність проблеми полягає в тому, що під час передавання даних користувач обирає отримувача зі списку доступних пристроїв, які знаходяться в зоні дії безпроводового сигналу. При цьому відсутній механізм, який гарантує,

що обраний пристрій дійсно є цільовим. У результаті інформація може бути передана сторонньому пристрою.

Однією з основних причин виникнення такої ситуації є відкритий характер безпроводового середовища передачі. На відміну від дротових мереж, де канал зв’язку є фізично обмеженим, у безпроводових системах сигнал поширюється у просторі, охоплюючи всі пристрої, що знаходяться в зоні дії. Це означає, що будь-який пристрій у радіусі дії сигналу може бути потенційним отримувачем даних.

Помітний вплив має і інтерфейс користувача. У більшості систем передавання запускається через автоматично сформований список доступних пристроїв, а користувач орієнтується переважно на назву. Якщо поруч є кілька пристроїв із подібними або неінформативними назвами, імовірність помилкового вибору зростає.

Особливо небезпечними є сценарії, що виникають у публічних місцях, таких як кафе, транспорт або навчальні заклади. У таких умовах одночасно може працювати велика кількість пристроїв, що призводить до перевантаження списку доступних варіантів. Користувач не має можливості точно ідентифікувати свій пристрій серед інших, що підвищує ризик помилкового вибору.

Крім того, значний вплив на виникнення проблеми має людський фактор. Більшість користувачів не приділяє достатньої уваги перевірці отримувача перед передаванням даних. Поспішність, звичка до автоматичних дій та довіра до системи призводять до того, що рішення приймаються інтуїтивно, без належного аналізу.

Також важливу роль відіграють фізичні характеристики безпроводового сигналу. Рівень сигналу залежить від відстані між пристроями, наявності перешкод та зовнішніх завад. У результаті пристрої можуть з’являтися або зникати зі списку доступних, що ускладнює процес вибору та створює додаткову невизначеність.

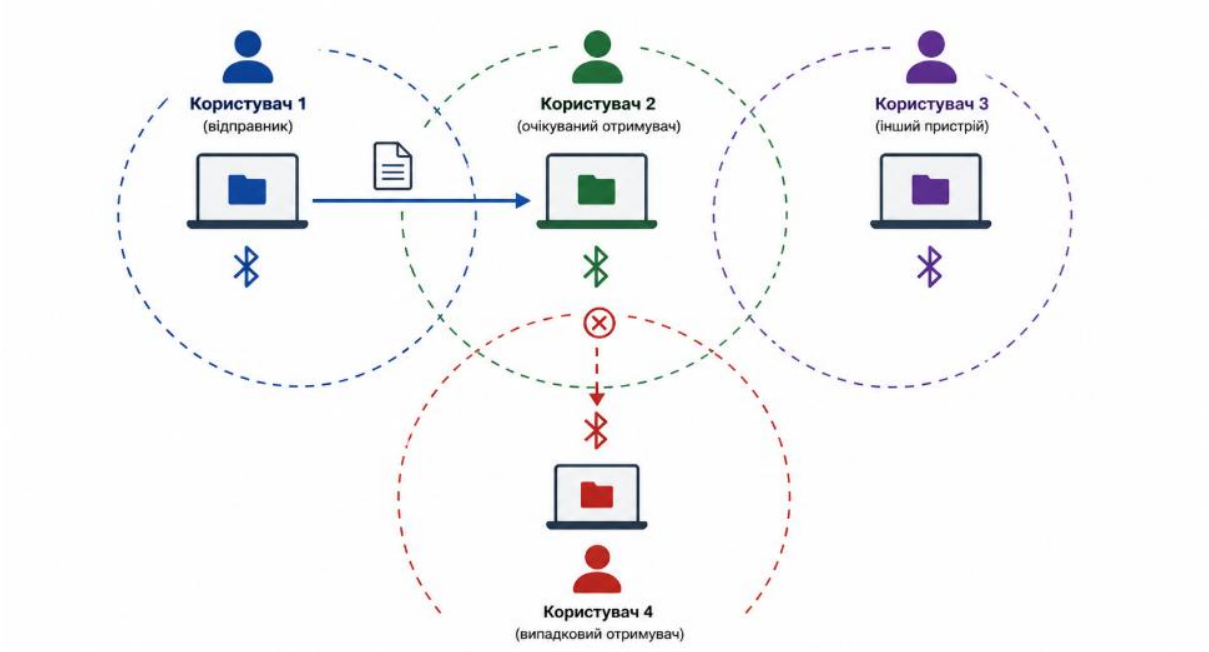


Рисунок 2.2 - Ініціація передавання інформації користувачу

У підсумку, випадкова передача приватних даних є комплексною проблемою, що виникає внаслідок взаємодії технічних особливостей безпроводових технологій та поведінкових факторів користувача. Вона не може бути повністю усунена традиційними методами захисту, що обумовлює необхідність подальшого дослідження та розробки нових підходів.

## 2.2 Методи виявлення випадкового передавання даних

Виявлення випадкової передачі приватних даних у безпроводових мережах є складним завданням, оскільки на відміну від класичних кіберзагроз, цей процес не супроводжується явними ознаками атаки. Передача інформації відбувається у межах легітимного функціонування системи, що ускладнює ідентифікацію помилки. Саме тому традиційні методи виявлення загроз, такі як системи моніторингу мережевого трафіку або засоби виявлення вторгнень, не здатні ефективно визначати подібні ситуації [10-12].

Основною проблемою є те, що система сприймає дії користувача як коректні, навіть якщо вони фактично призводять до витоку інформації. У зв’язку з цим виникає необхідність застосування нових підходів до виявлення, які враховують не лише технічні параметри передачі, але й контекст взаємодії між пристроями.

Одним із ключових напрямків є контекстний аналіз передавання даних. Під контекстом розуміється сукупність параметрів, що описують умови, у яких відбувається взаємодія між пристроями. До таких параметрів належать відстань між пристроями, рівень сигналу, тривалість з'єднання, історія попередніх підключень, а також тип переданих даних. Аналіз цих характеристик дозволяє визначити, наскільки поточна передача відповідає типовій поведінці користувача [10-12].

Особливе значення у цьому контексті має показник **RSSI (Received Signal Strength Indicator)**, який використовується для оцінки сили прийнятого сигналу. Оскільки рівень сигналу зменшується зі збільшенням відстані між пристроями, цей параметр може бути використаний як непрямий індикатор їх просторового розташування. У випадку, якщо передача здійснюється до пристрою з низьким рівнем сигналу, це може свідчити про те, що він знаходиться поза безпечною зоною взаємодії, що підвищує ймовірність помилки.

Ще одним важливим підходом є аналіз поведінки користувача. У цьому випадку система відслідковує типові сценарії використання, зокрема, до яких пристроїв користувач підключається найчастіше, у яких умовах відбувається передавання даних та які типи файлів передаються. Якщо поточна дія суттєво відрізняється від звичайної поведінки, вона може бути класифікована як потенційно небезпечна. Наприклад, передача конфіденційного файлу на невідомий пристрій може розглядатися як аномалія.

Крім того, може застосовуватися **метод часової кореляції**, який передбачає аналіз часу взаємодії між пристроями. Якщо передача здійснюється занадто швидко після появи пристрою у списку доступних, це може свідчити про відсутність належної перевірки з боку користувача.

Ще одним підходом є використання **додаткових підтверджень передачі**, які дозволяють перевірити правильність вибору отримувача. Це може включати відображення додаткової інформації про пристрій, підтвердження через інший канал зв'язку або використання фізичної взаємодії між пристроями. Хоча такі

методи не є прямими засобами виявлення, вони дозволяють знизити ймовірність помилки та виступають як механізм додаткового контролю.

Важливим напрямком також є **комбінування кількох методів**. Окремо жоден із підходів не забезпечує достатнього рівня точності, однак їх спільне використання дозволяє підвищити ефективність виявлення. Наприклад, поєднання аналізу RSSI та поведінкових характеристик дозволяє більш точно визначити, чи відповідає передача типовому сценарію використання.

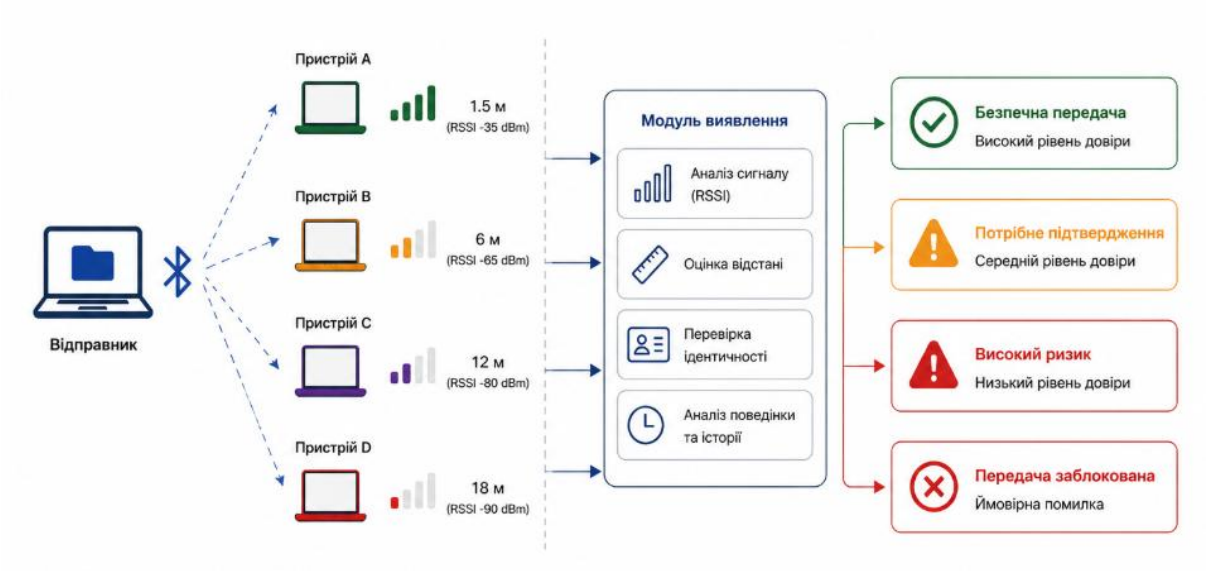


Рисунок 2.3 - Методи виявлення випадкового передавання даних

Водночас, існуючі підходи мають низку обмежень. Зокрема, показник RSSI може змінюватися під впливом перешкод, що знижує точність оцінки відстані. Поведінковий аналіз потребує накопичення статистичних даних, що не завжди можливо на початкових етапах використання системи. Крім того, надмірна кількість перевірок може негативно впливати на зручність користування.

У підсумку, виявлення випадкового передавання даних потребує комплексного підходу, який поєднує аналіз фізичних параметрів сигналу, поведінкових характеристик користувача та контексту взаємодії між пристроями. Це дозволяє сформувати основу для подальшої розробки ефективних методів запобігання витоку інформації.

## 2.3 Методи запобігання випадковій передачі приватних даних

Запобігання випадковій передачі приватних даних є одним із ключових завдань забезпечення безпеки у безпроводових мережах. На відміну від традиційних кіберзагроз, ця проблема виникає не через порушення захисту системи, а через недосконаліть механізмів взаємодії та людський фактор. Це означає, що стандартні підходи, такі як шифрування або автентифікація, не здатні повністю усунути ризик помилкової передачі.

Одним із базових напрямків запобігання є **удосконалення інтерфейсів користувача**. Оскільки саме через інтерфейс здійснюється вибір отримувача, його якість безпосередньо впливає на ймовірність помилки. Зокрема, доцільним є відображення додаткових параметрів, таких як рівень сигналу, приблизна відстань до пристрою або індикатор довіри. Це дозволяє користувачу приймати більш обґрунтовані рішення.

Іншим важливим підходом є обмеження зони передавання даних. Ідея полягає у тому, щоб дозволити передачу лише тим пристроям, які знаходяться в межах певної фізичної відстані. Такий підхід може бути реалізований за допомогою аналізу рівня сигналу RSSI. Якщо сигнал перевищує заданий поріг, пристрій вважається таким, що знаходиться у «зоні довіри». У протилежному випадку передача блокується або потребує додаткового підтвердження.

Також ефективним є використання технологій короткої дальності, зокрема NFC. Оскільки для передавання даних необхідно фізично наблизити пристрої один до одного, ризик випадкового вибору значно знижується. Однак цей підхід має обмеження, пов’язані з невеликою швидкістю передачі та необхідністю фізичної взаємодії.

Ще одним методом є використання багатофакторного підтвердження. У цьому випадку передавання даних здійснюється лише після підтвердження через додатковий канал, наприклад, введення коду, що відображається на обох пристроях. Це дозволяє переконатися, що передача здійснюється саме між потрібними пристроями.

Важливу роль відіграє також **використання списків довірених пристроїв**. Передача даних дозволяється лише між пристроями, які вже були

раніше підтверджені користувачем. Проте цей підхід не є універсальним, оскільки не враховує зміну фізичного контексту, наприклад, якщо пристрій знаходиться на значній відстані.

Додатково можуть застосовуватися **методи інтелектуального аналізу**, які враховують поведінкові характеристики користувача. Система може блокувати або обмежувати передачу, якщо вона не відповідає типовим сценаріям використання. Наприклад, передача великого обсягу даних на невідомий пристрій може вимагати додаткового підтвердження.

Однак усі наведені методи мають певні недоліки. Обмеження зони передачі може бути неточним через нестабільність сигналу. Додаткові підтвердження ускладнюють процес взаємодії та знижують зручність використання. Використання списків довірених пристроїв не враховує зміну умов середовища.

Основною проблемою існуючих підходів є те, що вони розглядають безпеку переважно з погляду захисту каналу передачі, але не враховують правильність вибору отримувача. У результаті навіть при наявності шифрування та автентифікації інформація може бути передана нецільовому пристрою.

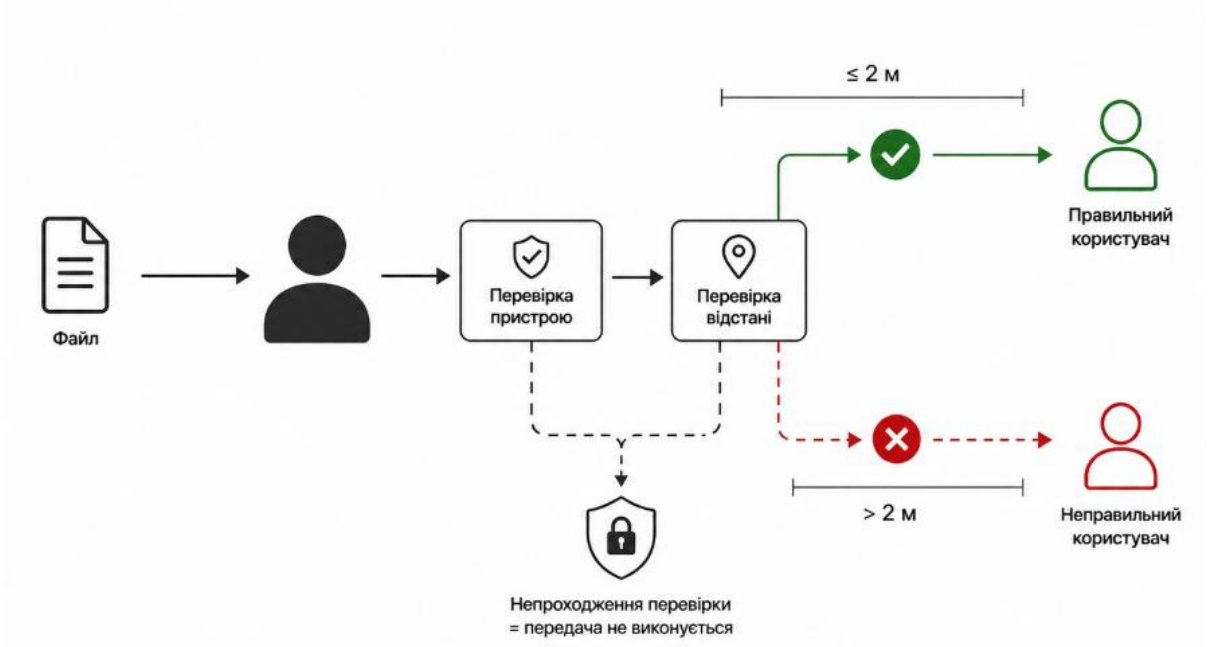


Рисунок 2.4 - Методи запобігання випадковому передаванню даних

У підсумку, ефективне запобігання випадковому передаванню даних можливе лише при комплексному підході, який поєднує аналіз фізичних параметрів сигналу, удосконалення інтерфейсів користувача та врахування поведінкових факторів. Це створює передумови для розробки нових методів, які забезпечують контроль не лише безпеки каналу, але й правильності передавання даних.

### 2.4 Висновки за розділом 2

У другому розділі було проведено детальний аналіз загроз безпеці, пов’язаних із передаванням даних у безпроводових мережах. Особливу увагу приділено проблемі випадкової передачі приватної інформації, яка є недостатньо дослідженою, але має значний вплив на рівень безпеки сучасних мобільних систем.

Було встановлено, що основними причинами виникнення проблеми є відкритий характер безпроводового середовища, велика кількість пристроїв у зоні дії сигналу, недосконалість інтерфейсів та людський фактор.

Розглянуто основні підходи до виявлення таких ситуацій, серед яких аналіз рівня сигналу, поведінкові методи та контекстна оцінка взаємодії. Водночас встановлено, що існуючі рішення не забезпечують повноцінного контролю правильності передавання даних.

Аналіз методів запобігання показав, що найбільш перспективним є використання підходів, заснованих на обмеженні зони передачі та врахуванні фізичної близькості пристроїв.

Отримані результати є основою для розробки методу безпечної передачі приватних даних, який буде розглянуто у наступному розділі.

# 3. ОГЛЯД МЕТОДІВ ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ

## 3.1 Методи шифрування та автентифікації

За нинішнього розвитку мобільних та безпроводових технологій питання захисту інформації набуває особливої актуальності. Смартфони, планшети, ноутбуки та інші мобільні пристрої використовуються не лише для комунікації, але й для зберігання великої кількості конфіденційної інформації. До таких даних належать персональні фотографії, фінансові документи, електронне листування, корпоративні файли, медичні дані, паролі та інша приватна інформація.

Передача даних між пристроями найчастіше здійснюється за допомогою безпроводових технологій, серед яких найбільш поширеними є Bluetooth, Wi-Fi Direct та NFC. Ці технології забезпечують швидкий та зручний обмін файлами між користувачами без необхідності використання кабельного підключення або зовнішніх носіїв інформації. Проте спрощення процедури передавання даних одночасно призвело до виникнення нових загроз інформаційній безпеці.

Однією з найбільш поширених проблем є випадкова передача приватних даних сторонньому користувачу. На практиці користувач під час вибору отримувача орієнтується переважно на назву пристрою, яка часто не є унікальною. Наприклад, у межах одного приміщення можуть одночасно знаходитись декілька пристроїв з однаковими назвами «iPhone», «Galaxy», «Laptop» або «Redmi». У результаті користувач може випадково вибрати неправильний пристрій та передати конфіденційну інформацію сторонній особі.

Ця проблема є особливо небезпечною через те, що більшість сучасних систем захисту орієнтована переважно на запобігання перехопленню інформації, атакам типу «людина посередині» або несанкціонованому доступу. При цьому правильність вибору отримувача у більшості випадків повністю покладається на самого користувача.

Для забезпечення безпечного передавання інформації сучасні системи використовують криптографічні методи захисту. Основною метою шифрування є забезпечення конфіденційності даних навіть у випадку перехоплення трафіку.

У Bluetooth для цього використовуються алгоритми AES та механізми генерації тимчасових криптографічних ключів. У Wi-Fi мережах застосовуються протоколи WPA2 та WPA3, які забезпечують захист каналу зв’язку між пристроями. NFC також використовує криптографічні механізми для захисту платіжних операцій та обміну службовою інформацією [8, 15].

Основною перевагою шифрування є те, що навіть у випадку перехоплення інформації стороння особа не зможе отримати доступ до вмісту даних без відповідного ключа дешифрування. Саме тому криптографічний захист є базовим елементом сучасних систем інформаційної безпеки.

Проте шифрування має суттєві обмеження у контексті досліджуваної проблеми. Насамперед криптографічні механізми не перевіряють правильність вибору отримувача. Якщо користувач помилково обере сторонній пристрій та самостійно підтвердить передачу, система вважатиме таку операцію безпечною, оскільки канал зв’язку буде захищеним з погляду криптографії.

Крім того, шифрування не враховує фізичну близькість між пристроями. Система не аналізує, чи дійсно пристрій-отримувач знаходиться поруч із користувачем, чи передача здійснюється на значній відстані. У результаті навіть повністю захищений канал передачі не гарантує відсутності витоку конфіденційної інформації.

Ще одним важливим механізмом захисту є автентифікація пристроїв. Перед встановленням з’єднання системи виконують процедуру підтвердження справжності пристрою. У Bluetooth для цього використовуються PIN-коди, підтвердження однакових чисел, QR-коди та механізми Secure Simple Pairing. У Wi-Fi мережах застосовується автентифікація за допомогою паролів або цифрових сертифікатів. NFC також використовує криптографічні токени та механізми підтвердження доступу [2, 8].

Автентифікація дозволяє знизити ризик підключення невідомих пристроїв та підвищує загальний рівень безпеки системи. Проте вона також не вирішує проблему випадкового передавання даних повністю. У багатьох випадках

користувач самостійно підтверджує з’єднання, не маючи достатньої інформації про реального власника пристрою.

Особливо це помітно у режимах спрощеного сполучення, наприклад Just Works у Bluetooth Low Energy. Такий режим майже не вимагає додаткової перевірки отримувача і насамперед орієнтований на швидкість та зручність підключення.

Отже, аналіз сучасних методів шифрування та автентифікації показує, що вони ефективно захищають дані від перехоплення та несанкціонованого доступу, проте не забезпечують повного захисту від випадкової передачі приватної інформації стороннім користувачам. Це обґрунтовує необхідність створення додаткових механізмів захисту, які будуть враховувати фізичний контекст взаємодії між пристроями та дозволять перевіряти реальну близькість користувачів під час передавання даних.


Рисунок 3.1 - Процес шифрування та автентифікації під час передавання даних

### 3.2 Використання безпроводових технологій (Bluetooth, Wi-Fi, NFC, BLE, UWB)

Сучасні безпроводові технології забезпечують швидке та зручне передавання інформації між пристроями без використання фізичного кабельного підключення. Саме завдяки розвитку Bluetooth, Wi-Fi, NFC, BLE та UWB користувачі отримали можливість практично миттєво передавати файли, виконувати синхронізацію даних, здійснювати безконтактні платежі та взаємодіяти з великою кількістю цифрових сервісів.

Попри значну зручність використання, кожна із зазначених технологій має власні особливості, переваги та недоліки з погляду безпеки передачі приватних

даних. Частина технологій орієнтована на швидкість передачі, інші - на мінімальне енергоспоживання або високу точність визначення відстані між пристроями.

Bluetooth є однією з найбільш поширених технологій безпроводового передавання даних на короткі відстані. Ця технологія використовується у смартфонах, ноутбуках, навушниках, автомобільних системах, смарт-годинниках та великій кількості IoT-пристроїв [2].

Основною перевагою Bluetooth є універсальність та підтримка практично всіма сучасними мобільними пристроями. Користувач може швидко встановити з'єднання між пристроями та передати файли без необхідності використання додаткового обладнання.

Для захисту з'єднання Bluetooth застосовує шифрування та автентифікацію. Під час сполучення пристроїв формується криптографічний ключ, який надалі використовується для захисту передаваних даних.

У сучасних версіях Bluetooth використовуються механізми Secure Simple Pairing, які дозволяють знизити ризик перехоплення даних або підміни пристрою. Також застосовуються алгоритми AES для шифрування трафіку [2].

Проте Bluetooth має ряд суттєвих обмежень у контексті досліджуваної проблеми. Насамперед система не перевіряє, чи дійсно користувач обрав правильний пристрій для передачі файлу. Якщо користувач помилково підтвердить передачу сторонньому пристрою, система вважатиме таке з'єднання легітимним.

Окремою проблемою є те, що у громадських місцях користувач може бачити велику кількість доступних Bluetooth-пристроїв з однаковими або схожими назвами. Через це ймовірність помилки значно зростає.

Крім того, Bluetooth має відносно велику дальність роботи. У сучасних версіях технології дистанція передачі може становити десятки метрів, що збільшує ризик випадкового підключення стороннього пристрою.

У підсумку, Bluetooth забезпечує достатній рівень криптографічного захисту, проте не вирішує проблему контролю фізичної близькості між користувачами.

Технологія Wi-Fi широко використовується для побудови локальних мереж та передачі великих обсягів інформації. Однією з переваг Wi-Fi є висока швидкість передавання даних, що дозволяє передавати великі файли значно швидше порівняно з Bluetooth.

У контексті прямої взаємодії між пристроями особливий інтерес становить технологія Wi-Fi Direct. Вона дозволяє пристроям створювати пряме з'єднання без використання маршрутизатора або точки доступу [5].

Для захисту даних у Wi-Fi використовуються сучасні протоколи WPA2 та WPA3, які забезпечують шифрування трафіку та захист від несанкціонованого доступу [14].

Попри це, Wi-Fi також має низку обмежень у контексті безпечної передачі приватних даних. Насамперед технологія орієнтована переважно на швидкість передачі та стабільність каналу зв'язку, а не на контроль фізичної близькості між користувачами.

Дальність роботи Wi-Fi може досягати десятків метрів навіть у приміщеннях. Через це користувач може випадково передати інформацію пристрою, який знаходиться поза межами безпечної зони.

Крім того, Wi-Fi мережі є більш вразливими до різноманітних атак, пов'язаних із підміною точки доступу або створенням фальшивих мереж. У випадку недостатньої уважності користувача це також може призвести до компрометації інформації.

У підсумку, Wi-Fi є ефективним інструментом для швидкого передавання даних, проте не забезпечує достатнього контролю безпечної дистанції між пристроями.

Технологія NFC використовується для безконтактної взаємодії між пристроями на дуже малих відстанях. У більшості випадків дистанція роботи NFC становить декілька сантиметрів [4].

Саме завдяки цьому NFC вважається однією з найбільш безпечних технологій у контексті підтвердження фізичної присутності користувача. Для встановлення з’єднання користувачі повинні фактично торкнутися пристроями один одного або максимально наблизити їх [4, 13].

Дана особливість значно знижує ризик випадкового підключення стороннього пристрою. Саме тому NFC широко використовується у системах безконтактної оплати, цифрових ключах, електронних перепустках та механізмах швидкого сполучення пристроїв.

Проте NFC має і суттєві недоліки. Основною проблемою є низька швидкість передавання даних. Через це технологія практично не використовується для передачі великих файлів.

У більшості сучасних систем NFC застосовується лише для первинної ініціалізації з’єднання, після чого передавання інформації продовжується через Bluetooth або Wi-Fi.

Отже, NFC ефективно забезпечує фізичне підтвердження близькості пристроїв, але не може повністю виконувати роль універсального каналу передавання даних.

Bluetooth Low Energy є спеціалізованою версією Bluetooth, яка орієнтована на мінімальне енергоспоживання. Ця технологія активно використовується у смарт-годинниках, фітнес-трекерах, IoT-пристроях та інших системах, які потребують постійного обміну невеликими обсягами інформації [3].

Однією з ключових особливостей BLE є можливість аналізу параметра RSSI - рівня сили прийнятого сигналу. Значення RSSI дозволяє приблизно оцінити відстань між пристроями [3, 12].

У сучасних системах RSSI вже використовується для визначення пристроїв поблизу, автоматичного блокування при віддаленні користувача або побудови геозон.

Проте RSSI має низку обмежень. На точність вимірювання впливають стіни, меблі, люди, електромагнітні перешкоди та особливості конкретних моделей пристроїв.

Через це значення RSSI може значно змінюватися навіть при однаковій фізичній дистанції між пристроями.

Попри зазначені недоліки, RSSI є перспективним інструментом для приблизної оцінки фізичної близькості між користувачами. Саме тому у цій роботі пропонується використовувати RSSI як один із додаткових механізмів перевірки безпечності передавання даних.

Ultra Wideband є сучасною технологією безпроводового зв'язку, яка дозволяє з високою точністю визначати фізичну відстань між пристроями [6].

На відміну від RSSI, де оцінка дистанції базується на силі сигналу, UWB використовує аналіз часу проходження імпульсу між пристроями. Це дозволяє визначати відстань з точністю до кількох сантиметрів [6].

UWB вже використовується у сучасних системах цифрових ключів автомобілів, механізмах захищеного доступу та технологіях просторового позиціонування.

Однією з головних переваг UWB є складність реалізації relay-атак. Система може перевіряти реальну фізичну дистанцію між пристроями, що підвищує рівень безпеки.

Проте технологія має і певні недоліки. Насамперед UWB підтримується не всіма мобільними пристроями. Крім того, для роботи необхідне спеціалізоване обладнання, що збільшує вартість реалізації системи.

Також використання UWB може призводити до підвищеного енергоспоживання, що є важливим фактором для мобільних пристроїв.

Попри це, UWB є однією з найбільш перспективних технологій для реалізації систем безпечної передачі приватних даних на близькій відстані.

Таблиця 3.2 - Порівняння безпроводових технологій передавання даних

| **Технологія** | **Типова дистанція роботи** | **Швидкість передачі даних** | **Основні переваги** | **Основні недоліки** | **Використання у контексті безпеки** |
|---|---|---|---|---|---|
| Bluetooth | До 10-50 м | Середня | Універсальність, | Можливість | Використовується для |

| | | | | | |
|---|---|---|---|---|---|
| | | | підтримка більшістю пристроїв, простота використання | випадкового підключення сторонньо го пристрою, велика кількість доступних пристроїв у зоні дії | передачі файлів та сполучення пристроїв |
| Wi-Fi / Wi-Fi Direct | До 50-100 м | Висока | Висока швидкість передачі, можливість передавати великі файли | Велика дистанція роботи, ризик передачі даних поза безпечною зоною | Захищені канали передачі даних через WPA2/WPA3 |
| NFC | До 10 см | Низька | Фізичне підтвердженн я близькості пристроїв, низька ймовірність випадкового підключення | Низька швидкість передачі, непридатн ість для великих файлів | Безконтактн і платежі, ініціалізація безпечного з’єднання |
| BLE | До 10-30 м | Низька / середня | Низьке енергоспожив ання, можливість аналізу RSSI | Неточн ість оцінки дистанції через вплив перешкод | IoT-пристрої, контроль близькості |
| UWB | До 10-30 м | Середн я | Високоточ не визначення дистанції, захист від relay-атак | Висока вартість, підтримує ться не всіма пристроям и | Визначення фізичної близькості та побудова зона довіри |

### 3.3 Обмеження існуючих рішень та обґрунтування запропонованого методу

Проведений аналіз існуючих методів захисту показує, що сучасні системи інформаційної безпеки переважно орієнтовані на захист даних від зовнішніх загроз. Більшість технологій спрямована на запобігання перехопленню інформації, несанкціонованому доступу, підміні пристроїв або компрометації криптографічних ключів. Для цього використовуються механізми шифрування, автентифікації, цифрові сертифікати, токени доступу та інші інструменти захисту [8-12].

Проте проблема випадкової передачі приватних даних сторонньому користувачу досі залишається недостатньо дослідженою. У більшості сучасних систем правильність вибору отримувача фактично повністю залежить від самого користувача. Система не виконує додаткової перевірки того, чи дійсно файл надсилається потрібній особі.

Одним із головних недоліків сучасних рішень є відсутність аналізу фізичної близькості між пристроями. У більшості випадків система не враховує, наскільки близько знаходиться отримувач. Через це користувач може випадково передати файл сторонньому пристрою, який знаходиться у зоні дії безпроводового сигналу.

Особливо актуальною ця проблема є у громадських місцях: офісах, університетах, торгових центрах, аеропортах або конференц-залах. У таких умовах одночасно можуть знаходитися десятки пристроїв з подібними назвами, через що ризик помилкового вибору значно зростає.

Ще однією проблемою є орієнтація систем переважно на назву пристрою. У більшості мобільних операційних систем користувач бачить лише коротке ім’я пристрою без додаткової інформації про його власника. Через це навіть уважний користувач не завжди може однозначно визначити правильного отримувача.

Також сучасні системи практично не враховують фізичний контекст взаємодії. Система не аналізує середовище передачі, стабільність сигналу, реальне положення пристроїв або зміну відстані між ними. У результаті навіть захищене з’єднання може використовуватись для помилкової передачі конфіденційної інформації.

Додатковою проблемою є надмірне спрощення процедури підключення. Для підвищення зручності користувача сучасні системи намагаються мінімізувати кількість підтверджень та скоротити час встановлення з’єднання. Проте зменшення кількості перевірок одночасно збільшує ризик помилки з боку користувача.

Крім того, існуючі рішення не використовують механізм оцінки ризику передачі залежно від типу інформації. Наприклад, система однаково обробляє передачу звичайної фотографії та передачу фінансових документів або паролів, хоча рівень потенційних наслідків у цих випадках суттєво відрізняється.

На сьогодні існують окремі рішення, які частково дозволяють знизити ризик випадкового передавання даних. Наприклад, NFC забезпечує дуже малу дистанцію для ініціалізації з’єднання, а RSSI дозволяє приблизно оцінити близькість пристроїв. Технологія UWB взагалі дозволяє визначати відстань з високою точністю [4, 6, 12].


Рисунок 3.3 - Проблема випадкового передавання даних сторонньому пристрою

Проте кожна з цих технологій окремо має власні обмеження. NFC не підходить для передачі великих обсягів інформації через низьку швидкість передавання даних. RSSI має недостатню точність через вплив навколишнього

середовища, перешкод та особливостей конкретних пристроїв. UWB забезпечує високу точність вимірювання, але потребує спеціального обладнання та підтримується не всіма мобільними пристроями.

У підсумку, проведений аналіз показує, що існуючі методи безпеки вирішують проблему лише частково. Шифрування забезпечує конфіденційність інформації, автентифікація підтверджує справжність пристрою, NFC дозволяє виконати фізичне підтвердження на короткій дистанції, RSSI використовується для приблизної оцінки близькості, а UWB забезпечує точне визначення відстані.

Проте жодне із зазначених рішень окремо не забезпечує комплексного захисту саме від випадкової передачі приватних даних сторонньому користувачу. Саме тому у цій роботі пропонується комбінований метод, який об’єднує переваги декількох технологій одночасно та враховує фізичний контекст взаємодії між пристроями.

### 3.4 Висновки за розділом 3

У цьому розділі було проведено детальний аналіз сучасних методів захисту передавання даних у безпроводових мережах. Розглянуто особливості використання шифрування, автентифікації, контролю доступу та сучасних безпроводових технологій, серед яких Bluetooth, Wi-Fi, NFC, BLE та UWB.

Проведений аналіз показав, що сучасні системи безпеки ефективно забезпечують захист інформації від перехоплення, несанкціонованого доступу та ряду мережевих атак. Для цього використовуються криптографічні алгоритми, механізми підтвердження особи пристрою, цифрові сертифікати та захищені канали передавання даних.

Проте встановлено, що більшість існуючих рішень орієнтована переважно на захист каналу передавання інформації, а не на перевірку правильності вибору отримувача. У результаті проблема випадкової передачі приватних даних сторонньому користувачу залишається актуальною навіть при використанні сучасних засобів захисту.

Також встановлено, що існуючі технології лише частково дозволяють вирішити зазначену проблему. NFC забезпечує фізичне підтвердження

близькості пристроїв, RSSI дозволяє приблизно оцінювати дистанцію між ними, а UWB забезпечує високоточне визначення відстані. Проте кожна із технологій окремо має власні обмеження та не забезпечує комплексного підходу до безпечної передачі приватної інформації.

У результаті аналізу було обґрунтовано необхідність створення нового комбінованого методу, який буде враховувати не лише криптографічний захист інформації, але й фізичний контекст взаємодії між пристроями.

У цій роботі запропоновано метод безпечної передачі приватних даних на близькій відстані, який базується на комбінуванні NFC, Bluetooth Low Energy, RSSI та UWB. Основною особливістю запропонованого підходу є формування зони довіри - контрольованої безпечної області, у межах якої дозволяється передача конфіденційної інформації.

Запропонований метод дозволяє знизити ризик випадкового передавання даних стороннім користувачам, забезпечити додаткову перевірку фізичної близькості між пристроями та підвищити загальний рівень безпеки безпроводової взаємодії.

Отже, результати проведеного аналізу підтверджують доцільність використання комбінованого підходу для реалізації більш безпечної передачі приватних даних у сучасних мобільних системах.

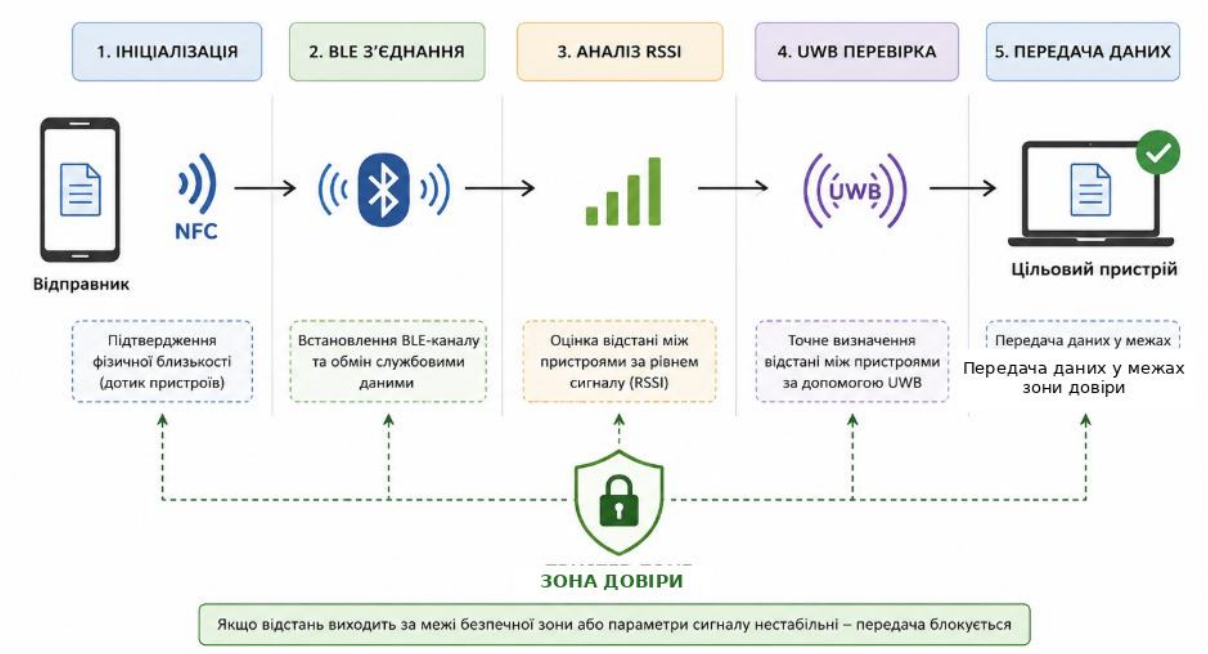


Рисунок 3.4 - Структура запропонованого комбінованого методу безпечного передавання даних

# 4. МЕТОД БЕЗПЕЧНОЇ ПЕРЕДАЧІ ПРИВАТНИХ ДАНИХ НА БЛИЗЬКІЙ ВІДСТАНІ

## 4.1 Загальна концепція методу

Запропонований у роботі метод призначений для зменшення ризику випадкової передачі приватних даних нецільовому отримувачу під час використання безпроводових каналів короткої та середньої дальності. Його основна ідея полягає не лише у захисті каналу передавання, а й у перевірці контексту самої дії передавання: який саме файл передається, кому він надсилається, на якій відстані розташований отримувач і чи можна вважати поточні умови достатньо безпечними [2-6, 12].

На відміну від класичних механізмів шифрування й автентифікації, запропонований метод не обмежується перевіркою криптографічної коректності з'єднання. Шифрування захищає інформацію від перехоплення, але не запобігає ситуації, коли сам користувач помилково надсилає файл іншому пристрою. Тому в роботі пропонується додати до процесу передавання шар контекстної перевірки, який оцінює фізичну близькість, довіру до пристрою та рівень приватності даних.

Практичне значення методу полягає у тому, що система може автоматично відрізняти звичайні файли від чутливих, розпізнавати довірений пристрій серед інших доступних пристроїв і приймати рішення про передавання без повного перекладання відповідальності на користувача. Таким чином, метод виконує роль додаткового захисного фільтра між дією користувача та фактичним надсиланням приватної інформації.

У межах розробленого підходу передавання даних розглядається як послідовність взаємопов'язаних етапів. Спочатку система аналізує сам файл і визначає його рівень приватності. Далі виконується ідентифікація потенційного отримувача, перевірка фізичної близькості через NFC, BLE/RSSI або UWB, формування зони довіри та прийняття кінцевого рішення. Якщо хоча б один із критичних параметрів не відповідає вимогам, передавання блокується або потребує додаткового підтвердження.

У роботі пропонується використовувати адаптивну модель безпеки. Її сутність полягає у тому, що однакові правила не застосовуються до всіх файлів без винятку. Для відкритих або малочутливих даних достатньо базової перевірки отримувача, тоді як для персональних, фінансових або службових документів необхідний посилений контроль. Такий підхід дозволяє не перевантажувати користувача зайвими підтвердженнями під час передавання звичайних файлів, але підвищує рівень захисту для інформації, витік якої може мати серйозні наслідки.

Структурно метод складається з п'яти основних модулів: модуля визначення приватності даних, модуля розпізнавання отримувача, модуля оцінювання відстані, модуля формування зони довіри та модуля прийняття рішення. Кожен з цих модулів виконує власну функцію, однак остаточний висновок формується лише після їх спільного аналізу.

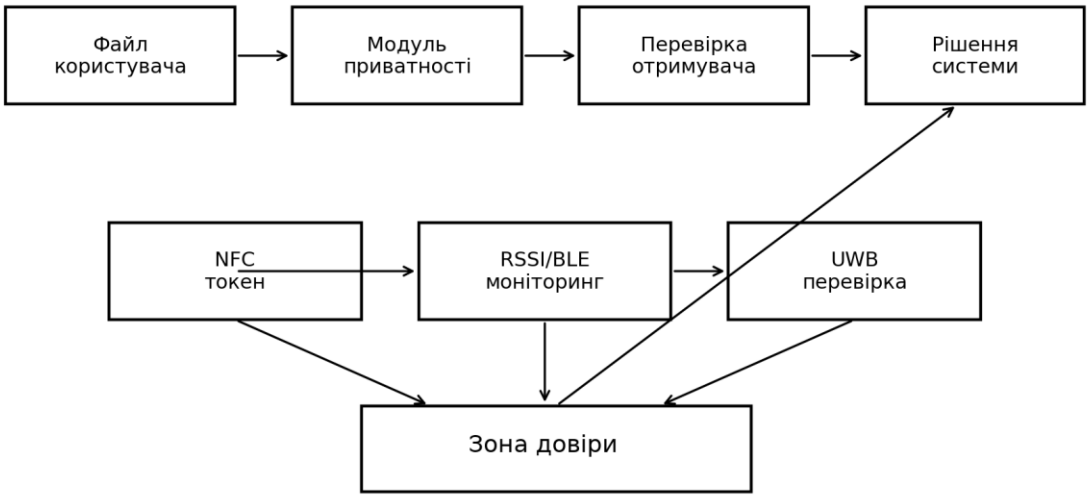


Рисунок 4.1 - Загальна структура запропонованого методу безпечної передачі приватних даних

Перший модуль відповідає за попередню класифікацію даних. Він аналізує назву файлу, його тип, розширення, метадані, наявність типових маркерів конфіденційності та за потреби короткий фрагмент вмісту. Наприклад, файл з назвою «passport_scan.pdf» або «bank_statement.xlsx» має вищий початковий

рівень приватності, ніж файл із загальнодоступним зображенням. Такий аналіз не замінює повноцінної системи запобігання витоку даних, але створює достатню основу для прийняття рішення в межах локального передавання між пристроями.

Другий модуль призначений для перевірки отримувача. У звичайних системах користувач бачить лише назву пристрою, що є недостатнім у середовищі з великою кількістю однотипних смартфонів або ноутбуків. У запропонованому методі до назви додаються інші ознаки: чи був пристрій раніше підтверджений, чи отримано NFC-токен, чи відповідає його ідентифікатор запису в локальному списку довіри, чи зберігається стабільна фізична близькість протягом усього часу передачі.

Третій модуль виконує оцінювання відстані. Базовим джерелом інформації є RSSI, оскільки цей показник доступний у більшості реалізацій Bluetooth Low Energy і не потребує спеціального обладнання. Для пристроїв, які підтримують UWB, метод може використовувати точніше вимірювання відстані. У такому випадку RSSI застосовується як швидкий фільтр, а UWB - як механізм підтвердження.

Четвертий модуль формує зона довіри. Під зоною довіри у роботі розуміється не просто геометрична відстань між пристроями, а логічна безпечна область, у межах якої виконуються умови для передавання даних певного рівня приватності. Наприклад, для звичайного файлу допустимою може бути відстань до 5 метрів, тоді як для фінансового документа - не більше 1-2 метрів і лише за наявності додаткового підтвердження.

П'ятий модуль приймає рішення про подальшу дію. Рішення може мати три основні варіанти: передавання дозволяється, передавання дозволяється лише після підтвердження користувача або передавання блокується. Така градація є важливою, оскільки не кожне відхилення параметрів означає явну небезпеку. Наприклад, короткочасне погіршення RSSI може бути наслідком перешкоди, а не спроби помилкового передавання. Тому метод враховує не лише одиничне значення параметра, а й його стабільність у часі.

Концептуально запропонований підхід можна розглядати як поєднання технічної та поведінкової безпеки. Технічна складова полягає у використанні RSSI, NFC, UWB і криптографічного підтвердження. Поведінкова складова полягає у тому, що система допомагає користувачу уникнути помилки під час вибору отримувача, не покладаючись лише на його уважність.

Важливо, що метод не потребує повної заміни існуючих протоколів передавання. Він може бути реалізований як додатковий рівень над уже наявними механізмами Bluetooth, Wi-Fi Direct або локального обміну файлами. У такому випадку стандартний канал відповідає за фактичну передавання даних, а запропонований метод - за попереднє рішення щодо безпечності такої передачі.

Особливістю запропонованого рішення є можливість роботи у двох режимах. У першому режимі система використовує лише доступні на більшості пристроїв параметри, зокрема BLE та RSSI. У другому режимі за наявності UWB застосовується високоточна перевірка дистанції. Це дозволяє використовувати метод як на масових мобільних пристроях, так і на новіших моделях із розширеними можливостями просторового позиціонування.

Таблиця 4.1 - Основні функціональні модулі запропонованого методу

| **Модуль** | **Вхідні дані** | **Результат роботи** | **Практичне призначення** |
|---|---|---|---|
| Визначення приватності | Тип файлу, назва, метадані, маркери вмісту | Клас приватності даних | Вибір рівня перевірок перед передаванням |
| Розпізнавання отримувача | Ім’я пристрою, ідентифікатор, історія довіри, NFC-токен | Оцінка належності пристрою до довірених | Зменшення ризику вибору стороннього пристрою |
| Оцінка відстані | RSSI, динаміка сигналу, UWB-вимірювання | Орієнтовна або точна дистанція | Перевірка фізичної близькості |
| зона довіри | Клас даних, дистанція, стабільність сигналу | Статус безпечної зони | Обмеження передавання у межах допустимої області |

| | | | |
|---|---|---|---|
| Прийняття рішення | Оцінки всіх попередніх модулів | Дозвіл, підтвердження або блокування | Фінальний контроль перед фактичною передачею |

Для визначення рівня приватності у роботі використовується набір правил, який може бути реалізований як простий локальний класифікатор. На практиці це важливо, оскільки не всі користувачі самостійно оцінюють чутливість файлу перед надсиланням. Система, навпаки, може звернути увагу на ознаки ризику і застосувати відповідний режим захисту.

Наприклад, якщо користувач передає фотографію без персональних ознак, система може застосувати спрощений сценарій: перевірити, що пристрій отримувача перебуває поблизу, і дозволити передачу. Якщо ж файл містить слова «паспорт», «договір», «рахунок», «пароль», «медична довідка» або має формат документа з персональними даними, метод переходить до посиленого сценарію, де потрібне підтвердження близькості та довіреності отримувача.

Таблиця 4.2 - Класифікація даних за рівнем приватності

| **Рівень** | **Типові приклади** | **Ознаки для автоматичного визначення** | **Рекомендований режим передачі** |
|---|---|---|---|
| P0 - відкриті дані | Загальні зображення, відкриті презентації, публічні матеріали | Відсутність персональних маркерів, нейтральна назва файлу | Базова перевірка отримувача |
| P1 - особисті дані | Приватні фото, нотатки, особисті повідомлення | Слова «private», «особисте», «фото», «листування», метадані користувача | Контроль RSSI та підтвердження отримувача |
| P2 - конфіденційні дані | Паспортні копії, фінансові документи, договори, медичні файли | Слова «паспорт», «банк», «договір», «рахунок», PDF/DOCX/XLSX із персональними полями | Посилена зона довіри, RSSI + додаткова перевірка |
| P3 - критичні дані | Паролі, токени доступу, | Слова «password», «token», | Передача лише у ближній зоні з |

| | | | |
|---|---|---|---|
| | банківські реквізити, ключі | «key», «seed», «PIN», «CVV» | NFC/UWB та ручним підтвердженням |

Класифікація, наведена у таблиці 4.2, не є жорстко фіксованою. У реальній системі користувач або адміністратор може змінювати правила відповідно до власних вимог. Наприклад, у корпоративному середовищі до конфіденційних можуть належати будь-які файли з внутрішніми позначками компанії, тоді як у персональному використанні пріоритетними будуть документи, фотографії та фінансова інформація.

Метод також враховує, що автоматичне визначення приватності не може бути абсолютно безпомилковим. Тому замість категоричного висновку використовується оцінка ризику. Якщо файл має кілька ознак чутливості, йому призначається вищий клас захисту. Такий підхід є безпечнішим, оскільки у випадку невизначеності система обирає більш обережний сценарій.

Для формального опису рівня приватності може використовуватися інтегральний показник P, який формується на основі кількості виявлених ознак, типу файлу та контексту передачі. У спрощеному вигляді його можна подати як зважену суму окремих факторів.

$$P = w1Ftype + w2Fname + w3Fmeta + w4Fcontent \quad (4.1)$$

де P - узагальнений показник приватності; Ftype - ознака типу файлу; Fname - ознака ризикових слів у назві; Fmeta - ознака наявності чутливих метаданих; Fcontent - ознака чутливого вмісту; w1, w2, w3, w4 - вагові коефіцієнти, які визначають важливість кожного фактора.

Значення показника P використовується не для остаточного «вироку», а для вибору режиму безпеки. Якщо показник низький, система дозволяє стандартну передачу після мінімальної перевірки. Якщо показник середній або високий, активується посилений алгоритм із контролем близькості. Якщо показник критичний, передавання без фізичного підтвердження блокується.

Важливим є те, що запропонований метод не намагається повністю автоматизувати рішення замість користувача. Його завдання - зменшити

кількість помилок у тих випадках, коли користувач діє поспіхом, бачить кілька пристроїв з однаковими назвами або не усвідомлює рівень чутливості файлу. Тому метод поєднує автоматичну перевірку та контроль з боку користувача.

У практичній реалізації система може працювати як службовий модуль мобільної операційної системи або як окрема прикладна програма для захищеного обміну файлами. У другому варіанті користувач обирає файл у застосунку, після чого застосунок самостійно виконує пошук отримувачів, аналізує їхню близькість і відображає лише ті пристрої, які відповідають вимогам зони довіри.

Отже, загальна концепція методу полягає у переході від простого принципу «користувач вибрав пристрій - система передала файл» до принципу «користувач вибрав пристрій - система перевірила приватність, близькість і довіру - лише після цього дозволила передачу». Такий підхід робить процес передавання більш керованим і суттєво знижує ризик випадкового розголошення приватних даних.

### 4.2 Використання RSSI для визначення відстані

Одним із центральних параметрів запропонованого методу є RSSI - індикатор рівня прийнятого сигналу. У безпроводових системах цей показник відображає силу сигналу, який приймає один пристрій від іншого. Хоча RSSI не є точним вимірювачем відстані, він може бути використаний як практичний інструмент для попередньої оцінки фізичної близькості між пристроями.

Перевага RSSI полягає у його доступності. Більшість пристроїв із підтримкою Bluetooth Low Energy або Wi-Fi здатні отримувати значення RSSI без використання додаткового обладнання. Це робить параметр зручним для реалізації у масових мобільних системах, де застосування спеціалізованих сенсорів або зовнішніх модулів може бути недоцільним.

У межах роботи RSSI використовується не як самостійний доказ безпечності, а як один із сигналів контекстного аналізу. Це важливе уточнення, оскільки сила сигналу залежить не тільки від відстані, але й від перешкод,

орієнтації антен, положення пристрою у руці користувача, наявності стін, меблів та інших джерел радіозавад.

Для приблизного зв’язку між RSSI та відстанню може застосовуватися логарифмічна модель поширення сигналу. Вона використовується у багатьох практичних задачах позиціонування та дозволяє отримати орієнтовну дистанцію за умови попереднього калібрування параметрів середовища.

$$d = 10^{((A - RSSI) / (10n))} \quad (4.2)$$

де d - орієнтовна відстань між пристроями; A - значення RSSI на відстані 1 м; RSSI - поточне виміряне значення сили сигналу; n - коефіцієнт втрат у середовищі, який залежить від умов поширення сигналу.

У відкритому просторі коефіцієнт n може бути меншим, а в приміщеннях із великою кількістю перешкод - більшим. Саме тому запропонований метод передбачає не використання одного універсального порогу, а гнучку систему діапазонів. Також важливо, що рішення приймається не за одним вимірюванням RSSI, а за усередненим значенням за певний інтервал часу.

Для зменшення впливу випадкових коливань сигналу система використовує ковзне середнє. Наприклад, протягом 2-3 секунд формується набір із k вимірювань RSSI, після чого обчислюється середнє значення. Це дозволяє уникнути ситуації, коли короткочасний спад сигналу через рух руки або появу перешкоди помилково сприймається як вихід пристрою із зони довіри.

$$RSSIavg = (RSSI1 + RSSI2 + ... + RSSIk) / k \quad (4.3)$$

Додатково оцінюється стабільність сигналу. Якщо середнє значення RSSI є прийнятним, але сам сигнал різко коливається, це може свідчити про нестабільні умови або про те, що пристрої знаходяться на межі допустимої зони. У такому випадку система не повинна автоматично дозволяти передачу конфіденційних даних без додаткової перевірки.

Стабільність може бути оцінена через стандартне відхилення значень RSSI у межах вікна спостереження. Чим менше відхилення, тим стабільнішим є канал і тим вищою є довіра до оцінки відстані.

$$\sigma RSSI = \sqrt{\frac{1}{k} \sum (RSSIi - RSSIavg)^2} \quad (4.4)$$

де σRSSI - показник нестабільності сигналу; RSSIi - окреме вимірювання; RSSIavg - середнє значення RSSI за обраний період; k - кількість вимірювань.

Якщо σRSSI перевищує допустиме значення, система може зробити висновок, що канал є нестабільним. Для звичайних даних це може призвести лише до попередження, а для конфіденційних або критичних даних - до блокування передачі або запуску UWB-перевірки.

Практична інтерпретація RSSI у методі побудована на порогових діапазонах. Вони не претендують на абсолютну точність, але дозволяють класифікувати ситуацію як безпечну, умовно безпечну, сумнівну або небезпечну. Такий підхід є доцільним саме для задачі запобігання випадковій передачі, де важливо не виміряти дистанцію з сантиметровою точністю, а відсікти явно віддалені або нестабільні пристрої.

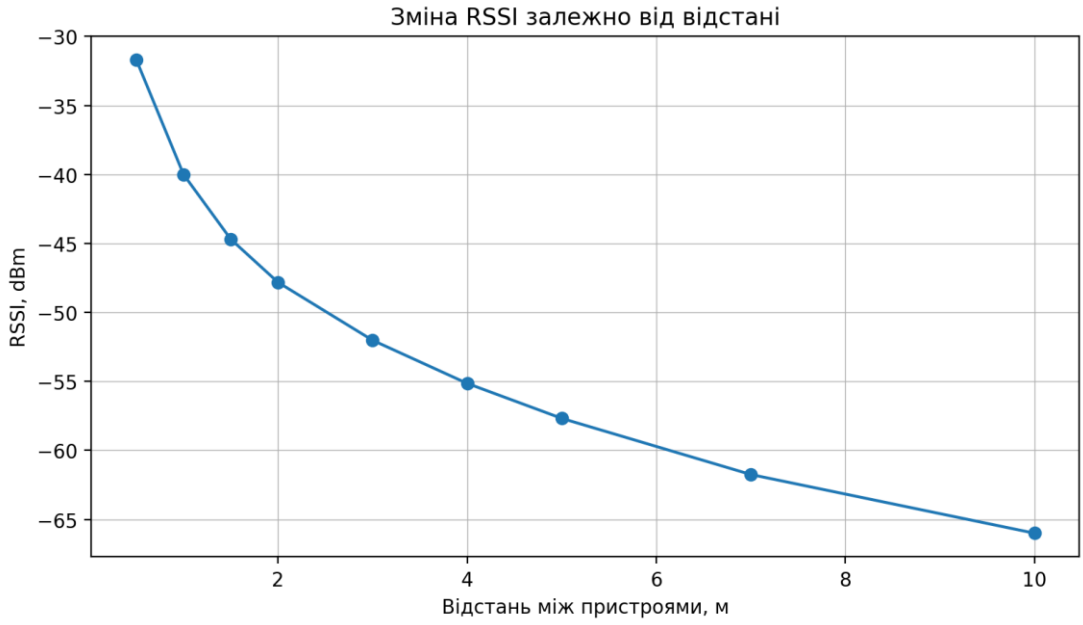


Рисунок 4.2 - Модельна залежність RSSI від відстані між пристроями

Таблиця 4.3 - Інтерпретація значень RSSI у запропонованому методі

| Діапазон RSSI | Орієнтовна дистанція | Стан з'єднання | Рекомендована дія системи |
|---|---|---|---|
| від -30 до -45 dBm | до 1 м | Дуже сильний та стабільний сигнал | Передавання дозволяється для всіх класів за наявності довіреного отримувача |

| | | | |
|---|---|---|---|
| від -46 до -60 dBm | 1-3 м | Стабільний сигнал ближньої взаємодії | Дозволяється для P0-P1, для P2-P3 потрібна додаткова перевірка |
| від -61 до -70 dBm | 3-5 м | Ослаблений сигнал | Передавання P0 можливе, P1-P3 потребують підтвердження або блокуються |
| від -71 до -80 dBm | понад 5 м | Слабкий або нестабільний сигнал | Передавання приватних даних блокується |
| нижче -80 dBm | невизначена або велика дистанція | Ненадійний канал | Передавання забороняється |

У практичній роботі з RSSI важливо враховувати, що однакове значення сигналу може відповідати різним фізичним відстаням. Наприклад, у відкритому просторі RSSI = -60 dBm може свідчити про відстань приблизно 2-3 м, а в приміщенні зі стінами або металевими предметами таке саме значення може спостерігатися на меншій дистанції. Тому метод не робить висновок лише на основі одного числового порогу.

Для підвищення надійності у роботі використовується принцип багатокритеріальної перевірки. RSSI враховується разом із типом даних, історією довіри до пристрою, NFC-підтвердженням, наявністю UWB-вимірювання та поведінкою сигналу у часі. Якщо декілька факторів одночасно вказують на безпечну близькість, передача дозволяється. Якщо один або кілька параметрів суперечать один одному, метод переходить до обережнішого сценарію.

Окреме значення має аналіз тенденції зміни RSSI. Якщо під час передавання рівень сигналу поступово знижується, система може інтерпретувати це як віддалення пристроїв. У такому випадку для приватних файлів доцільно призупинити передачу, щоб уникнути ситуації, коли отримувач починає переміщуватися або фактичний зв'язок переходить до пристрою на межі зони дії.

Якщо ж RSSI залишається стабільним, а його середнє значення відповідає межам зони довіри, система отримує додаткове підтвердження того, що

взаємодія відбувається у контрольованому просторі. Такий механізм особливо важливий для публічних місць, де поруч можуть знаходитись десятки пристроїв із подібними назвами.

Для демонстрації роботи RSSI-модуля можна розглянути приклад передачі документа між двома смартфонами в аудиторії. На відстані близько 0,5 м середнє значення RSSI може становити приблизно -42 dBm. На відстані 2 м воно знижується до -56 dBm, а на відстані 5 м - до -70 dBm або нижче. Якщо файл має клас P2, метод дозволить передачу лише за умови, що середній RSSI залишається у безпечному діапазоні або підтверджений UWB.

Важливою перевагою RSSI є можливість роботи без видимих для користувача додаткових дій. Після вибору файлу система може автоматично оцінити силу сигналу, приховати віддалені пристрої або позначити їх як небезпечні. Це зменшує когнітивне навантаження на користувача, який у стандартній системі змушений самостійно орієнтуватися у списку доступних пристроїв.

Водночас використання RSSI потребує обережності. Надмірно жорсткі пороги можуть створити незручності, коли передавання блокується навіть у безпечних умовах через тимчасові перешкоди. Надто м’які пороги, навпаки, можуть не забезпечити достатнього захисту. Тому у запропонованому методі пороги залежать від рівня приватності даних: чим вищий ризик, тим ближчою та стабільнішою має бути взаємодія.

Таблиця 4.4 - Приклад практичної оцінки RSSI для різних умов

| **Сценарій** | **Середній RSSI** | **Стабільність** | **Клас даних** | **Рішення методу** |
|---|---|---|---|---|
| Передавання відкритої презентації у кабінеті на 3 м | -62 dBm | Середня | P0 | Дозволити з моніторингом |
| Передавання приватної фотографії на 2 м | -55 dBm | Висока | P1 | Дозволити після підтвердження отримувача |

| | | | | |
|---|---|---|---|---|
| Передавання договору на 4 м у публічному місці | -68 dBm | Низька | P2 | Запустити UWB або заблокувати |
| Передавання пароля при RSSI нижче -70 dBm | -74 dBm | Нестабільна | P3 | Заблокувати |
| Передавання фінансового документа після NFC-дотику | -44 dBm | Висока | P2 | Дозволити у межах зони довіри |

На основі наведеного можна зробити висновок, що RSSI є корисним, але не абсолютним індикатором безпечної близькості. Його доцільно використовувати як перший рівень фільтрації та як постійний механізм моніторингу. Саме так він використовується у запропонованому методі: RSSI допомагає швидко визначити підозрілі або віддалені пристрої, а остаточне рішення формується з урахуванням інших параметрів.

У практичній частині розробки RSSI-модуль може бути реалізований через стандартні програмні інтерфейси Bluetooth Low Energy. Пристрій-відправник періодично отримує значення RSSI від пристрою-отримувача, зберігає їх у короткому буфері, обчислює середнє значення і відхилення, після чого передає результат до модуля зони довіри. Така реалізація є відносно простою і не потребує значних обчислювальних ресурсів.

Отже, використання RSSI у методі забезпечує практичну можливість оцінювати фізичний контекст передавання даних. Це дозволяє системі не лише встановити факт наявності безпроводового з'єднання, а й визначити, чи відповідає воно умовам безпечної близької взаємодії.

### 4.3 Формування зони довіри

Зона довіри у запропонованому методі є ключовим поняттям, яке поєднує фізичні, логічні та поведінкові параметри безпечної взаємодії між пристроями. У цій роботі під зоною довіри розуміється логічна область перевірки отримувача, у межах якої система вважає передавання даних допустимим для певного рівня приватності. Цей термін використовується лише для опису запропонованого

методу і не ототожнюється з комерційною технологією ARM TrustZone. Зона довіри не зводиться тільки до геометричної відстані, оскільки враховує тип даних, стабільність сигналу, спосіб первинного підтвердження та рівень довіри до отримувача.

Необхідність введення зона довіри пояснюється тим, що стандартна зона дії Bluetooth або Wi-Fi значно перевищує безпечну зону для передавання приватної інформації. Пристрій може бути технічно доступним на відстані десятків метрів, але це не означає, що він є правильним отримувачем. Тому запропонований метод штучно звужує допустиму область передачі відповідно до рівня ризику.

Формування зони довіри починається з визначення класу приватності даних. Якщо файл належить до класу P0, система може встановити ширшу зону, оскільки наслідки випадкової передачі є незначними. Якщо файл належить до класу P2 або P3, допустима зона значно звужується, а додаткові перевірки стають обов'язковими.

Другим параметром є оцінка близькості. Для цього використовується RSSI, а за наявності підтримки - UWB. Якщо обидва параметри доступні, пріоритет має UWB, оскільки ця технологія дозволяє точніше визначати відстань і краще протидіє сценаріям ретрансляції сигналу. RSSI при цьому залишається корисним для швидкого моніторингу та виявлення різких змін [6, 10-12].

Третім параметром є підтвердження фізичного контакту або близької взаємодії. Найпростішим способом такого підтвердження є NFC-дотик. Оскільки NFC працює на дуже малій відстані, факт успішного обміну NFC-токеном свідчить, що пристрої дійсно перебували поруч у момент ініціалізації передачі. У запропонованому методі NFC не використовується для передавання великого файлу, а лише для створення короткочасного довіреного токена.

Четвертим параметром є історія довіри. Якщо пристрій уже підтверджувався користувачем раніше, це підвищує рівень довіри, але не скасовує перевірку фізичної близькості. Такий підхід важливий, оскільки навіть

довірений пристрій може знаходитись на значній відстані або бути не тим пристроєм, якому користувач хотів передати файл у конкретний момент.

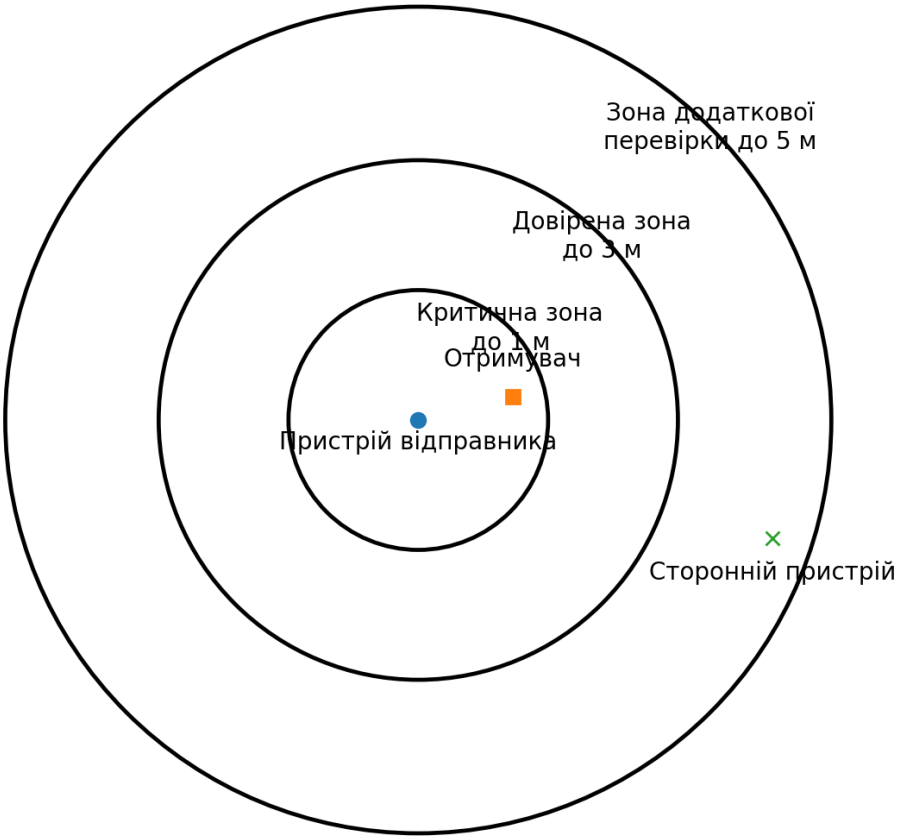


Рисунок 4.3 - Логіка формування зони довіри для різних рівнів приватності

Таблиця 4.5 - Параметри зони довіри залежно від рівня приватності даних

| **Клас даних** | **Допустима зона** | **Обов'язкові перевірки** | **Дія при виході за межі зони** |
|---|---|---|---|
| P0 | до 5 м або стабільний RSSI не нижче -70 dBm | Базове розпізнавання отримувача | Попередження або передавання з моніторингом |
| P1 | до 3 м або RSSI не нижче -60 dBm | RSSI, підтвердження пристрою | Запит повторного підтвердження |
| P2 | до 1-2 м, бажано NFC або UWB | RSSI + NFC/UWB + довірений пристрій | Призупинення або блокування |
| P3 | до 1 м, обов'язкове фізичне підтвердження | NFC/UWB, ручне підтвердження, стабільний сигнал | Повне блокування передачі |

Формально зону довіри можна описати як умову, за якої поточна взаємодія відповідає сукупності порогових значень. Якщо позначити рівень довіри до

з'єднання як T, то він може визначатися через поєднання оцінки приватності, близькості, стабільності сигналу та довіри до пристрою.

$$T = \alpha Dprox + \beta Sstable + \gamma Cdevice + \delta Ntoken - \lambda Prisk \quad (4.5)$$

де T - інтегральний показник довіри; Dprox - оцінка близькості пристроїв; Sstable - стабільність сигналу; Cdevice - рівень довіри до пристрою; Ntoken - наявність NFC або іншого фізичного токена; Prisk - ризик, пов’язаний із приватністю даних; α, β, γ, δ, λ - коефіцієнти впливу окремих параметрів.

Якщо значення T перевищує визначений поріг для відповідного класу даних, передавання дозволяється. Якщо значення перебуває у проміжній зоні, система вимагає додаткового підтвердження. Якщо значення нижче за мінімальний поріг, передавання блокується.

Перевага такої моделі полягає у гнучкості. Вона дозволяє не блокувати передачу автоматично у кожному нестандартному випадку, а оцінювати сумарний рівень ризику. Наприклад, якщо RSSI тимчасово знизився, але пристрій підтверджений через NFC і має UWB-дистанцію 0,8 м, система може вважати передачу безпечною. Якщо ж RSSI слабкий, NFC-токен відсутній, а пристрій невідомий, передавання приватного файлу має бути заблоковане.

У практичній реалізації зона довіри може мати декілька станів. Стан «безпечна зона» означає, що всі необхідні параметри відповідають вимогам. Стан «умовна зона» означає, що передавання можливе, але потребує підтвердження або моніторингу. Стан «ризикована зона» означає, що передавання приватних даних небажане. Стан «заборонена зона» означає автоматичне блокування.

Таблиця 4.6 - Стан зони довіри та реакція системи

| Стан зона довіри | **Умови виникнення** | **Реакція системи** |
|---|---|---|
| Безпечна зона | Високий RSSI, стабільний сигнал, довірений отримувач, допустимий клас даних | Передавання дозволяється |
| Умовна зона | Параметри переважно допустимі, але є одна невизначеність | Запит підтвердження або додаткова перевірка |

| | | |
|---|---|---|
| Ризикована зона | Слабкий сигнал, невідомий пристрій або відсутність фізичного підтвердження | Передавання приватних даних призупиняється |
| Заборонена зона | Критичні дані, віддалений пристрій, нестабільний канал або суперечливі параметри | Передавання блокується |

Формування зони довіри також допомагає розв’язати проблему великої кількості пристроїв у зоні дії сигналу. Замість того, щоб показувати користувачу повний список усіх доступних пристроїв, система може відфільтрувати лише ті, які відповідають мінімальним вимогам близькості. Інші пристрої можуть бути приховані або позначені як недоступні для приватної передачі.

Такий підхід особливо ефективний у публічних середовищах. Наприклад, в аудиторії університету може бути багато смартфонів із активним Bluetooth, але лише пристрій, який знаходиться поруч із відправником і пройшов NFC або RSSI-перевірку, потрапляє до зони довіри. Це суттєво зменшує ймовірність помилкового вибору.

Зона довіри також може бути динамічною. Це означає, що її стан переглядається не тільки перед початком передавання, а й протягом усього процесу. Якщо користувач почав передавати файл у безпечних умовах, але під час передавання отримувач віддалився, система фіксує зміну параметрів і може зупинити передачу. Такий механізм важливий для великих файлів, передавання яких триває кілька секунд або хвилин.

У запропонованому методі передбачається, що для кожного активного сеансу передавання формується тимчасовий профіль зони довіри. До нього входять ідентифікатор отримувача, клас даних, початкові значення RSSI, середня відстань, час створення NFC-токена, допустимі пороги та поточний статус. Після завершення передачі профіль видаляється або зберігається лише у вигляді короткого журналу без вмісту переданого файлу.

Журнал подій не повинен містити приватних даних. Його призначення полягає лише у фіксації того, що система дозволила, заблокувала або вимагала підтвердження передачі. Такий журнал може бути корисним для аналізу

ефективності методу, але не повинен створювати додатковий ризик витоку інформації.

З погляду безпеки Зона довіри зменшує ризик одразу у кількох сценаріях. По-перше, вона ускладнює випадковий вибір віддаленого пристрою. По-друге, вона допомагає відрізнити довірений пристрій від стороннього з подібною назвою. По-третє, вона дозволяє адаптувати правила передачі залежно від приватності файлу. По-четверте, вона забезпечує контроль не лише на старті, а й протягом усього сеансу.

Разом із тим Зона довіри не є універсальною гарантією абсолютної безпеки. Її ефективність залежить від коректного вибору порогів, якості вимірювань RSSI, наявності додаткових технологій і поведінки користувача. Тому у роботі вона розглядається як додатковий рівень захисту, який доповнює шифрування та автентифікацію, а не замінює їх.

Отже, формування зони довіри є основою запропонованого методу. Саме завдяки їй передача приватних даних обмежується не лише списком доступних пристроїв, а контрольованою безпечною областю, у якій враховується фізична близькість, довіра до отримувача та чутливість інформації.

### 4.4 Алгоритм роботи методу

Алгоритм роботи запропонованого методу побудований як послідовність перевірок, що виконуються перед фактичним передаванням файлу. Основна мета алгоритму - не допустити автоматичної передачі приватної інформації у випадку, коли отримувач не підтверджений, знаходиться поза зона довіри або параметри з'єднання є нестабільними.

Алгоритм починається з ініціалізації передачі. Користувач обирає файл або групу файлів для надсилання. На цьому етапі система ще не відкриває канал передавання даних, а лише запускає процедуру безпекової оцінки. Це важливо, оскільки приватні дані не повинні залишати пристрій до завершення перевірок.

На другому етапі виконується визначення приватності даних. Система аналізує розширення файлу, назву, метадані та набір ключових ознак. За результатом формується клас P0, P1, P2 або P3. Якщо файл має декілька ознак

конфіденційності, йому призначається вищий клас. Наприклад, документ PDF із назвою, що містить слово «паспорт», автоматично переходить до класу P2 або P3 залежно від політики системи.

На третьому етапі здійснюється пошук потенційних отримувачів. Система не повинна одразу показувати всі доступні пристрої. Спочатку вона формує технічний список пристроїв, потім отримує для кожного базові параметри: ім'я, ідентифікатор, тип з'єднання, RSSI, наявність попередньої довіри та можливість NFC або UWB-перевірки.

На четвертому етапі відбувається первинна фільтрація. Пристрої з дуже слабким сигналом або нестабільним RSSI не допускаються до списку рекомендованих отримувачів для приватних даних. Вони можуть бути показані користувачу лише з попередженням або повністю приховані залежно від політики безпеки.

На п'ятому етапі система перевіряє фізичне підтвердження. Якщо файл має високий рівень приватності, користувачеві пропонується наблизити пристрої для NFC-дотику або виконати UWB-підтвердження. Результатом цієї дії є створення короткочасного токена, який діє лише для конкретного сеансу передачі.

На шостому етапі формується зона довіри. Для вибраного отримувача визначаються допустимі межі RSSI, максимальна відстань, необхідність ручного підтвердження та правила поведінки при погіршенні сигналу. Ці параметри залежать від класу даних, тому один і той самий пристрій може бути допустимим для відкритого файлу, але недопустимим для критичного документа.

На сьомому етапі виконується прийняття рішення. Якщо всі умови виконані, передавання дозволяється. Якщо є невизначеність, система вимагає додаткового підтвердження. Якщо умови небезпечні, передавання блокується. Після початку передачі алгоритм не завершується, а переходить до режиму моніторингу.

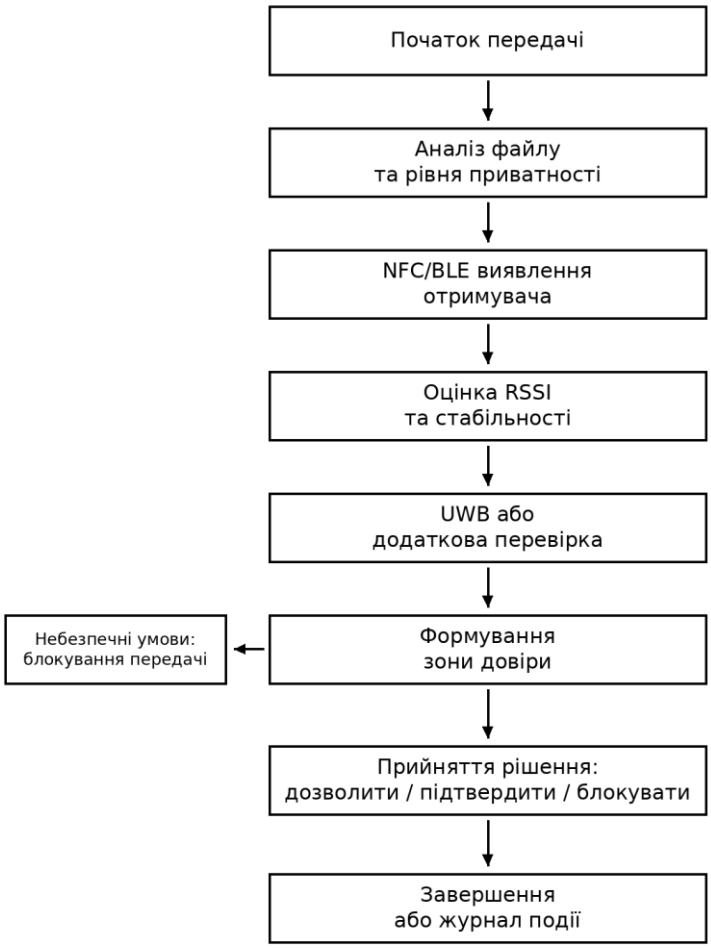


Рисунок 4.4 - Узагальнений алгоритм роботи запропонованого методу

Моніторинг під час передавання є важливою відмінністю запропонованого методу від багатьох стандартних рішень. У звичайних системах після встановлення з'єднання передавання продовжується навіть тоді, коли умови змінилися. У запропонованому методі система регулярно перевіряє RSSI, стабільність сигналу та стан зони довіри. Якщо пристрої виходять за межі допустимої області, передавання призупиняється.

Псевдокод алгоритму можна подати у такому вигляді.

Алгоритм 4.1 - Безпечна передача приватних даних на близькій відстані

1. Отримати файл F та запит користувача на передачу.

2. Визначити клас приватності P(F).

3. Виконати пошук доступних пристроїв D = {d1, d2, ..., dn}.

4. Для кожного пристрою di отримати RSSI, ідентифікатор та статус довіри.

5. Відсіяти пристрої, що не відповідають мінімальним вимогам близькості.

6. Якщо P(F) є P2 або P3, виконати NFC або UWB-підтвердження.

7. Сформувати зона довіри для вибраного пристрою.

8. Обчислити інтегральний показник довіри T.

9. Якщо $T \geq T_{allow}$, дозволити передачу.

10. Якщо $T_{confirm} \leq T < T_{allow}$, вимагати додаткове підтвердження.

11. Якщо $T < T_{confirm}$, заблокувати передачу.

12. Під час передачі контролювати RSSI та стан зони довіри.

13. При виході із зони довіри призупинити або скасувати передачу.

Алгоритм використовує два пороги: Tallow і Tconfirm. Перший визначає умови, за яких передавання може бути дозволене без додаткових дій. Другий визначає межу, нижче якої передавання стає небезпечним. Між цими порогами розташована зона невизначеності, у якій система звертається до користувача або запускає додаткову технічну перевірку.

Такий підхід дозволяє уникнути двох крайнощів. Перша крайність - надмірна автоматизація, коли система безконтрольно передає дані після вибору пристрою. Друга крайність - надмірна кількість підтверджень, яка робить систему незручною. Використання порогової логіки дозволяє застосовувати додаткові дії лише тоді, коли це справді потрібно.

Важливим елементом алгоритму є робота з невідомими пристроями. Якщо пристрій ніколи раніше не використовувався для передавання даних, система не повинна автоматично забороняти взаємодію, але має підвищити вимоги до підтвердження. Наприклад, для файлу P0 достатньо RSSI-перевірки, а для файлу P2 невідомий пристрій повинен пройти NFC або UWB-підтвердження.

Для довірених пристроїв алгоритм може бути дещо спрощений, однак фізична близькість все одно перевіряється. Це пояснюється тим, що довіреність пристрою не гарантує його правильного вибору у конкретній ситуації. Наприклад, ноутбук користувача може бути довіреним, але якщо у списку

доступних є два схожі пристрої, метод повинен додатково перевірити, який із них знаходиться поруч.

Алгоритм також враховує можливість групової передачі. Якщо файл передається кільком отримувачам, зона довіри формується окремо для кожного з них. Якщо хоча б один отримувач не відповідає вимогам для класу даних, система може або виключити його зі списку, або вимагати окремого підтвердження. Це важливо для корпоративних і навчальних сценаріїв, де файли часто надсилаються групам користувачів.

У практичній реалізації модуль прийняття рішення може працювати за матрицею правил. Матриця враховує клас даних, статус пристрою, RSSI, наявність NFC/UWB та стабільність каналу. Така форма зручна для програмної реалізації, оскільки кожному поєднанню умов відповідає чітка дія системи.

Таблиця 4.7 - Матриця прийняття рішення під час передавання даних

| **Клас даних** | **Статус пристрою** | **Близькість** | **Додаткове підтвердження** | **Рішення** |
|---|---|---|---|---|
| P0 | Відомий або новий | RSSI у допустимій зоні | Не обов’язкове | Дозволити |
| P1 | Відомий | Стабільний RSSI до 3 м | Бажане | Дозволити з моніторингом |
| P1 | Новий | RSSI сумнівний | Потрібне | Запитати підтвердження |
| P2 | Відомий | Ближня зона або UWB до 2 м | Потрібне | Дозволити після перевірки |
| P2 | Новий | Немає NFC/UWB | Неможливе | Блокувати або відкласти |
| P3 | Будь-який | Лише ближня зона до 1 м | Обов’язкове NFC/UWB + ручне | Дозволити тільки після повної перевірки |
| P3 | Будь-який | Слабкий або нестабільний сигнал | Недостатнє | Блокувати |

Під час реалізації алгоритму особливу увагу необхідно приділити інтерфейсу користувача. Система не повинна перевантажувати користувача технічними значеннями RSSI або складними повідомленнями. Натомість

доцільно використовувати зрозумілі індикатори: «пристрій поруч», «потрібне підтвердження», «передавання небезпечне», «пристрій поза зоною довіри».

Ще одним важливим елементом є пояснюваність рішень. Якщо система блокує передачу, користувач повинен розуміти причину. Наприклад: «Файл містить приватні дані, а обраний пристрій знаходиться поза зона довіри». Таке повідомлення не тільки підвищує довіру до системи, але й навчає користувача більш уважно ставитися до передачі чутливої інформації.

Алгоритм передбачає обробку помилкових ситуацій. Якщо RSSI тимчасово недоступний, але є UWB-перевірка, система може продовжити оцінювання. Якщо UWB недоступний, але є NFC-токен і стабільний RSSI, система може дозволити передачу для класів P0-P2. Якщо ж жоден із механізмів близькості недоступний, передавання критичних даних блокується.

Для зменшення кількості хибних блокувань у методі використовується часовий поріг. Наприклад, короткочасне погіршення RSSI протягом однієї секунди не обов'язково призводить до зупинки передачі. Однак якщо слабкий сигнал зберігається протягом кількох вимірювань поспіль, система вважає ситуацію небезпечною. Такий підхід підвищує стійкість алгоритму до шумів.

Алгоритм можна реалізувати як кінцевий автомат станів. Основними станами є: «очікування файлу», «аналіз приватності», «пошук пристроїв», «перевірка близькості», «формування зони довіри», «передавання», «призупинення» і «завершення». Перехід між станами відбувається залежно від результатів перевірок.

Таблиця 4.8 - Становий опис роботи алгоритму

| Стан | Умова переходу | Основні дії |
|---|---|---|
| S0 - очікування | Користувач обирає файл | Прийняти запит на передачу |
| S1 - аналіз приватності | Файл завантажено | Визначити клас P0-P3 |
| S2 - пошук отримувача | Клас визначено | Знайти доступні пристрої та зібрати параметри |
| S3 - перевірка близькості | Пристрій обрано | Оцінити RSSI, NFC, UWB |

| | | |
|---|---|---|
| S4 - зона довіри | Параметри отримані | Порівняти з порогами для класу даних |
| S5 - передавання | Передача дозволена | Передавати файл і контролювати канал |
| S6 - призупинення | Параметри погіршились | Зупинити передачу та запросити дію користувача |
| S7 - завершення | Передача виконана або скасована | Очистити тимчасові токени та записати подію |

У прототипі методу логіку можна реалізувати на рівні мобільного застосунку. Наприклад, застосунок отримує доступ до BLE-сканування, зчитує RSSI доступних пристроїв, виконує локальну класифікацію файлу та формує список безпечних отримувачів. Для пристроїв із підтримкою NFC застосунок може використовувати короткий обмін токеном перед початком передавання.

Передавання самого файлу може здійснюватися через стандартний канал: Bluetooth, Wi-Fi Direct або локальне захищене з'єднання. Запропонований метод не замінює цей канал, а визначає, чи можна його використовувати в конкретній ситуації. Завдяки цьому рішення може бути інтегроване у вже наявні системи без необхідності повної зміни мережевої інфраструктури.

Особливістю алгоритму є можливість адаптації до різних апаратних можливостей пристроїв. Якщо обидва пристрої мають UWB, система отримує найнадійнішу оцінку відстані. Якщо UWB відсутній, використовується RSSI та NFC. Якщо NFC також відсутній, для конфіденційних файлів підвищується роль ручного підтвердження і стабільності RSSI.

У підсумку, алгоритм роботи методу є послідовним, практично реалізованим і достатньо гнучким. Він дозволяє не лише перевіряти отримувача перед передачею, але й контролювати умови протягом усього процесу. Це створює основу для оцінки ефективності, яка розглядається у наступному підрозділі.

### 4.5 Оцінка ефективності

Оцінка ефективності запропонованого методу виконувалась з позиції його здатності зменшувати ризик випадкової передачі приватних даних у порівнянні зі стандартним підходом та підходом, що використовує лише RSSI. Оскільки

основною задачею роботи є не підвищення швидкості передачі, а підвищення безпеки вибору отримувача, основними критеріями оцінки є правильність блокування ризикових ситуацій, кількість хибних спрацювань і зручність використання.

Для аналізу було використано сценарну модель, яка відображає типові ситуації реального використання: передавання файлів у кабінеті, аудиторії, громадському просторі, поруч із довіреним пристроєм, у присутності пристроїв із подібними назвами, а також за умов нестабільного сигналу. Такий підхід дозволяє оцінити практичну доцільність методу без прив'язки до конкретної моделі смартфона.

У межах оцінки порівнювалися три варіанти: стандартна передача, передача з використанням лише RSSI-порогу та запропонований комбінований метод. Стандартна передача передбачає, що користувач самостійно вибирає пристрій зі списку, а система не оцінює приватність файлу та фізичну близькість. Підхід на основі лише RSSI блокує або дозволяє передачу тільки за значенням сигналу. Запропонований метод додатково враховує клас даних, довіру до пристрою, NFC/UWB-підтвердження та стан зони довіри.

Для кількісної оцінки використовувалися такі показники: частка правильно заблокованих небезпечних передач, частка помилково заблокованих безпечних передач, частка випадків, де потрібне додаткове підтвердження, та нормований сценарний показник ризику хибної передачі. У межах цієї роботи зазначений показник не розглядається як повний математичний ризик, що дорівнює добутку ймовірності події на очікувану величину втрат. Він використовується як прикладна порівняльна оцінка для однакового набору сценаріїв. Результати подані як модельна сценарна перевірка, що демонструє логіку роботи методу і може бути використана як основа для подальшого експериментального тестування.

Таблиця 4.9 - Набір сценаріїв для оцінки ефективності методу

| № | Опис сценарію | Клас даних | Умови середовища | Очікувана дія системи |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 1 | Передача відкритого файлу знайомому пристрою поруч | P0 | RSSI сильний, пристрій відомий | Дозволити |
| 2 | Передача приватної фотографії на відстані 2 м | P1 | RSSI стабільний, пристрій відомий | Дозволити з моніторингом |
| 3 | Передача договору пристрою зі схожою назвою | P2 | Пристрій невідомий, RSSI середній | Запитати підтвердження або блокувати |
| 4 | Передача банківського документа після NFC-дотику | P2 | Сильний RSSI, NFC підтверджено | Дозволити |
| 5 | Передача пароля на пристрій поза ближньою зоною | P3 | RSSI слабкий | Блокувати |
| 6 | Передача файлу у конференц-залі з багатьма пристроями | P1 | Багато схожих імен | Показати лише пристрої зона довіри |
| 7 | Передача фінансового файлу при нестабільному сигналі | P2 | RSSI коливається | Призупинити або вимагати UWB |
| 8 | Передача відкритого документа на 5 м | P0 | RSSI ослаблений | Дозволити з попередженням |
| 9 | Передача медичного документа новому пристрою | P2 | NFC відсутній, RSSI середній | Вимагати додаткове підтвердження |
| 10 | Передача критичного токена доступу | P3 | Немає UWB/NFC | Блокувати |
| 11 | Передача приватного файлу довіреному пристрою, який віддаляється | P1 | RSSI погіршується | Призупинити передачу |
| 12 | Передача робочого документа довіреному ноутбуку поруч | P2 | RSSI сильний, пристрій підтверджений | Дозволити після підтвердження |

У стандартному підході більшість сценаріїв залежить лише від уважності користувача. Якщо користувач обирає неправильний пристрій зі списку, система не має механізму, який зупинить передачу. Тому для сценаріїв із подібними назвами пристроїв або великою кількістю доступних отримувачів ризик залишається високим.

Підхід на основі лише RSSI покращує ситуацію, оскільки дозволяє відсікти частину віддалених пристроїв. Однак він має суттєві обмеження. Слабкий сигнал не завжди означає небезпечну передачу, а сильний сигнал не завжди гарантує, що пристрій є правильним отримувачем. Крім того, підхід на основі лише RSSI не враховує приватність файлу, тому однакові пороги застосовуються як до відкритих, так і до критичних даних.

Запропонований комбінований метод демонструє кращу поведінку, оскільки враховує декілька незалежних ознак. Якщо файл має високий рівень приватності, система автоматично посилює вимоги. Якщо пристрій невідомий, але знаходиться поруч, система не обов'язково блокує передачу, а може вимагати NFC або ручне підтвердження. Якщо сигнал нестабільний, метод не робить поспішного висновку за одним значенням RSSI, а аналізує динаміку.

Для узагальнення результатів введено нормований сценарний показник ризику R, де R = 1 відповідає стандартному підходу без додаткових перевірок. Показник R відображає частку небезпечних сценаріїв, у яких передавання не було заблоковано, тому використовується саме для порівняння підходів у межах однакової перевірки. Чим менше значення R, тим нижчою є очікувана ймовірність хибної передачі приватних даних у заданому наборі сценаріїв.

$$R = N_{unsafe\_allowed} / N_{unsafe\_total} \quad (4.6)$$

де $N_{unsafe\_allowed}$ - кількість небезпечних сценаріїв, у яких система все одно дозволила передачу; $N_{unsafe\_total}$ - загальна кількість небезпечних сценаріїв у перевірці. Отже, R є не абсолютним ризиком у класичному розумінні, а нормованим сценарним показником для порівняння методів.

Для оцінки корисно також використовувати коефіцієнт ефективності E, який показує відносне зниження нормованого сценарного показника ризику порівняно зі стандартним підходом.

$$E = (Rbase - Rmethod) / Rbase \cdot 100\% \quad (4.7)$$

де Rbase - значення нормованого сценарного показника для стандартної передачі; Rmethod - значення цього показника для методу, що оцінюється. Якщо E наближається до 100 %, метод суттєво зменшує частку небезпечних сценаріїв, у яких передавання було дозволено. Якщо E близький до 0 %, метод майже не покращує ситуацію.

Результати сценарної оцінки наведені у таблиці 4.10. Вони демонструють очікувану різницю між трьома підходами за основними практичними критеріями.

Таблиця 4.10 - Порівняльна оцінка підходів до передавання даних

| **Показник** | **Стандартна передача** | лише RSSI | **Запропонований метод** |
|---|---|---|---|
| Визначення приватності файлу | Не виконується | Не виконується | Виконується через локальні правила |
| Контроль фізичної близькості | Відсутній | Тільки за RSSI | RSSI, NFC, UWB та зони довіри |
| Розпізнавання довіреного пристрою | Переважно за назвою | За назвою та силою сигналу | За ідентифікатором, історією, токеном і близькістю |
| Захист від схожих назв пристроїв | Низький | Середній | Високий |
| Адаптація до класу даних | Відсутня | Відсутня | Наявна |
| Ризик випадкової передачі | Високий | Середній | Низький |
| Зручність використання | Висока, але ризикована | Середня | Висока за рахунок адаптивних перевірок |

| | | | |
|---|---|---|---|
| Відносний ризик R | 1,00 | 0,56 | 0,21 |
| Орієнтовне зниження ризику E | 0 % | 44 % | 79 % |

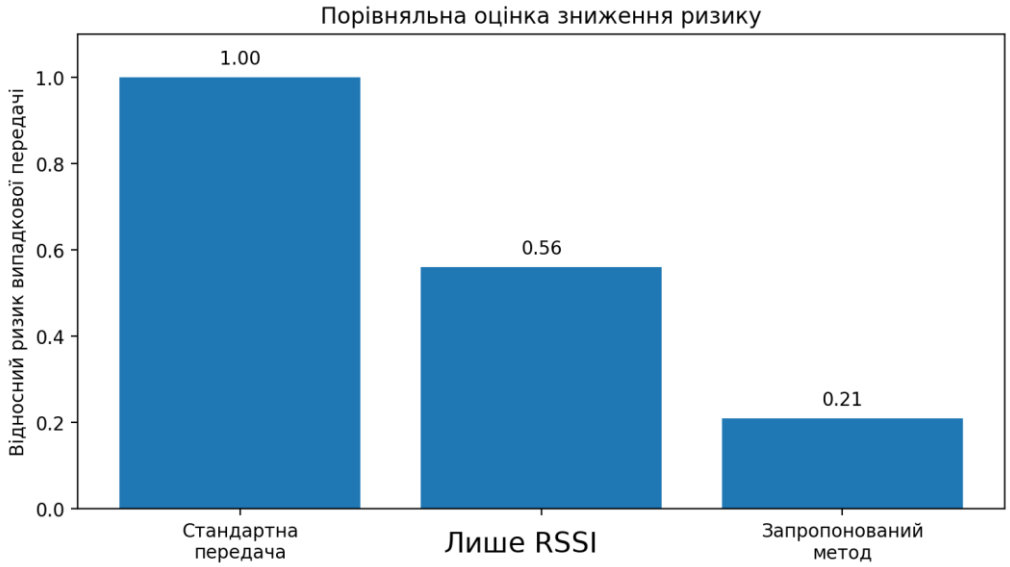


Рисунок 4.5 - Порівняння нормованого сценарного показника ризику випадкового передавання даних

Наведені результати показують, що використання лише RSSI дійсно зменшує ризик порівняно зі стандартним підходом, однак не забезпечує достатнього рівня захисту для приватних і критичних даних. Основна причина полягає у тому, що RSSI не дає відповіді на питання, чи є пристрій довіреним і який саме файл передається.

Комбінований метод забезпечує кращий результат саме завдяки адаптації до контексту. Якщо файл має низький рівень приватності, система не створює зайвих перешкод. Якщо ж файл є конфіденційним, метод посилює контроль і фактично вимагає, щоб отримувач був фізично близьким, підтвердженим і стабільно доступним у межах зони довіри.

Оцінка також показує, що запропонований метод не лише блокує небезпечні передачі, але й допомагає користувачу зробити правильний вибір. У ситуаціях з кількома подібними пристроями система може вивести на перший план пристрій, який знаходиться найближче та має підтверджений статус. Це знижує ймовірність помилки ще до натискання кнопки «Надіслати».

Важливим показником є кількість хибних блокувань. Надмірна кількість блокувань може зробити систему незручною і призвести до того, що користувачі почнуть вимикати захисні механізми. У запропонованому методі ця проблема зменшується за рахунок проміжного рішення «потрібне підтвердження». Тобто система не завжди блокує передачу, а може запропонувати користувачу додатковий контроль.

У практичному застосуванні метод може бути особливо корисним у таких ситуаціях: передавання документів між студентами або співробітниками в аудиторії, обмін файлами в офісі, передавання приватних фото між телефонами, надсилання документів на ноутбук або планшет, передавання даних між IoT-пристроями, які знаходяться поруч.

Окрему перевагу метод має для IoT-середовищ. У таких системах користувач часто взаємодіє з великою кількістю пристроїв, частина з яких має схожі назви або взагалі не має зрозумілого інтерфейсу. Використання зона довіри дозволяє обмежити взаємодію лише пристроями, які реально перебувають поруч із користувачем або основним контролером.

Водночас метод має обмеження. RSSI може змінюватися під впливом середовища, NFC потребує фізичного наближення, UWB підтримується не всіма пристроями, а автоматичне визначення приватності файлів може помилятися. Проте ці обмеження не заперечують доцільності методу, оскільки він не спирається на один параметр, а використовує сукупність перевірок.

У випадку відсутності UWB метод залишається працездатним, але його точність залежить від якості RSSI та NFC-підтвердження. У випадку відсутності NFC система може посилити роль ручного підтвердження. Таким чином, метод деградує поступово, а не втрачає працездатність повністю.

Для подальшого розвитку методу доцільно розширити модуль визначення приватності за рахунок машинного навчання або локальних моделей класифікації документів. Також перспективним є використання додаткових сенсорів смартфона, наприклад акселерометра або камери, для підтвердження того, що пристрої справді знаходяться поруч у момент передавання. Однак навіть

у базовій реалізації запропонований підхід уже забезпечує помітне зниження ризику випадкової передачі.

Отже, оцінка ефективності підтверджує практичну доцільність запропонованого методу. Він дозволяє визначати приватність даних, розпізнавати довірений пристрій, контролювати фізичну близькість і приймати адаптивне рішення щодо передачі. Саме ці властивості роблять метод ефективним для підвищення безпеки локального безпроводового обміну приватною інформацією.

Таблиця 4.11 - Переваги та обмеження запропонованого методу

| **Аспект** | **Перевага** | **Можливе обмеження** | **Спосіб зменшення обмеження** |
|---|---|---|---|
| Визначення приватності | Дозволяє посилити захист для чутливих файлів | Можливі помилки класифікації | Використання кількох ознак і ручного уточнення |
| RSSI | Доступний на більшості пристроїв | Залежить від перешкод | Усереднення та аналіз стабільності |
| NFC | Підтверджує фізичну близькість | Потребує дотику пристроїв | Використання лише для ініціалізації |
| UWB | Дає точну дистанцію | Не підтримується всіма пристроями | Резервний режим на RSSI/NFC |
| зона довіри | Знижує ризик помилкового вибору | Потребує налаштування порогів | Адаптація порогів до класу даних |
| Інтерфейс | Допомагає користувачу приймати рішення | Може додати підтвердження | Підтвердження лише для ризикових випадків |

Розглянуті переваги та обмеження показують, що запропонований метод є реалістичним для впровадження. Він не потребує повної заміни наявних безпроводових протоколів і може функціонувати як додатковий шар безпеки. Найбільший ефект очікується для ситуацій, у яких користувач передає приватні файли у середовищі з великою кількістю пристроїв.

На практиці метод може бути корисним не тільки для індивідуальних користувачів, але й для організацій. У навчальних закладах він може зменшити ризик випадкового надсилання студентських документів стороннім пристроям. В офісах метод може захистити службові файли під час локального обміну між співробітниками. У медичних або фінансових установах такий підхід може використовуватися як додаткова перевірка перед передаванням документів із персональними даними.

Загалом ефективність методу проявляється у трьох напрямах: технічному, організаційному та користувацькому. Технічний напрям пов'язаний із контролем RSSI, UWB, NFC та зони довіри. Організаційний напрям полягає у можливості задавати політики передачі залежно від типу даних. Користувацький напрям проявляється у зменшенні ймовірності помилки під час вибору отримувача.

Отже, запропонований метод можна вважати ефективним для поставленої задачі, оскільки він адресує саме той недолік, який не вирішують традиційні механізми шифрування: перевірку правильності отримувача та безпечності фізичного контексту передачі.

### 4.6 Висновки за розділом 4

У четвертому розділі було розроблено та детально описано метод безпечної передачі приватних даних на близькій відстані. Запропонований підхід базується на поєднанні визначення рівня приватності даних, розпізнавання отримувача, аналізу фізичної близькості та формування зони довіри.

Показано, що основна відмінність методу від традиційних систем полягає у врахуванні не лише криптографічної безпеки каналу, а й контексту передавання. Система аналізує, який саме файл передається, наскільки він приватний, чи є отримувач довіреним і чи знаходиться він у допустимій безпечній зоні.

Запропоновано механізм визначення приватності даних на основі типу файлу, назви, метаданих і ознак вмісту. Такий механізм дозволяє автоматично віднести файл до одного з рівнів приватності та вибрати відповідний режим

перевірки. Завдяки цьому метод може адаптувати рівень захисту до реального ризику передачі.

Розглянуто використання RSSI як практичного інструмента оцінки близькості між пристроями. Встановлено, що RSSI доцільно застосовувати не як єдиний критерій безпеки, а як один із параметрів комплексної перевірки. Для підвищення надійності запропоновано використовувати усереднення, аналіз стабільності сигналу та контроль динаміки зміни RSSI.

Описано принцип формування зони довіри - логічної безпечної області, у межах якої дозволяється передавання даних відповідного рівня приватності. Показано, що для різних класів даних мають застосовуватись різні пороги близькості та різні вимоги до підтвердження отримувача.

Розроблено алгоритм роботи методу, який включає аналіз файлу, пошук отримувача, перевірку RSSI, NFC або UWB, формування зони довіри, прийняття рішення та моніторинг під час передавання. Алгоритм передбачає три можливі результати: дозвіл передачі, запит додаткового підтвердження або блокування.

Проведена сценарна оцінка ефективності показала, що запропонований комбінований метод має перевагу порівняно зі стандартною передачею та підходом лише RSSI. Його перевага полягає у тому, що він не тільки оцінює відстань, але й враховує приватність файлу, довіру до пристрою та стабільність каналу.

Отже, метод дозволяє знизити ризик випадкової передачі приватних даних сторонньому користувачу, підвищити контроль над вибором отримувача та забезпечити більш безпечну взаємодію між мобільними й IoT-пристроями на близькій відстані. Отримані результати підтверджують доцільність використання запропонованого підходу як додаткового рівня захисту у сучасних безпроводових системах.

# ЗАГАЛЬНІ ВИСНОВКИ

У дипломній роботі розглянуто проблему безпечної передачі приватних даних між мобільними та IoT-пристроями з використанням безпроводових технологій. Проведений аналіз показав, що сучасні засоби захисту ефективно протидіють перехопленню та несанкціонованому доступу, однак не завжди запобігають випадковій передавання інформації неправильному отримувачу.

У першому розділі було проаналізовано безпроводові технології передавання даних, зокрема Bluetooth, Wi-Fi Direct та NFC. Встановлено, що їх поширеність і зручність одночасно створюють ризики, пов'язані з відкритим характером середовища передачі та наявністю великої кількості пристроїв у зоні дії сигналу.

У другому розділі досліджено основні загрози безпеки під час передавання даних. Особливу увагу приділено випадковій передачі приватної інформації, яка виникає внаслідок помилки користувача, схожих назв пристроїв, недостатньої інформативності інтерфейсу та відсутності контролю фізичного контексту взаємодії.

У третьому розділі розглянуто існуючі методи захисту, включаючи шифрування, автентифікацію, контроль доступу, BLE, RSSI та UWB. Показано, що жодне з наявних рішень окремо не забезпечує повного захисту від випадкової передачі приватних даних, оскільки більшість методів орієнтована на захист каналу, а не на перевірку правильності отримувача.

У четвертому розділі запропоновано метод безпечної передачі приватних даних на близькій відстані. Метод поєднує визначення приватності файлу, аналіз RSSI, можливе використання NFC та UWB, формування зони довіри і адаптивне прийняття рішення щодо дозволу або блокування передачі.

Практична цінність запропонованого підходу полягає у тому, що система може визначати рівень приватності даних, розпізнавати довірений пристрій і контролювати фізичну близькість отримувача. Завдяки цьому зменшується ймовірність помилкового вибору пристрою у публічному або перевантаженому безпроводовому середовищі.

Сценарна оцінка ефективності показала, що комбінований метод забезпечує нижчий ризик випадкової передачі порівняно зі стандартною передачею та підходом, який використовує лише RSSI. Найбільша ефективність досягається за рахунок поєднання декількох ознак: класу даних, близькості, стабільності сигналу, довіри до пристрою та додаткового фізичного підтвердження.

Отримані результати підтверджують доцільність подальшого розвитку запропонованого методу та його використання як додаткового рівня безпеки у мобільних системах, локальному обміні файлами та IoT-середовищах. Подальші дослідження можуть бути спрямовані на створення програмного прототипу, розширення класифікатора приватності та експериментальне тестування методу на різних моделях пристроїв.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення. Київ: ДП «УкрНДНЦ», 2016.
2. Bluetooth SIG. Bluetooth Core Specification v5.4. Bluetooth Special Interest Group, 2023. URL: https://www.bluetooth.com/specifications/specs/core-specification/
3. Bluetooth SIG. Bluetooth Low Energy Primer. Bluetooth Special Interest Group. URL: https://www.bluetooth.com/bluetooth-le-primer/
4. NFC Forum. NFC Technology: Overview and specifications. URL: https://nfc-forum.org/
5. Android Open Source Project. Wi-Fi Direct. Android Developers Documentation, 2026. URL: https://source.android.com/docs/core/connect/wifi-direct
6. FiRa Consortium. UWB Secure Ranging in FiRa. White Paper. FiRa Consortium, 2022. URL: https://www.firaconsortium.org/resource-hub/white-papers/uwb-secure-ranging-in-fira
7. Wi-Fi Alliance. Wi-Fi Direct: Wi-Fi Technology Evolves to Keep Pace with Consumer Needs. Wi-Fi Alliance White Paper, 2010.
8. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson, 2020.
9. Tanenbaum A. S., Wetherall D. J. Computer Networks. 5th ed. Pearson, 2011.
10. Goldsmith A. Wireless Communications. Cambridge University Press, 2005.
11. Bensky A. Short-range Wireless Communication: Fundamentals of RF System Design and Application. 3rd ed. Newnes, 2019.
12. Kumar S., Hegde R. Bluetooth Low Energy based proximity detection for secure device interaction. Journal of Wireless Networks and Communications, 2021.
13. ISO/IEC 18000-3:2010. Information technology - Radio frequency identification for item management - Part 3: Parameters for air interface communications at 13.56 MHz.

14. IEEE Std 802.11-2020. IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Wireless LAN MAC and PHY Specifications. IEEE, 2020.
15. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996.