ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:
«Антенний комплекс для виявлення слабких радіовипромінювань на базі SDR-радіоприймача»

на здобуття освітнього ступеня магістра

зі спеціальності __125 - Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Георгій ЧУПРІН

Виконав: здобувач вищої освіти групи СЗДМ-61

_____ЧУПРІН Георгій_____

Керівник: _____ПЕПА Юрій_____
(ПРІЗВИЩЕ, Ім’я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім’я)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ЧУПРІНУ Георгію Владиславовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Антенний комплекс для виявлення слабких радіовипромінювань на базі SDR-радіоприймача».
Керівник кваліфікаційної роботи: ПЕПА Юрій, к.т.н., доцент.
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

Затверджена наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи: 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи:
Способи витоку інформації через радіоканал в ефір.
Радіомоніторинг і антенні системи.
Оцінка застосування дискоконусної антени.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Провести аналіз технічних засобів для моніторингу радіоефіру.
2. Аналіз методів в способів розпізнавання небезпечних сигналів на фоні завад в ефірі.
3. Моделювання і розрахунок параметрів дискоконусної антени.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах

6. Дата видачі завдання 15.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз літературних джерел		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Георгій ЧУПРІН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Юрій ПЕПА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра містить: 75 стор., 5 рис., 4 табл., 19 джерел.

Мета роботи – підвищення ефективності виявлення та локалізації сучасних радіозакладних пристроїв, що використовують методи приховування інформації (LPI, FHSS, пакетна передача) шляхом розробки комплексної методики застосування програмно-визначеного радіо (SDR) та спеціалізованих антенних систем.

Об'єкт дослідження – процес технічного захисту інформації від витоку електромагнітними каналами зв'язку в умовах використання зловмисниками сучасних телекомунікаційних технологій.

Предмет дослідження – методи та апаратно-програмні засоби радіомоніторингу на базі SDR-приймачів.

Короткий зміст роботи: в роботі проведено аналіз еволюції засобів негласного отримання інформації, досліджено вразливості сучасних мереж, розроблено математичну модель радіозакладки на базі автогенератора Колпітца, обґрунтовано та розраховано параметри пошукового комплексу, розроблено практичні рекомендації щодо налаштування аналізатора спектра TinySA Ultra для виявлення сигналів з низькою ймовірністю перехоплення.

Апробація:

Є.В. Шарай, Г.В. Чупрін, НЕБЕЗПЕЧНІ РАДІОВИПРОМІНЮВАННЯ ТЕХНІЧНИХ ЗАСОБІВ ОБРОБКИ ІНФОРМАЦІ. *Всеукраїнської науково-практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.53-54. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

КЛЮЧОВІ СЛОВА: технічний захист інформації, SDR, радіоприймач, радіомоніторинг, радіозакладка, антена, пошуковий комплекс.

ABSTRACT

The text part of the qualification work for obtaining a master's degree contains: 75 pages, 5 pictures, 4 tables, 19 sources.

The purpose of the work – to increase the efficiency of detection and localization of modern radio embedded devices that select information reception methods (LPI, FHSS, packet transmission) by developing a comprehensive methodology for using software-defined radio (SDR) and specialized antenna systems.

Object of research – the process of technical protection of information from leakage via electromagnetic communication channels in the context of the use of modern telecommunication technologies by attackers.

Subject of research – methods and hardware and software for radio monitoring based on SDR receivers.

Summary of the work: the work analyzes the evolution of means of covert information acquisition, investigates the vulnerabilities of modern networks, develops a mathematical model of radio beacons based on the Kolpitz oscillator, justifies and calculates the parameters of the search complex, and develops practical recommendations for configuring the TinySA Ultra spectrum analyzer to detect signals with a low probability of interception.

KEYWORDS: technical protection of information, SDR, radio receiver, radio monitoring, radio beacon, antenna, search complex.

ЗМІСТ

ВСТУП

Сучасний етап розвитку інформаційного суспільства характеризується безпрецедентною інтеграцією бездротових технологій у всі сфери життя та діяльності. Стрімке розгортання мереж мобільного зв’язку нових поколінь (4G/5G), масове використання пристроїв Інтернету речей (IoT) та доступність програмно-визначених радіосистем (SDR) докорінно змінили електромагнітну обстановку. Радіоефір став не лише насиченим, але й складним для контролю, що створює сприятливе середовище для несанкціонованого отримання інформації.

Паралельно з розвитком легальних технологій відбувається якісна трансформація засобів технічної розвідки. Традиційні аналогові радіозакладки («жучки»), що працюють на фіксованих частотах і легко виявляються простими індикаторами поля, відходять у минуле. На їх місце приходять інтелектуальні цифрові пристрої, реалізовані на базі SDR-архітектури. Такі засоби здатні використовувати складні методи маскування: псевдовипадкове перелаштування робочої частоти (FHSS), пакетну передачу даних надкороткої тривалості (Burst Transmission) та шумоподібні сигнали з низькою ймовірністю перехоплення (LPI).

Проблема полягає у тому, що класичні методики пошуку та наявний парк пошукового обладнання (сканери, частотоміри, нелінійні локатори) часто виявляються неефективними проти новітніх загроз. Сигнал сучасної закладки може маскуватися під легітимний трафік Wi-Fi, ховатися в шумах або з’являтися в ефірі лише на частки секунди. Це вимагає перегляду підходів до технічного захисту інформації та впровадження нових інструментів радіомоніторингу, здатних проводити глибокий спектральний аналіз у реальному часі.

У цьому контексті особливої важливості набуває розробка доступних та ефективних пошукових комплексів на базі SDR-приймачів (наприклад, TinySA) та спеціалізованих антенних систем. Такий підхід дозволяє не лише візуалізувати

спектр для виявлення аномалій, але й адаптувати параметри пошуку під конкретні

типи сигналів, що робить тему кваліфікаційної роботи своєчасною та практично значущою для сфери інформаційної безпеки.

РОЗДІЛ 1
АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ СКЛАДНИХ РАДІОСИГНАЛІВ

Програмно-визначене радіо, більш відоме у світі як SDR (Software-Defined Radio), являє собою одну з найбільш значущих та фундаментальних революцій у сфері телекомунікацій та радіоелектроніки за останні десятиліття, фактично знаменуючи собою перехід від ери «заліза» до ери алгоритмів та математики. Якщо спробувати осягнути цю технологію максимально глобально, то SDR — це радіосистема, де компоненти, які традиційно були реалізовані апаратно (змішувачі частот, фільтри, модулятори, демодулятори, детектори), замінені програмним забезпеченням, що працює на персональному комп'ютері, вбудованій системі або цифровій логіці. Це докорінно змінює саму філософію радіозв'язку: якщо класичний супергетеродинний приймач є жорстко спеціалізованим пристроєм, спроєктованим інженерами для виконання конкретного завдання у вузькому діапазоні частот і з фіксованим типом модуляції, то SDR приймач є універсальним «комбайном», чиї можливості обмежуються лише фізичними параметрами вхідного тракту та потужністю обчислювального ядра, а не спаяними на платі компонентами.

1.1. Концептуальні засади та архітектура програмно-визначеного радіо (SDR)

У серці архітектури будь-якого SDR приймача лежить принцип максимально ранньої цифровізації сигналу, що є ключовою відмінністю від аналогових попередників. Процес починається з антени, яка вловлює електромагнітні коливання з ефіру, після чого слабкий сигнал потрапляє у вхідний аналоговий тракт, що зазвичай складається з малошумного підсилювача (LNA) для підняття рівня сигналу над шумами та, можливо, вхідних смугових фільтрів для захисту від перевантаження потужними позасмуговими перешкодами. Однак, на відміну від

класичного радіо, де сигнал далі проходить через каскади аналогових перетворень, у SDR він прямує до найважливішого елемента системи — аналогово-цифрового перетворювача (АЦП). Саме АЦП виконує перетворення неперервної синусоїдальної напруги, що надходить з антени, у нескінченний потік цифрових даних, що складається з нулів та одиниць. Цей процес називається дискретизацією або семплюванням, і його якість визначається частотою дискретизації (яка впливає на те, наскільки широку смугу радіоефіру приймач може «бачити» одночасно) та розрядністю (яка визначає динамічний діапазон, тобто здатність чути дуже слабкі сигнали поруч із дуже потужними). Після проходження через АЦП радіохвиля перестає бути фізичним явищем електричного струму і стає масивом математичних даних, готовим до обробки.

Отриманий цифровий потік зазвичай формується у вигляді так званих квадратурних сигналів, відомих як I (In-phase) та Q (Quadrature). Це поняття є критично важливим для розуміння глибини технології SDR, оскільки саме I/Q дані містять абсолютно повну інформацію про сигнал — не лише його амплітуду, але й фазу, що дозволяє програмному забезпеченню згодом реконструювати будь-який вид модуляції. Цей потік даних передається далі по швидкісному інтерфейсу, наприклад USB або Ethernet, до обчислювального блоку, яким може виступати центральний процесор звичайного комп'ютера, спеціалізований цифровий сигнальний процесор (DSP) або програмована логічна інтегральна схема (FPGA). Саме тут відбувається справжня обробка, яка раніше вимагала шаф з обладнанням. Процесор застосовує складні математичні алгоритми, такі як Швидке Перетворення Фур'є (FFT), для аналізу спектра, цифрову фільтрацію для виділення корисного сигналу з шуму, та демодуляцію. Оскільки всі ці процеси є віртуальними, користувач може змінювати ширину фільтра, тип модуляції (AM, FM, SSB, CW, цифрові види) чи частоту налаштування просто кліком миші, без необхідності брати в руки паяльник чи змінювати кварцові резонатори.

Однією з найбільш вражаючих візуальних особливостей роботи з SDR є можливість спостерігати за радіоефіром за допомогою «водоспаду» (waterfall display). Це графічне представлення спектра, де по горизонталі відкладена частота,

по вертикалі — час, а колір позначає інтенсивність сигналу. Це дозволяє оператору миттєво оцінити обстановку в широкій смузі частот, побачити появу нових станцій, ідентифікувати тип сигналу за його візуальним «почерком» та налаштуватися на нього з хірургічною точністю. Така візуалізація перетворює «сліпий» пошук станцій, характерний для старих аналогових приймачів, на повноцінний радіомоніторинг, де ви бачите все, що відбувається в ефірі, ще до того, як почуєте звук.

Спектр застосування SDR технології є надзвичайно широким і виходить далеко за межі звичайного прослуховування радіопередач. Завдяки своїй універсальності, один і той самий недорогий пристрій, наприклад, популярний RTL-SDR (який, до речі, розпочав еру доступного SDR, будучи спочатку простим телевізійним тюнером), може використовуватися для прослуховування радіоаматорів, моніторингу переговорів авіадиспетчерів та пілотів, декодування сигналів морських суден (AIS) для відображення їх на карті в реальному часі, прийому телеметрії та зображень з метеорологічних супутників, аналізу сигналів автомобільних ключів та датчиків розумного будинку, і навіть для експериментів з радіоастрономією. У професійній сфері SDR використовується військовими для створення захищених адаптивних систем зв'язку, мобільними операторами для тестування мереж 5G, та спецслужбами для радіорозвідки та аналізу загроз. Технологія SDR фактично демократизувала радіоефір, надавши будь-кому з комп'ютером можливість досліджувати невидимий світ електромагнітних хвиль з рівнем інструментарію, який ще двадцять років тому був доступний лише науковим інститутам та військовим лабораторіям.

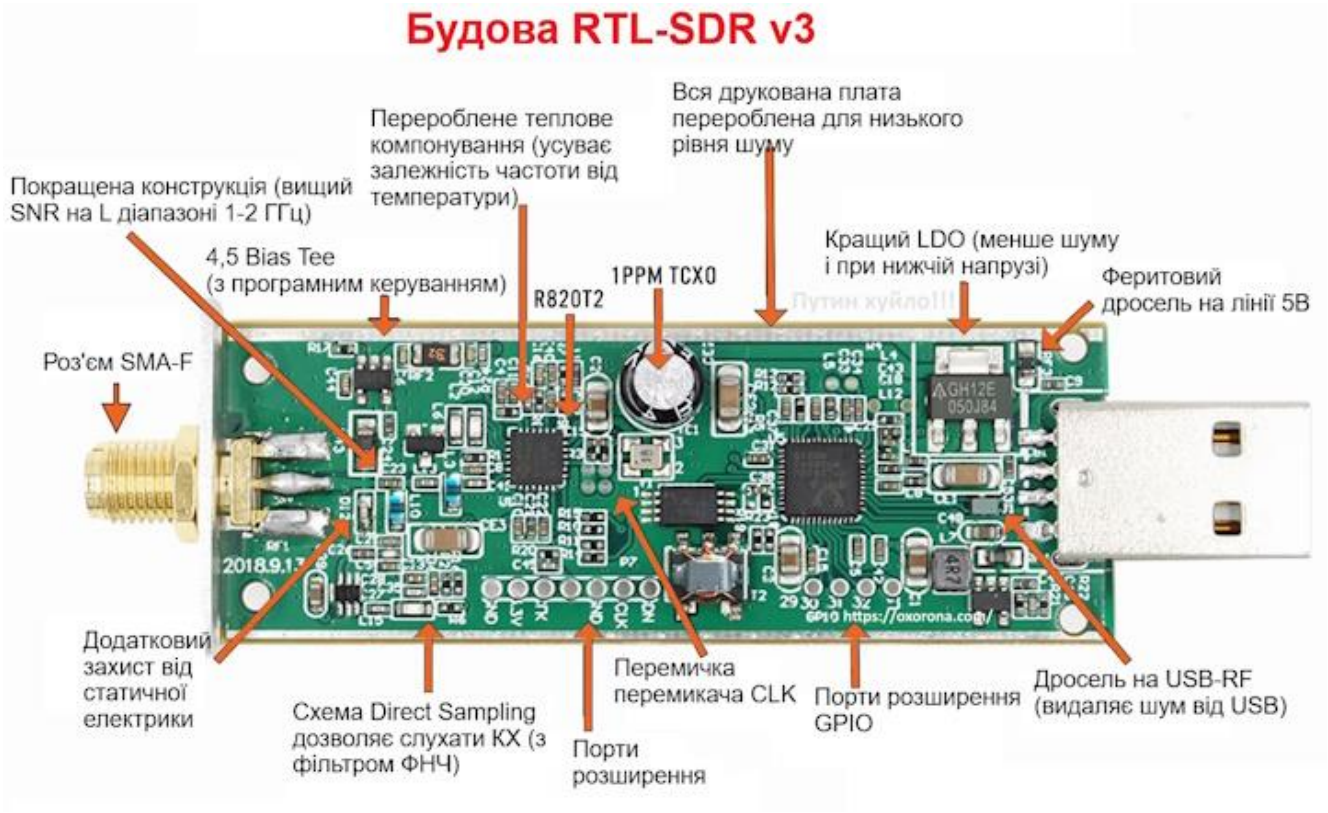

Рис. 1.1 – Один з прикладів будови SDR-радіоприймача

У світі технічного захисту інформації (ТЗІ) поняття «небезпеки» радіозакладного пристрою (так званого «жучка») вимірюється не його потужністю чи розміром, а передусім складністю його виявлення та здатністю передавати інформацію непомітно для стандартних пошукових комплексів. Найбільшу загрозу становлять пристрої, що використовують методи маскування сигналу, працюють у нестандартних діапазонах або використовують легальні протоколи зв'язку.

1.2 Технології скритної передачі даних (LPI/LPD), аналіз загроз

Burst Transmission (або у сленгу радіорозвідки — "Squirt"), становить фундаментальний інтерес як об'єкт науково-технічного дослідження. Цей клас систем, що виник як відповідь на еволюцію засобів радіопеленгації (DF — Direction Finding) в середині XX століття, сьогодні трансформувався у складні програмно-апаратні комплекси, що інтегрують принципи теорії інформації, криптографії, стеганографії та фізики поширення радіохвиль.

Сутність методу полягає у часовій компресії інформаційного потоку. Повідомлення, яке при використанні традиційних методів (наприклад, ручної маніпуляції ключем Морзе) займало б у ефірі хвилини, попередньо записується на буферний носій, кодується та передається за частки секунди або декілька секунд. Така стратегія має на меті мінімізацію "часового вікна вразливості" (window of vulnerability), протягом якого джерело випромінювання може бути виявлене, ідентифіковане та локалізоване засобами радіоелектронної розвідки (SIGINT) супротивника.

Актуальність даного дослідження зумовлена не лише історичним значенням технології у контексті "Холодної війни", але й її ренесансом у сучасних кіберфізичних системах. Принципи burst-передачі сьогодні імплементуються у протоколах Інтернету речей (IoT), системах супутникового зв'язку з низькою ймовірністю перехоплення (LPI/LPD), а також у складних апаратних імплантах (hardware implants) для ексфільтрації даних з ізольованих мереж (air-gapped networks).

У цьому звіті буде проведено вичерпний аналіз фізичних основ, схемотехнічних рішень, алгоритмів модуляції та методів протидії, що стосуються технології пакетної передачі даних, з акцентом на інженерну деталізацію та оперативно-тактичні аспекти застосування.

Інженерна задача створення burst-передавача зводиться до пошуку балансу між скритністю у часовій області та скритністю у спектральній області. Надмірно короткий імпульс стає широкосмуговим шумоподібним сигналом, який, хоч і важко демодулювати без знання коду, легко детектується як енергетична аномалія спектральними аналізаторами реального часу.

На відміну від потокової передачі, де синхронізація може встановлюватися поступово, burst-системи вимагають миттєвої синхронізації приймача та передавача. Структура пакету, або "Burst Profile", є критично важливою для успішного декодування.

Типова архітектура пакету включає наступні елементи:

- Преамбула (Preamble): Послідовність бітів з високою автокореляційною функцією (наприклад, послідовності Баркера або М-послідовності). Вона необхідна для того, щоб демодулятор приймача міг здійснити "захват" частоти та фази (Carrier Recovery & Symbol Timing Recovery) за мінімальний час. У системі WSA-6 використовувалася 55-бітна преамбула.

- Унікальне слово (Unique Word / Start Frame Delimiter): Маркер початку корисних даних.

- Заголовок (Header): Містить метадані: довжину повідомлення, тип кодування, ідентифікатор адресата, параметри модуляції. Це дозволяє реалізувати адаптивні схеми, де параметри змінюються від пакету до пакету.

- Корисне навантаження (Payload): Власне зашифрована інформація.

- Мідамбула (Midamble): У довгих пакетах вставляється в середину для повторної оцінки каналу (channel estimation) та компенсації ефектів завмирання або доплерівського зсуву.

- FCS/CRC (Frame Check Sequence): Циклічний надлишковий код для перевірки цілісності.

- Захисний інтервал (Guard Time): Часовий проміжок для запобігання накладанню пакетів через багатопроменеве поширення (multipath propagation).

Специфікою каналів burst-передачі є виникнення так званих пакетних помилок (burst errors), коли внаслідок імпульсної завади або короткочасного завмирання пошкоджується ціла послідовність бітів, а не окремі ізольовані символи. Стандартні коди корекції (наприклад, прості коди Геммінга) неефективні проти таких помилок.

Для вирішення цієї проблеми застосовуються:

Циклічні коди (Cyclic Codes): Математично описуються як поліноми над полем Галуа. Вони здатні виявляти та виправляти пакети помилок певної довжини, якщо поліном-генератор підібраний відповідним чином. Теоретично доведено, що циклічні коди є оптимальними для виявлення пакетних помилок, оскільки їх здатність до виявлення обмежена лише ступенем полінома.

Перемішування (Interleaving): Техніка, при якій біти повідомлення переставляються за певним алгоритмом перед передачею. Якщо у каналі виникає пакетна помилка, що знищує групу сусідніх бітів, то після де-інтерлівінгу на приймачі ці помилки "розподіляються" по всьому повідомленню, перетворюючись на поодинокі помилки, з якими легко справляються алгоритми FEC (Forward Error Correction), такі як коди Ріда-Соломона або згорткові коди.

Сучасні burst-передавачі є програмно-визначеними радіосистемами (SDR), де параметри модуляції та кодування можуть змінюватися динамічно.

Для забезпечення низької ймовірності перехоплення (LPI) та високої енергоефективності застосовуються специфічні види модуляції.

AQ-DBPSK (Alternating Quadrature Differential Binary Phase Shift Keying): Цей метод є розвитком класичної DBPSK. Він дозволяє зменшити варіації огинаючої сигналу, що підвищує ефективність підсилювача потужності (можливість роботи у класі C або E) та економить заряд батареї автономного пристрою. Крім того, AQ-DBPSK демонструє високу стійкість до доплерівського зсуву частоти, що критично для зв'язку з рухомими об'єктами або супутниками.

Розширення спектру (Spread Spectrum):

DSSS (Direct Sequence Spread Spectrum): Інформаційний сигнал множиться на високошвидкісну псевдовипадкову послідовність. Це "розмазує" енергію сигналу у широкій смузі, роблячи його спектральну густину нижчою за рівень теплового шуму. Для стороннього спостерігача такий сигнал виглядає як незначне підвищення рівня шуму.

FHSS (Frequency Hopping Spread Spectrum): Передавач змінює частоту несучої сотні або тисячі разів на секунду за псевдовипадковим законом. Це ускладнює не лише перехоплення, але й створення прицільних завад (jamming).

Гідроакустичні burst-системи та біомімікрія

У підводному середовищі, де радіохвилі швидко загасають, використовуються акустичні хвилі. Тут технологія burst-передачі набула форми біомімікрії.

Імітація біологічних звуків: Сучасні акустичні модеми можуть формувати сигнали, що за часо-частотною структурою нагадують клацання креветок-лускунів або вокалізацію дельфінів. Оскільки океан наповнений такими звуками, короткий пакет даних, замаскований під біологічний імпульс, ігнорується автоматизованими системами спостереження як природний шум.

Chaotic DSSS: Використання хаотичних послідовностей дозволяє боротися з ефектом багатопроменевого поширення (реверберацією), який є основною проблемою гідроакустики.

Сучасна реалізація burst-передавача часто базується на архітектурі FPGA (Field-Programmable Gate Array) та SDR.

Приклад реалізації.

У роботі описано систему на базі GNU Radio та Python, яка пакетує дані у формат AX.25 і передає їх короткими серіями.

Noise-Shaped Signaling: Пропонується метод формування сигналу, який статистично ідентичний адитивному білому гауссовому шуму (AWGN). Використовуючи SDR, передавач модифікує I/Q компоненти сигналу таким чином, щоб сузір'я (constellation) виглядало як хаотична хмара точок ("dirty constellation"), і лише приймач, що знає ключ перетворення, може відновити дані.

З розвитком же цифрових мереж концепція burst-передачі мігрувала з радіоефіру у дротові мережі та комп'ютерні інтерфейси. Витік каталогу NSA ANT (Advanced Network Technology) у 2013 році надав унікальну можливість проаналізувати ці технології.

Тоді стало відомо про Апаратні імпланти (Hardware Implants):

COTTONMOUTH (USB-імплант): Цей пристрій, замаскований під звичайний USB-роз'єм, містить мініатюрний трансівер. Він створює прихований бездротовий міст (wireless bridge) до мережі зловмисника. Передача даних здійснюється короткими пакетами (bursts), щоб уникнути виявлення системами моніторингу спектру, які можуть бути встановлені в захищеному приміщенні.

IRONCHEF (BIOS/SMM-імплант): Програмно-апаратний комплекс, що інфікує BIOS/UEFI цільового сервера. Він використовує двосторонній радіозв'язок

для комунікації з апаратним "жучком". Особливістю є те, що передача ініціюється рідко і триває мікросекунди, що робить її виявлення вкрай складним без постійного моніторингу.

RF-ретрорефлектори (VAGRANT, PHOTOANGLO): Це пасивні пристрої, що не мають власного радіопередавача. Вони модулюють відбитий сигнал від зовнішнього радара (опромінювача). Це дозволяє передавати дані без енерговитрат і без активного випромінювання, яке міг би засікти звичайний детектор поля.
Також тоді ж здобули популярності Приховані канали (Covert Channels) у мережевих протоколах.

У мережах TCP/IP та IoT burst-передача реалізується через маніпуляцію службовими полями або таймінгом пакетів.

Timing Channels: інформація кодується у інтервалах між пакетами. Зловмисник відправляє легітимні пакети, але затримка між ними несе приховані біти. Це виглядає як звичайний мережевий джиттер (jitter).

Storage Channels у MQTT: протокол MQTT, широко використовуваний в IoT, має поля змінної довжини. Дослідження демонструють можливість створення прихованого каналу шляхом маніпуляції полем довжини повідомлення, що дозволяє передавати дані непомітно для стандартних брандмауерів.

1.3 Теоретичні основи виявлення сигналів з розширеним спектром

Одним з основних методів виявлення сигналів з розширеним спектром є пристрої з псевдовипадковим перелаштуванням робочої частоти (FHSS).

Технологія розширення спектра методом псевдовипадкового перелаштування робочої частоти (FHSS — Frequency Hopping Spread Spectrum) спочатку розроблялася для військового зв'язку, щоб уникнути глушіння та перехоплення, і по суті є мАетодом передачі радіосигналів, при якому носійна частота періодично змінюється (здійснює «стрибки») в межах широкої смуги частот відповідно до псевдовипадкової послідовності, відомої лише передавачу та авторизованому приймачу. На відміну від систем з фіксованою частотою, де вся енергія сигналу зосереджена у вузькій смузі протягом усього сеансу зв'язку,

системи FHSS розподіляють енергію у часі та частоті. У будь-який конкретний момент часу (dwell time) сигнал займає вузьку смугу, але протягом тривалого інтервалу спектр сигналу виглядає як широкосмуговий шум. Ця особливість забезпечує ключові переваги технології: високу завадостійкість (anti-jamming), низьку ймовірність перехоплення (LPI — Low Probability of Intercept) та можливість спільного використання спектра різними користувачами (CDMA — Code Division Multiple Access).

Історичний розвиток FHSS є прикладом переходу від електромеханічних рішень до повністю цифрових алгоритмів. Фундаментальна ідея була запатентована у 1942 році актрисою Геді Ламар (Гедвіга Кіслер) та композитором Джорджем Антейлом (Патент США № 2,292,387 «Secret Communication System»). Їхня пропозиція стосувалася системи захисту радіокерування торпедами від глушіння. Інновація полягала у використанні пари синхронізованих паперових стрічок з перфорацією, аналогічних тим, що використовувалися у механічних піанолах, для керування частотою передавача та приймача. Система передбачала використання 88 частотних каналів (відповідає кількості клавіш фортепіано). Хоча патент не був реалізований під час Другої світової війни через технологічні обмеження, він заклав концептуальну основу для майбутніх розробок.

Практична реалізація стала можливою лише з розвитком твердотільної електроніки та цифрових синтезаторів частоти у 1950-60-х роках. Поява транзисторів дозволила створити компактні генератори псевдовипадкових кодів (PRNG), які замінили механічні стрічки, а розвиток технологій фазового автопідлаштування частоти (PLL) забезпечив необхідну швидкість та точність перемикання каналів. Сучасні системи, такі як SINCGARS та Link 16, базуються на складних цифрових алгоритмах шифрування та високошвидкісних синтезаторах, здатних здійснювати десятки тисяч стрибків на секунду.

Аналіз ефективності систем FHSS базується на теорії інформації та статистичній радіофізиці. Ключовими показниками є коефіцієнт розширення спектра (Processing Gain) та запас завадостійкості (Jamming Margin), які визначають здатність системи функціонувати в умовах навмисних завад.

Коефіцієнт розширення спектра G_p є мірою переваги, яку отримує приймач за рахунок використання смуги частот, що значно перевищує мінімально необхідну для передачі інформації. У системах FHSS цей коефіцієнт визначається не тривалістю біта, як у системах прямого розширення (DSSS), а кількістю доступних частотних каналів у сітці стрибків.

Формально G_p можна виразити як відношення повної смуги частот системи W_{ss} до смуги частот інформаційного каналу B_{Ch}

$$G_p = \frac{W_{ss}}{B_{ch}} = N,$$

де N — кількість ортогональних частотних каналів. У логарифмічному масштабі (децибелах):

$$G_p(dB) = 10log_{10}N.$$

Варто зазначити, що на відміну від DSSS, де G_p досягається за рахунок когерентного накопичення енергії чіпів, у FHSS виграш реалізується через *ухилення* від завад (interference avoidance). Приймач FHSS "слухає" лише вузьку смугу B_{Ch} у конкретний момент часу, відфільтровуючи шуми та завади, що знаходяться в інших частинах спектра W_{ss}

Запас завадостійкості M_jє критичним параметром для військових систем, оскільки він визначає максимальне відношення потужності завади до потужності сигналу J/S, при якому система здатна забезпечити задану якість зв'язку.

$$M_j(dB) = G_p - \left[\left(\frac{E_b}{N_0}\right)_{req} + L_{sys}\right],$$

де

$\left(\frac{E_b}{N_0}\right)_{req}$ – це необхідне відношення енергії біта до спектральної щільності шуму для заданого методу модуляції та кодування; А L_{sys} – є сукупними системними

витратами (втрати в синхронізації, недосконаліть фільтрації, втрати через апаратуру, тощо).

Аналіз показує, що для ефективного придушення системи FHSS постановник завад повинен або розподілити свою потужність по всій смузі W_{ss} (що знижує спектральну щільність завади в кожному каналі в N разів), або намагатися вгадати поточну частоту. Якщо постановник завад використовує вузькосмугову заваду великої потужності, вона вражає лише один або декілька каналів. Завдяки механізму стрибків, система FHSS перебуватиме на ураженій частоті лише частку часу 1/N, що призводить до незначного зростання середнього BER, яке легко компенсується кодами корекції помилок (FEC).

Таблиця 1.1 – Реакція систем FHSS та DSSS на типові сценарії радіоелектронної боротьби

Тип завади (Jamming Scenario)	Механізм впливу на FHSS	Кількісна оцінка деградації (FHSS)	Порівняння з DSSS	Стратегія захисту FHSS
Вузькосмугова (Narrowband)	Ураження окремих каналів. Вплив лише при збігу частот.	Низька: зростання BER ~5%.[13]	Висока деградація (BER +40%), якщо завада в смузі сигналу.	Виключення уражених каналів (Adaptive FH), FEC.
Тональна (Tone Jamming)	Схожа на вузькосмугову, енергія зосереджена на одній частоті.	Мінімальна.	Значна (BER +25%).[13]	Інтерлівінг (Interleaving) розмазує пакет помилок.

Тип завади (Jamming Scenario)	Механізм впливу на FHSS	Кількісна оцінка деградації (FHSS)	Порівняння з DSSS	Стратегія захисту FHSS
Імпульсна (Pulsed Jamming)	Короткі потужні імпульси. Небезпечна при синхронізації з hop rate.	Середня: BER +20%.[13]	Висока (BER +35%), перевантаження АРП приймача.	Асинхронність стрибків, швидке перелаштування (Fast Hopping).
Частково-смугова (Partial-band)	Завада перекриває частину спектра W_{ss}	Помірна: BER +10-20% пропорційно перекриттю.[13]	Залежить від перекриття основної пелюстки спектра.	Використання широкого Hopset, рознесення частот.
Слідкувальна (Follower Jammer)	Детектування частоти та швидка перестройка завади.	Критична, якщо $T_{react} < T_{dwell}$	Не застосовується (DSSS не змінює частоту).	Зменшення часу перебування на частоті T_{dwell}, Fast FH (>1000 hops/s).

З таблиці видно, що FHSS демонструє значно вищу стійкість до зосереджених за спектром завад порівняно з DSSS, але є потенційно вразливою до "розумних" слідкувальних завад, якщо швидкість перелаштування недостатньо висока.

Загалом ефективність FHSS залежить від фізичної реалізації синтезатора частот, який повинен забезпечувати швидке перемикання (settling time), спектральну чистоту та фазову стабільність.

Традиційні системи (наприклад, ранні версії SINCGARS) використовували синтезатори на основі петлі фазового автопідлаштування (PLL).

- Принцип роботи: PLL складається з генератора, керованого напругою (VCO), дільника частоти, фазового детектора та фільтра петлі. Вихідна частота F_{out}= N * F_{ref} стабілізується шляхом зворотного зв'язку.

- Проблема часу встановлення (Settling Time): Головним обмеженням PLL є інерційність. Для зміни частоти петлі потрібен час для перехідного процесу, який обернено пропорційний смузі пропускання фільтра петлі. Для швидкого перемикання потрібна широка смуга, але це погіршує фазовий шум і рівень побічних складових (spurs).

- Обмеження: Для систем типу GSM час встановлення має бути < 577 мкс. Для швидких систем FHSS (Link 16) класичні PLL занадто повільні. Використовують архітектури "Ping-Pong" (два синтезатори працюють по черзі) або методи попереднього встановлення напруги VCO (pre-steering).

Прямий цифровий синтез (DDS).

Сучасні високошвидкісні системи переходять на технологію прямого цифрового синтезу (DDS).

- Принцип роботи: DDS генерує форму хвилі цифровим способом. Акумулятор фази накопичує значення з кожним тактовим імпульсом, які перетворюються на амплітуду через таблицю (Look-Up Table) і подаються на цифро-аналоговий перетворювач (DAC).

Переваги:

- Швидкість: Час перемикання обмежений лише затримкою цифрової логіки і складає наносекунди, що дозволяє реалізувати Fast FHSS.

- Неперервність фази: DDS дозволяє змінювати частоту без розриву фази (Continuous Phase), що критично для спектральної ефективності та зменшення позасмугових випромінювань.

- Точність: Роздільна здатність по частоті може досягати мілігерц.

Генерація псевдовипадкових послідовностей (PRNG).

"Серцем" системи FHSS є генератор псевдовипадкових чисел, який визначає патерн стрибків (hopping pattern).

Вимоги: Послідовність повинна мати довгий період повторення, рівномірний розподіл по спектру та бути криптографічно стійкою (непередбачуваною для ворога).

Реалізація: Використовуються нелінійні регістри зсуву зі зворотним зв'язком (NLFSR) або криптографічні алгоритми (наприклад, AES у режимі лічильника) в сучасних SDR. У військових системах алгоритм генерації залежить від змінного ключа (TRANSEC variable) та точного часу доби (Time of Day - TOD), що робить патерн унікальним для кожного моменту часу.

Синхронізація є найскладнішим аспектом експлуатації FHSS. Для успішної демодуляції приймач повинен знати не тільки послідовність частот, але й точний час перемикання з точністю до мікросекунд.

Етапи та методи синхронізації.

Процес синхронізації зазвичай включає кілька етапів:

Пошук та виявлення (Acquisition): Приймач, не знаючи точного часу передавача, сканує ймовірні частоти або слухає виділений канал управління (CUE channel / Control Channel). Передавач може відправляти спеціальну преамбулу синхронізації на фіксованій частоті або циклічно по всьому набору частот.

Захоплення часу (Timing Lock): Після детектування преамбули приймач підлаштовує свій локальний годинник під час мережі. Використовуються корелятори та петлі стеження за затримкою (DLL).

Підтримка (Tracking): Компенсація дрейфу кварцових генераторів та ефекту Доплера (актуально для авіації) під час сеансу зв'язку.

Процедура "Late Entry" (Пізнє входження).

У тактичних умовах радіостанції часто вимикаються або виходять із зони дії. Процедура "Late Entry" дозволяє станції приєднатися до активної мережі FHSS без повторної ініціалізації всієї мережі.

Механізм: Активні вузли періодично передають інформацію про час мережі (Network Time) та стан лічильника стрибків у складі заголовків пакетів або

службових повідомлень. Станція, що входить у мережу, використовує спеціальний режим пошуку (наприклад, сканування підмножини частот), щоб "зловити" цей сигнал і синхронізувати свій внутрішній час (TOD) з часом мережі.

Алгоритм: Якщо локальний час відрізняється від мережевого в межах певного вікна (наприклад, ±1 хвилина), корелятор приймача зможе знайти пік кореляції, зсуваючи локальну копію коду. Якщо відхилення значне, потрібен "холодний старт" (Cold Start) через отримання часу від майстра мережі (Net Control Station - NCS) через CUE-канал (фіксована частота виклику).

Роль GPS та автономна синхронізація.

Сучасні системи (Link 16, SINCGARS ASIP) активно використовують GPS для отримання єдиного точного часу (Universal Time Coordinated - UTC). Це значно спрощує синхронізацію, оскільки всі вузли вже мають спільну шкалу часу. Однак, в умовах РЕБ (глушіння GPS), системи повинні переходити на внутрішні високостабільні генератори (Rubidium або термостатовані кварцові OCXO) та використовувати протоколи взаємної синхронізації (Round-Trip Timing), де вузли обмінюються пакетами для вимірювання затримок і корекції годинників.

Розглянемо технічні характеристики та особливості функціонування трьох основних стандартів НАТО, які демонструють різні підходи до реалізації FHSS.

SINCGARS (Single Channel Ground and Airborne Radio System).

SINCGARS є основним стандартом тактичного УКХ-зв'язку (VHF-FM) армії США та багатьох країн-партнерів.

Частотний план: Діапазон 30 – 87.975 МГц із кроком сітки 25 кГц, що забезпечує 2320 дискретних каналів.

Режим стрибків (Hop Rate): Система використовує повільне перелаштування (Slow Frequency Hopping) зі швидкістю приблизно 100 стрибків на секунду. Це означає, що час перебування на одній частоті T_{dwell} становить близько 10 мс. За цей час передається значна кількість бітів інформації (голос або дані).

Захист та керування: Для роботи в режимі FHSS радіостанція повинна мати завантажені:

1. Hopset: Набір дозволених частот. Оператор може виключити частоти, що створюють завади цивільним службам або уражені РЕБ (Lockout frequencies).

2. TRANSEC: змінна (ключ) для генерації псевдовипадкової послідовності.

3. Net ID: ідентифікатор мережі, що визначає зсув у послідовності стрибків, дозволяючи кільком мережам працювати на одному Hopset без колізій (ортогональність).

4. Sync Time: час синхронізації (від NCS або GPS).

5. Модифікації (SIP/ASIP): вдосконалені версії (System Improvement Program) додали потужні алгоритми корекції помилок (Forward Error Correction - FEC) на основі кодів Ріда-Соломона, що дозволяє відновлювати втрачені пакети навіть при сильному частково-смуговому глушінні, а також покращили передачу даних до 16 кбіт/с.

Link 16 (TADIL-J).

Link 16 — це високошвидкісна система обміну тактичними даними, що використовується авіацією, флотом та ППО.

Діапазон: 960 – 1215 МГц (L-діапазон), спільно з авіаційними навігаційними системами (TACAN, DME).

Архітектура сигналу (Fast Hopping): На відміну від SINCGARS, Link 16 використовує швидке перелаштування (Fast Frequency Hopping). Швидкість становить 76 923 стрибків на секунду (тривалість імпульсу 13 мкс, один стрибок на імпульс). Використовується 51 частотний канал з розносом 3 МГц.

Стійкість до РЕБ: Надзвичайно висока швидкість стрибків робить Link 16 практично невразливою до *слідкувальних джамерів* (Follower Jammers). Джамер просто не встигає детестувати частоту, обробити сигнал і випромінити заваду до того, як Link 16 перейде на нову частоту.

Модуляція та кодування: Використовується комбінація DSSS та FHSS. Кожен 5-бітний символ даних кодується 32-чіповою послідовністю (CCSK — Cyclic Code Shift Keying), а потім модулюється методом MSK (Minimum Shift Keying). Це забезпечує додатковий процесинг-гейн.

Часовий поділ (TDMA): Робота мережі жорстко синхронізована в часі. Доба ділиться на епохи (112.5 хв), кадри (12 с) і тайм-слоти (7.8125 мс). Кожен слот містить захисні інтервали (Jitter) для запобігання передбачуваності часу передачі.

Таблиця 1.2 – Порівняльна таблиця характеристик військових систем

Характеристика	SINCGARS	HAVE QUICK II	Link 16 (JTIDS/MIDS)	Racal Jaguar V
Діапазон частот	30 – 88 МГц (VHF)	225 – 400 МГц (UHF)	960 – 1215 МГц (L-Band)	30 – 88 МГц
Швидкість стрибків	~100 стрибків/с	Засекречено (середня)	76 923 стрибків/с (Fast)	100-500 стрибків/с
Кількість каналів	2320 (крок 25 кГц)	~7000 (крок 25 кГц)	51 (крок 3 МГц)	2319
Метод модуляції	FM (Frequency Modulation)	AM/FM	MSK + CCSK	FM
Синхронізація	ERF, CUE channel, GPS	Word of Day (WOD) + TOD	Global TDMA (GPS req.)	Hailing Tone
Основне призначення	Сухопутні війська (голос)	Авіація (голос)	Обмін даними, ситуаційна обізнаність	Піхота (голос)
Захист від РЕБ	Hopset lockout, FEC	WOD randomization	Fast Hopping, Reed-Solomon	Бар'єрні частоти

Крім того, технології FHSS знайшли також широке застосування у цивільному секторі, зокрема у діапазоні ISM (Industrial, Scientific, and Medical), де вони дозволяють багатьом пристроям співіснувати без взаємних завад.

Bluetooth (IEEE 802.15.1) та Адаптивне перелаштування (AFH).

Bluetooth є класичним прикладом комерційної реалізації FHSS.

Параметри: Працює в діапазоні 2.402–2.480 ГГц, використовуючи 79 каналів шириною 1 МГц. Швидкість стрибків становить 1600 стрибків/с для передачі даних і 3200 стрибків/с для запиту/виклику (Inquiry/Page).

Адаптивне перелаштування частоти (AFH — Adaptive Frequency Hopping): Це ключова інновація для неліцензованих діапазонів. Оскільки діапазон 2.4 ГГц перенасичений (Wi-Fi, ZigBee, мікрохвильові печі), статична послідовність стрибків призводила б до частих колізій.

Механізм AFH: Пристрій Bluetooth (майстер) постійно моніторить якість сигналу на кожному каналі (вимірює Packet Error Rate або RSSI). Канали з високим рівнем завад позначаються як "погані" (Bad Channels) і виключаються з карти стрибків (Hop Map). Передача ведеться тільки на "хороших" каналах, при цьому псевдовипадковий порядок зберігається в межах скороченого набору.

Ефективність: Це дозволяє Bluetooth працювати поруч із потужним передавачем Wi-Fi, який займає фіксовану смугу 20 МГц, просто "обстрибуючи" зайняті частоти.

Системи керування БПЛА (OcuSync, LoRa).

Сучасні дрони (наприклад, DJI) використовують пропрієтарні протоколи (OcuSync, Lightbridge), які є варіаціями FHSS. Вони працюють у діапазонах 2.4 ГГц та 5.8 ГГц, динамічно аналізуючи спектр і перемикаючись на вільні ділянки. Використання широкої смуги (до 40 МГц) і адаптивного FHSS дозволяє передавати потокове HD-відео на великі відстані (до 10 км) навіть в умовах міських завад. Технологія LoRa (Long Range) використовує CSS (Chirp Spread Spectrum), але в деяких регіональних налаштуваннях також застосовує FHSS для дотримання норм використання спектра (duty cycle).

Мережеві аспекти та протоколи маршрутизації (MANET).

Інтеграція засобів FHSS у мобільні однорангові мережі (MANET) створює специфічні виклики для протоколів маршрутизації (Network Layer).

Проблема прихованого вузла в контексті FHSS.

У класичних мережах проблема прихованого вузла вирішується обміном RTS/CTS (Request to Send / Clear to Send). У мережах FHSS вузли можуть

знаходитися на різних частотах у момент передачі RTS, тому вони просто "не почують" один одного. Це призводить до колізій даних, які важко детектувати. Синхронізація патернів стрибків всієї мережі або використання спеціальних загальних каналів сигналізації є необхідними умовами стабільності.

Традиційні протоколи маршрутизації (AODV, OLSR) оперують метриками "кількість хопів" і не знають про стан фізичного середовища. У мережах FHSS, особливо при наявності РЕБ, це неефективно.

Для часткового вирішення цього, протокол (наприклад, модифікований OLSR) може вибирати маршрут не за найменшою кількістю стрибків, а за критерієм надійності каналу (Link Quality Aware routing), обходячи ділянки з сильним глушінням, навіть якщо фізичний шлях довший. Дослідження показують, що протокол AODV часто показує кращі результати в динамічних тактичних мережах FHSS порівняно з OLSR через менші накладні витрати на службовий трафік, хоча OLSR кращий для стабільних сенсорних мереж.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ТА ГІБРИДНИХ ЗАГРОЗ

Сучасні телекомунікаційні мережі, особливо цивільної, побутової якості, являють собою доволі вразливу, як до завад, так і до методів перехоплення інформації, систему. Так, наприклад, незважаючи на глобальне впровадження 5G, мережі GSM залишаються критичним вектором атаки через механізм зворотньої сумісності. Сучасні смартфони, потрапляючи в зону глушіння 4G/5G або під дію "IMSI-catcher", автоматично переходять на 2G, де відсутня взаємна аутентифікація вежі та телефону.

Отже, розглянемо найвідоміші, та найбільш важливі для розуміння контексту загальних принципів роботи таких «закладок», вразливості та методи їх використання.

2.1 Вразливості мобільних мереж поколінь 2G/3G/4G/5G

Архітектура GSM (2G): Спадщина вразливостей та PDU-ін’єкції та приховані канали в форматі SMS PDU

Служба коротких повідомлень (SMS) у стандарті GSM передбачає два режими роботи: текстовий (Text Mode) та режим протокольного блоку даних (PDU Mode). Саме PDU Mode надає можливість маніпулювати бінарною структурою повідомлення на низькому рівні, створюючи приховані канали передачі даних (covert channels).

Маніпуляція заголовком даних користувача (UDH).

Формат PDU дозволяє включати заголовок даних користувача (User Data Header — UDH), який зазвичай використовується для конкатенації (об'єднання) довгих повідомлень або передачі спеціального контенту (наприклад, налаштувань WAP).

Механізм вразливості: Стандарт GSM дозволяє використання UDH навіть у поодиноких SMS. Імплант може сформувати повідомлення, в якому встановлено

біт TP-UDHI (Transfer Layer Protocol - User Data Header Indicator), що сигналізує модему про наявність спеціального заголовка.

Техніка стеганографії: Дослідження демонструють, що поля UDH, такі як "Reference Number" (Ідентифікатор посилання, Октет 4 заголовка), можуть бути використані для передачі прихованих байтів інформації. Оскільки ці поля обробляються стеком модему, але часто ігноруються прикладним рівнем (якщо повідомлення не є частиною реального ланцюжка), користувач не бачить жодних ознак активності.

Пропускна здатність: Експерименти з інструментарієм "GeheimSMS" показали можливість передачі близько 1 КБ даних (наприклад, ключів шифрування або координат) менш ніж за 3 хвилини шляхом відправки серії з 26 модифікованих SMS. Для білінгової системи оператора ці повідомлення виглядають як легітимний трафік.

Експлуатація AT-команд.

Керування GSM-модемом здійснюється через набір AT-команд (Hayes command set). Апаратні або програмні закладки використовують внутрішній послідовний інтерфейс (UART) для прямої взаємодії з модемом.

Команди: Використовуються команди AT+CMGS (відправка SMS у PDU режимі) та AT+CMGR (читання повідомлень).

Прихована робота: Імплант може перехоплювати вхідні SMS-команди (наприклад, "Wake-up" тригер), блокувати їх передачу до операційної системи телефону та видаляти з пам'яті SIM-картки одразу після обробки. Таким чином, екран телефону не засвічується, і звуковий сигнал не лунає.

Signaling System No. 7 (SS7) — це набір протоколів сигналізації, що використовується для налаштування дзвінків, роумінгу та обміну SMS. Фундаментальним недоліком SS7 є відсутність перевірки джерела повідомлень — мережа довіряє будь-якому вузлу, що має доступ до сигнальної мережі.

Геолокація через MAP-повідомлення.

Протокол MAP (Mobile Application Part) використовується для запитів до баз даних HLR (Home Location Register) та VLR (Visitor Location Register).

SRI-SM (Send Routing Info for Short Message): Зловмисник або мережева закладка надсилає запит SRI-SM до HLR жертви, нібито для доставки SMS. HLR повертає адресу комутатора MSC та VLR, які наразі обслуговують абонента, а також його IMSI.

PSL (Provide Subscriber Location): Отримавши адресу VLR, зловмисник надсилає запит PSL. VLR запитує у підсистеми базових станцій (BSS) поточний Cell ID (ідентифікатор соти) і, в деяких випадках, Timing Advance (часове випередження), що дозволяє визначити координати абонента з точністю від кількох сотень метрів до кількох кілометрів.

Перехоплення дзвінків та SMS.

Використовуючи команду RegisterSS (реєстрація додаткових послуг), закладка може дистанційно налаштувати безумовну переадресацію викликів жертви на номер зловмисника ("Man-in-the-Middle"). Дзвінок проходить через сервер запису, а потім перенаправляється реальному абоненту, що робить перехоплення прозорим для обох сторін.

Архітектура 4G/LTE: Перехід до IP та нові вектори атак.

Впровадження 4G LTE ознаменувало перехід до повністю пакетної комутації (All-IP Network). Голосовий зв'язок трансформувався у VoLTE (Voice over LTE), а сигналізація перейшла на протокол Diameter. Це змінило природу загроз, відкривши шлях для атак, характерних для IP-мереж.

Протокол Diameter: Спадкоємець проблем SS7.

Diameter замінив SS7 у функціях аутентифікації, авторизації та обліку (AAA). Хоча він підтримує IPsec та TLS, на практиці мережі часто покладаються на довіру на рівні IPX (IP Exchange).

Міжмережевий інтерфейс (S6a/S9): Інтерфейс S6a з'єднує MME (Mobility Management Entity) у візитовій мережі з HSS у домашній. Закладка, що імітує вузол MME іноземного оператора, може надсилати повідомлення Update-Locaton-Request (ULR) або User-Data-Request (UDR).

Витік даних: У відповідь HSS може передати вектори аутентифікації (RAND, AUTN, KASME), профіль абонента та інформацію про місцезнаходження.

Отримання векторів аутентифікації дозволяє зловмиснику емулювати абонента або розшифрувати його трафік, якщо вдасться перехопити радіообмін.

Спуфінг Origin-Realm: Атаки часто базуються на підробці поля AVP "Origin-Realm", що дозволяє обходити фільтри на межових маршрутизаторах (Diameter Edge Agents).

Тунелювання GTP: Вразливості User Plane.

GPRS Tunneling Protocol (GTP) інкапсулює трафік користувача (GTP-U) та сигналізацію (GTP-C) для передачі через опорну мережу (Evolved Packet Core).

Відсутність цілісності GTP-U: Історично склалося, що оператори перевіряли лише сигналізацію (GTP-C), залишаючи тунелі даних (GTP-U) без перевірки цілісності. Це дозволяє імплантам, розташованим на проміжних вузлах або в роумінгових шлюзах, ін’єктувати шкідливі пакети безпосередньо в сесію користувача.

Передбачуваність TEID: Кожен тунель ідентифікується 32-бітним числом TEID (Tunnel Endpoint Identifier). Якщо алгоритм генерації TEID є передбачуваним, зловмисник може "вгадати" ідентифікатор активної сесії та перехопити або підмінити трафік (наприклад, DNS-запити).

Приховані канали фізичного рівня (PHY) LTE.

Складність модуляції OFDM (Orthogonal Frequency Division Multiplexing) в LTE створює можливості для бездротової стеганографії.

Формування сузір'я (Constellation Shaping).

У цифровій модуляції (наприклад, 16-QAM або 64-QAM) дані кодуються як точки на комплексній площині (сузір'я).

Закладка може накладати низькопотужний прихований сигнал на легітимний сигнал користувача. Це досягається шляхом мікроскопічного зміщення точок сузір'я від їх ідеальних позицій.

Для звичайного приймача (eNodeB) ці зміщення виглядають як тепловий шум або наслідок завмирань у каналі, і вони коригуються алгоритмами корекції помилок. Однак спеціалізований приймач, який знає "кодову книгу" зміщень, може демодулювати цей "шум" як корисну інформацію. Цей метод дозволяє досягти

високої прихованості, оскільки спектральна маска сигналу залишається в межах норми.

Приховування у протоколах RLC та PDCP.

PDCP (Packet Data Convergence Protocol): Заголовок PDCP містить три зарезервовані біти (R-bits), призначені для майбутніх розширень. Імплант може модулювати ці біти для створення низькошвидкісного командного каналу, який ігнорується стандартним мережевим обладнанням.

RLC Padding: На рівні Radio Link Control, якщо пакет даних не заповнює транспортний блок повністю, додається заповнювач (padding). Імплант може замінювати нульові байти заповнювача на зашифровані дані екфільтрації. Оскільки padding відкидається на приймальній стороні перед передачею даних вище по стеку, це забезпечує непомітну передачу.

Архітектура 5G (NR): Кіберфізичні загрози нового покоління.

Перехід до 5G — це не просто збільшення швидкості, а повна зміна парадигми архітектури мережі. Впровадження сервіс-орієнтованої архітектури (SBA), віртуалізації мережевих функцій (NFV) та нових радіотехнологій створює безпрецедентно широкий ландшафт загроз.

5G Core та вразливості API.

Ядро 5G (5GC) відмовилося від специфічних телеком-протоколів на користь веб-стандартів: HTTP/2, JSON та RESTful API.

SBA (Service Based Architecture): Мережеві функції (AMF, SMF, UDM) тепер взаємодіють як мікросервіси. Це робить мережу вразливою до класичних веб-атак: ін’єкцій в API, підробки запитів (SSRF) та атак на логіку серіалізації JSON.

Імпланти в контейнерах: Зловмисник може скомпрометувати Docker-контейнер або Kubernetes-под, що виконує функцію мережі (наприклад, NRF — Network Repository Function). Такий імплант може непомітно дзеркалювати трафік або змінювати маршрутизацію для окремих слайсів мережі.

Network Slicing: Порушення ізоляції

Технологія Network Slicing дозволяє створювати декілька логічних мереж на одній фізичній інфраструктурі.

Атака через спільні ресурси: Якщо слайс високої безпеки (наприклад, для керування енергомережами) та слайс низької безпеки (публічний Wi-Fi) використовують спільний процесорний кеш (L3 Cache) на серверах віртуалізації, можливе застосування атак побічного каналу (типу Spectre/Meltdown). Імплант у "дешевому" слайсі може зчитувати криптографічні ключі з пам'яті захищеного слайсу.

URSP (UE Route Selection Policy): Сучасні пристрої можуть одночасно підключатися до кількох слайсів. Імплант на рівні UE може діяти як міст, пересилаючи конфіденційні дані з корпоративного слайсу в публічний Інтернет-слайс, ігноруючи політики безпеки.

Massive MIMO та просторові приховані канали.

Технологія Massive MIMO використовує сотні антен для формування вузькоспрямованих променів (Beamforming).

Просторова модуляція: Компрометована базова станція (gNodeB) може використовувати бічні пелюстки діаграми спрямованості (side-lobes) для передачі даних. Поки головний промінь обслуговує легітимного користувача, бічна пелюстка, яка зазвичай придушується, може модулюватися для передачі інформації на приймач зловмисника, розташований під іншим кутом.

LPI/LPD (Low Probability of Intercept/Detection): Використання вузьких променів робить перехоплення сигналу складним завданням для традиційних засобів радіомоніторингу, оскільки енергія не розсіюється у всіх напрямках. Імплант може використовувати це для організації скритних каналів зв'язку, спрямовуючи сигнал точно на приймач (наприклад, дрон).

Sidelink (PC5): Мережа "тіньового" зв'язку.

Інтерфейс PC5, розроблений для V2X (Vehicle-to-Everything) та IoT, дозволяє пристроям спілкуватися напряму (Device-to-Device), оминаючи базову станцію.

Mesh-мережі ексфільтрації: Імпланти можуть створювати локальні mesh-мережі між зараженими пристроями. Дані можуть передаватися "естафетою" від захищеного пристрою в "бункері" до менш захищеного пристрою (наприклад, автомобіля на парковці), який має доступ до зовнішньої мережі. Оскільки трафік

PC5 не проходить через ядро мережі (gNodeB/UPF), оператор не бачить цієї комунікації.

Вразливість Mode 2: У режимі 2 (автономний вибір ресурсів) пристрої самі обирають часові слоти для передачі. Імплант може маніпулювати цим процесом, створюючи колізії для блокування легітимного зв'язку або використовуючи механізми резервування ресурсів для прихованої передачі даних.

PRACH та сигнали пробудження (WUS)

PRACH (Physical Random Access Channel): Використовується для початкового доступу до мережі. Імплант може кодувати дані шляхом вибору специфічних послідовностей преамбул (Zadoff-Chu sequences) або маніпулюючи часовими затримками (Timing Advance). Оскільки PRACH є каналом з конкурентним доступом, такі аномалії легко маскуються під звичайні колізії або високе навантаження мережі.

Wake-Up Signal (WUS): Сигнал низької потужності, призначений для виведення IoT-пристроїв з глибокого сну (Deep Sleep). Імплант може бути налаштований на постійний моніторинг ефіру в очікуванні унікальної послідовності WUS, яка слугує тригером активації. Це дозволяє закладці роками перебувати в "сплячому" режимі, не споживаючи енергії, і активуватися лише при наближенні оператора зі спеціальним передавачем.

Оскільки програмні вразливості можуть бути усунені оновленнями ("патчами"), то для довготривалих операцій використовуються апаратні закладки.

Інтерпозери та модифікації PCB.

Сучасна електроніка має надзвичайно високу щільність монтажу, що ускладнює пайку сторонніх чіпів. Для рішення цієї задачі використовуються інтерпозери – проміжні плати.

Так, наприклад, оскільки багато компонентів смартфонів (камери, екрани, мікрофони) підключаються до материнської плати через гнучкі шлейфи (FPC), то зловмисник може замінити оригінальний шлейф на модифікований, який містить мікроскопічний чіп-перехоплювач, що називається Атаки на шлейфи (Flex Cable Attacks). Звісно, це не єдиний спосіб. От наприклад, високошвидкісна шина CSI-2

використовується для передачі зображення з камери. Інтерпозер (наприклад, на базі HSF100), встановлений у розрив цієї шини, може перехоплювати потік відеоданих у реальному часі або ін’єктувати фальшиві кадри для обходу біометричної аутентифікації (Face ID). Імплант повинен підтримувати диференціальну передачу сигналів на гігабітних швидкостях, щоб не порушити цілісність сигналу і не викликати збій системи.

Спадщина каталогу NSA ANT.

Витік каталогу підрозділу TAO (Tailored Access Operations) АНБ США продемонстрував технічні можливості спецслужб – такі як пристрої COTTONMOUTH: Апаратний імплант, вбудований у роз'єм USB-кабелю або конектора містить мікропроцесор ARM, FPGA та радіопередавач (Пристрій функціонує як мережевий міст, дозволяючи зловмиснику підключатися до комп'ютера жертви через радіоканал, навіть якщо той фізично ізольований від мережі); та RAGEMASTER: Пасивний ретровідбивач, встановлений у феритовий фільтр VGA-кабелю. Він перехоплює сигнал червоного кольору відеопотоку і перевипромінює його в радіодіапазоні при опроміненні зовнішнім радаром. Це дозволяє відновлювати зображення екрану дистанційно (атака TEMPEST).

Загрози SoftSIM та eSIM.

Перехід до програмних SIM-карт (SoftSIM) та вбудованих чіпів (eSIM) змінює вектор атак на ідентифікацію абонента. Для цього можуть використовуватись різні методи, серед яких можна виділити наприклад клонування ідентичності завдяки SoftSIM — це програмний додаток, що працює в довіреному середовищі виконання (TEE). Якщо імплант отримує root-доступ до TEE, він може екстрагувати ключі шифрування ($К_i$). Це дозволяє створити "клона" абонента на іншому пристрої для перехоплення SMS з кодами двофакторної аутентифікації. Або наприклад можна використовувати приховану зміну профілю: Імплант може мовчки перемикати активний профіль eSIM на профіль зловмисного оператора, перенаправляючи весь трафік через ворожу опорну мережу.

NB-IoT та проникнення в глибину будівель.

Технологія NB-IoT (Narrowband IoT) розроблена для забезпечення зв'язку у важкодоступних місцях (підвали, бункери) завдяки надзвичайно високому бюджету лінії зв'язку (Maximum Coupling Loss — MCL до 164 дБ).

Це робить NB-IoT ідеальним каналом для "глибоких" закладок, встановлених у захищених приміщеннях, де звичайний сигнал 3G/4G відсутній. Імплант може передавати невеликі пакети даних (телеметрію, ключі) навіть з-під землі, використовуючи існуючу інфраструктуру мобільних операторів.

Методи ексфільтрації даних та подолання "повітряного прошарку".

Для систем, ізольованих від Інтернету (air-gapped systems), імпланти використовують фізичні побічні канали для передачі даних. Такими каналами є Акустичні приховані канали, Електромагнітні канали, технологія TEMPEST, тощо.

Акустичні приховані канали працюють завдяки ультразвуковій передачі: Шкідливе ПЗ (наприклад, імплант Mosquito) маніпулює аудіосистемою комп'ютера, змушуючи динаміки випромінювати ультразвук у діапазоні 18-24 кГц. Цей звук не чутний для людини, але може бути прийнятий та декодований мікрофоном звичайного смартфона, що знаходиться поруч. Швидкість передачі низька, але достатня для крадіжки паролів та ключів шифрування.

Електромагнітні канали працюють черещ генерацію радіовипромінювання (RAMBO / AirHopper): Імплант маніпулює навантаженням на шину оперативної пам'яті (RAM) або відеокарту. Швидке перемикання станів транзисторів створює електромагнітне випромінювання на певних частотах. Модулюючи це навантаження, пристрій перетворюється на примітивний AM/FM-передавач, сигнал якого можна прийняти на відстані кількох метрів.

Засіб PowerHammer регулює навантаження процессора, що спричиняє коливання струму в кабелі живлення. Спеціальний датчик, підключений до електромережі будівлі, може зчитувати ці коливання та декодувати дані.

TEMPEST же використовується для еманації відеоінтерфейсів: Інтерфейси HDMI та VGA передають дані на високих частотах. Через недосконале екранування кабелів частина енергії випромінюється в ефір. Використовуючи методи машинного навчання та SDR-приймачі, зловмисники можуть реконструювати

зображення на моніторі з перехопленого радіосигналу на значній відстані. Сучасні алгоритми дозволяють відновити навіть текст.

Операційна безпека (OPSEC) закладок та методи протидії.

Для тривалого функціонування закладка повинна залишатися непомітною для засобів технічного захисту інформації (ТЗІ). Отже існують певні процедури, котрих необхідно дотримуватися, для забезпечення цього.

Наприклад, ротація ідентифікаторів (IMSI/IMEI).

Оскільки статичні ідентифікатори IMSI або IMEI дозволяють легко виявити та локалізувати пристрій, сучасні імпланти використовують пули віртуальних IMSI. Програмне забезпечення автоматично змінює активний ідентифікатор через випадкові проміжки часу (наприклад, кожні 24 години) або при зміні геолокації. Це унеможливлює побудову "патерну життя" (Pattern of Life) об'єкта. Або ж використовують рандомізація IMEI: На рівні операційної системи (наприклад, Android з root-правами) спеціалізовані модулі можуть генерувати новий IMEI при кожному перезавантаженні, роблячи пристрій "новим" для мережі.

Апаратний "дизеринг" (Dithering).

Для захисту від методів виявлення побічних каналів (наприклад, аналізу енергоспоживання), імпланти використовують техніку "дизерингу", тобто маскування активності. Вона полягає у внесенні випадкового шуму в процеси обробки даних — рандомізації тактових частот або споживання струму. Це розмиває характерну сигнатуру роботи імпланта, роблячи її нерозрізненною на фоні нормальної роботи пристрою.

Таблиця 2.1 – Порівняння векторів атак у різних поколіннях мереж

Покоління	Протокол сигналізації	Ключова вразливість	Тип імпланта	Метод ексфільтрації
2G (GSM)	SS7 (MAP)	Відсутність взаємної аутентифікації	IMSI Catcher, PDU Injection	SMS PDU, Перехоплення голосу

Покоління	Протокол сигналізації	Ключова вразливість	Тип імпланта	Метод ексфільтрації
3G/4G (LTE)	Diameter, GTP	Модель довіри, слабкий захист IP	Тунельний хайджекінг, Апаратні інтерпозери	GTP Tunneling, VoLTE Стеганографія
5G (NR)	HTTP/2 (SBA), PFCP	Вразливості API, Network Slicing, MIMO	Sidelink Mesh, Міжслайсовий бріджинг	MIMO Side-lobes, PRACH Bursts

2.2 Інфраструктурні закладки та архітектура "Store-and-Forward"

Сучасний ландшафт кібершпигунства та радіоелектронної боротьби (РЕБ) зазнав фундаментальних змін, переходячи від моделей постійного з'єднання до складних асинхронних архітектур типу «зберегти-та-передати» (Store-and-Forward). Цей стратегічний зсув зумовлений необхідністю подолання багаторівневих систем захисту периметра, поширенням ізольованих середовищ («повітряний прошарок» / air-gap) та вимогою до максимальної оперативної скритності.

Оперативна необхідність архітектури Store-and-Forward.

У контексті кібершпигунства термін «Store-and-Forward» описує методологію ексфільтрації даних, при якій імплант накопичує розвідувальну інформацію протягом тривалого часу («Store») та передає її у вигляді стиснутих, зашифрованих пакетів лише при настанні певних умов («Forward»). Ця архітектура є прямою відповіддю на можливості сучасних центрів моніторингу безпеки (SOC), здатних виявляти аномалії у постійних потоках трафіку.

Компонент «Store» спирається на здатність імпланта забезпечувати персистентність (закріплення в системі) та використовувати локальні ресурси зберігання. Це можуть бути приховані сектори жорсткого диска, як у випадку платформи GrayFish угруповання Equation Group , флеш-пам'ять маршрутизатора в

проекті CherryBlossom ЦРУ , або вбудований буфер шкідливого кабелю, такого як O.MG Cable.

Компонент «Forward» використовує бездротові протоколи для подолання фізичного розриву з оператором або постом прослуховування (Listening Post — LP). Використання Wi-Fi та Bluetooth зумовлене їх повсюдним поширенням та складністю виділення шкідливого сигналу на тлі природного радіочастотного шуму в міських умовах. Асинхронна природа передачі дозволяє атакуючим мінімізувати час перебування в ефірі, знижуючи ймовірність пеленгації засобами радіоконтролю.

Роль бездротових протоколів у прихованих каналах.

Wi-Fi та Bluetooth є ідеальними векторами для операцій Store-and-Forward, оскільки вони працюють у неліцензованих діапазонах ISM (Industrial, Scientific, and Medical). На відміну від дротових з'єднань, які проходять через корпоративні міжмережеві екрани та системи виявлення вторгнень (IDS), радіосигнали поширюються фізично за межі контрольованого периметра.

Wi-Fi (802.11): Забезпечує високу пропускну здатність для ексфільтрації великих масивів даних, але вимагає значних енерговитрат. Традиційно використовується для атак типу «parking lot», коли оперативник проїжджає повз цільовий об'єкт для збору накопичених логів, що було продемонстровано в проекті Elsa ЦРУ.

Bluetooth/BLE: Пропонує меншу пропускну здатність, але критично низьке енергоспоживання та малу помітність. BLE особливо небезпечний у контексті mesh-мереж, де дані можуть передаватися стрибкоподібно через ланцюжок некомпрометованих пристроїв (наприклад, через мережу Apple Find My) до точки виходу в інтернет.

Глибокий аналіз імплантів Wi-Fi з витоків CIA Vault 7.

Публкація архіву «Vault 7» організацією WikiLeaks у 2017 році надала безпрецедентний погляд на те, як Центральне розвідувальне управління США (ЦРУ) мілітаризувало інфраструктуру Wi-Fi для цілей спостереження. Основна

філософія цих інструментів полягає в трансформації стандартного мережевого обладнання в платформи для шпигунства.

Проект CherryBlossom: Мілітаризація інфраструктури.

CherryBlossom являє собою складний імплант рівня прошивки, розроблений для компрометації бездротових маршрутизаторів і точок доступу (AP), перетворюючи їх на підконтрольні вузли, що називаються «FlyTraps» (Мухоловки). На відміну від шкідливого ПЗ для кінцевих точок, яке знаходиться на ноутбуці жертви, CherryBlossom розташовується безпосередньо на мережевій інфраструктурі, що дає йому привілейоване положення для проведення атак «Людина посередині» (Man-in-the-Middle — MITM) та глибокої інспекції трафіку.

Технічна архітектура та механізм впровадження.

Архітектура CherryBlossom складається з трьох ключових компонентів:

- FlyTrap: Компрометований пристрій (роутер/точка доступу) з модифікованою прошивкою.

- CherryTree: Сервер управління та контролю (C2), розташований у захищеній мережі ЦРУ.

- CherryWeb: Веб-інтерфейс оператора для управління місіями та перегляду зібраних даних.

Процес зараження часто відбувається віддалено. Якщо пристрій має вразливості (наприклад, слабкі паролі адміністратора або вразливості UPnP), оператор може віддалено перепрошити його образом CherryBlossom. Після впровадження FlyTrap ініціює захищене з'єднання (beacon) із сервером CherryTree для отримання завдань («Місій»).

Механізм Store-and-Forward у CherryBlossom критично важливий для логіки виконання місій. Оператор може задати місію зі сканування всього трафіку, що проходить, на наявність специфічних селекторів: адрес електронної пошти, MAC-адрес пристроїв, номерів VoIP або ключових слів у чатах. При спрацьовуванні тригера FlyTrap копіює відповідний сегмент трафіку. Оскільки безперервна трансляція дзеркальованого трафіку (port mirroring) через інтернет негайно деградувала б продуктивність мережі та викликала підозри в адміністраторів,

FlyTrap використовує буферизацію. Перехоплені дані зберігаються в оперативній або флеш-пам'яті роутера («Store») і ексфільтруються на сервер CherryTree («Forward») в періоди низької мережевої активності або через зашифрований канал, що маскується під службовий трафік.

Можливості "Windex" та експлуатація браузерів.

Однією з найпотужніших функцій CherryBlossom є модуль Windex. Цей інструмент дозволяє перенаправляти HTTP-запити цілі на шкідливий сервер для експлуатації вразливостей браузера. Це створює замкнений цикл атаки Store-and-Forward: роутер спостерігає за запитом цілі, зберігає намір експлуатації та перенаправляє користувача на сервер, який доставляє вторинний імплант (наприклад, Athena або AfterMidnight) безпосередньо на комп'ютер жертви. Ця здатність демонструє, як імпланти Wi-Fi інфраструктури слугують плацдармом для глибшої компрометації мережі.

Проект Elsa: Геолокація через аналіз Wi-Fi оточення.

У той час як CherryBlossom націлений на роутери, проект Elsa фокусується на кінцевих точках (ноутбуках під управлінням Windows) для відстеження фізичного місцезнаходження об'єкта з використанням сигналів Wi-Fi, навіть якщо пристрій не підключено до інтернету.

Механізм "Store": Зашифроване логування.

Elsa є хрестоматійним прикладом розвідувального інструменту класу Store-and-Forward. Імплант не вимагає постійного інтернет-з'єднання для виконання своєї основної функції. Натомість він використовує Wi-Fi адаптер зараженого пристрою в режимі пасивного моніторингу для сканування видимих точок доступу (AP).

Алгоритм роботи Elsa включає наступні етапи:

- Сканування: Регулярне опитування радіоефіру для виявлення маяків (beacons) від сусідніх роутерів.

- Збір метаданих: Вилучення з кадрів 802.11 ключових параметрів: ESSID (ім'я мережі), BSSID (MAC-адреса точки доступу) та RSSI (рівень сигналу).

- Логування: Отримані дані, разом із часовими мітками, шифруються та зберігаються у локальному прихованому файлі на диску жертви.

Рішення зберігати дані локально, а не передавати їх у реальному часі, є навмисним компромісом на користь скритності. Постійна передача геоданих вимагає активного мережевого з'єднання, що створює шум і витрачає батарею. Локальне накопичення дозволяє Elsa залишатися невидимою для мережевих моніторів під час фази збору інформації.

Механізм "Forward": Ексфільтрація та тріангуляція.

Фаза «Forward» настає, коли пристрій підключається до інтернету, або коли оперативник вручну вилучає лог-файл через окремий бекдор. Важливо відзначити, що Elsa сама по собі часто не має механізму передачі даних, покладаючись на інші компоненти або ручний доступ.

Після отримання логів оператор використовує загальнодоступні бази даних геолокації (такі як ті, що підтримуються Google та Microsoft для сервісів карт) для перетворення BSSID у фізичні координати широти та довготи. Зіставляючи часові мітки з координатами та рівнями сигналу (для точнішої тріангуляції), аналітики можуть ретроспективно відновити маршрут пересування цілі з високою точністю, ґрунтуючись виключно на «цифровому вихлопі» навколишнього середовища Wi-Fi.

SomberKnave: Подолання «повітряного прошарку» через приховане обладнання.

SomberKnave — це імплант для Windows XP, описаний у каталозі ANT АНБ, але архітектурно схожий з інструментами ЦРУ. Він розроблений для забезпечення прихованого каналу зв'язку для цілей, які логічно ізольовані (підключені до внутрішньої закритої мережі, але не до інтернету).

SomberKnave сканує систему на наявність невикористовуваного Wi-Fi адаптера. Якщо такий виявлено, імплант приховано активує його і намагається асоціюватися з найближчою некерованою точкою доступу (наприклад, відкритим Wi-Fi сусіднього кафе або незахищеною домашньою мережею, сигнал якої проникає в офіс). Це створює міст між захищеною внутрішньою мережею та публічним інтернетом. Імплант ефективно «зберігає» відповіді на команди та «передає» їх через цей таємний Wi-Fi шлях, повністю оминаючи корпоративні

міжмережеві екрани та DLP-системи. Цей метод Store-and-Forward дозволяє здійснювати двосторонній зв'язок з ізольованим хостом, використовуючи його власні апаратні ресурси проти нього самого.

Апаратні закладки та фізичний рівень (Physical Layer).

Крім програмних та мікропрограмних рішень, апаратні імпланти представляють вершину інженерії Store-and-Forward. Ці пристрої фізично знаходяться всередині цільового середовища, часто замасковані під нешкідливі кабелі або периферійні пристрої.

O.MG Cable являє собою сучасну платформу для фізичного доступу і зовні не відрізняється від стандартного зарядного кабелю Lightning, USB-C або Micro-USB, але містить високомініатюризований комп'ютер і Wi-Fi трансивер, вбудовані в оболонку USB-коннектора. Цей пристрій є комерційно доступним аналогом імпланта COTTONMOUTH АНБ, вартість якого у 2008 році становила близько 20,000 доларів, тоді як O.MG доступний дослідникам безпеки менш ніж за 200 доларів.

O.MG Cable функціонує в трьох режимах: Програмування, Розгортання (Deployed) та Тригер (Triggered). У стані «Розгортання» він працює як прозорий кабель, забезпечуючи передачу даних та зарядку, що робить його функціонально невідмінним від легітимного кабелю. Це критично важливо для соціальної інженерії та фізичного впровадження.

Функція «Store» в елітній версії O.MG Cable (Elite) реалізується через вбудований буфер зберігання, здатний вміщувати до 650,000 натискань клавіш. Це дозволяє кабелю діяти як пасивний апаратний кейлогер. Він перехоплює і записує введення користувача (паролі, електронні листи, документи), зберігаючи їх у своїй зашифрованій бортовій пам'яті. Ця пам'ять енергонезалежна, що дозволяє даним зберігатися навіть при відключенні живлення.

Wi-Fi тригери та ексфільтрація.

Механізм «Forward» активується через Wi-Fi. Кабель може діяти як точка доступу (SoftAP) або клієнт існуючої мережі. Атакуючий може підключитися до веб-інтерфейсу кабелю зі смартфона або ноутбука, перебуваючи в радіусі дії

радіосигналу, щоб вилучити збережені логи натискань («Loot») або ініціювати ін'єкцію корисного навантаження (Payload).

Версія Elite підтримує функціонал Air Gap Comms, що передбачає двосторонній прихований канал, де дані можуть бути ексфільтровані, навіть якщо хост-комп'ютер не має активних мережевих інтерфейсів. У цьому сценарії кабель сам виступає в ролі мережевого моста, використовуючи свій вбудований Wi-Fi модуль для зв'язку із зовнішнім світом, в той час як для хоста він представляється стандартним USB-пристроєм введення (HID).

USBee: Ексфільтрація через електромагнітну маніпуляцію шиною.

USBee — це програмний імплант, який перетворює немодифіковані USB-пристрої на радіопередавачі, розмиваючи межу між програмними та апаратними закладками.

USBee працює шляхом швидкої модуляції даних, що відправляються на стандартний USB-накопичувач або будь-який інший USB-пристрій. Відправляючи специфічну послідовність бітів '0' і '1' на шину даних USB, шкідливе ПЗ змушує лінії даних USB (D+ і D-) генерувати електромагнітне випромінювання на частотах між 240 МГц і 480 МГц. Випромінювання модулюється з використанням Binary Frequency Shift Keying (B-FSK) (двійкової частотної маніпуляції).

У цьому сценарії фаза «Store» — це накопичення чутливих файлів на ізольованому (air-gapped) комп'ютері. Фаза «Forward» — це модуляція шини USB для трансляції цих даних по ефіру на найближчий приймач. На відміну від кабелю O.MG, який має власне радіо, USBee перетворює обладнання жертви на радіопередавач. Швидкість передачі даних низька (20–80 байт на секунду) , що диктує необхідність підходу Store-and-Forward, при якому невеликі, але цінні дані (наприклад, ключі шифрування) буферизуються і передаються короткими чергами, щоб уникнути виявлення або теплового троттлінгу контролера USB.

Bluetooth та BLE.

Bluetooth Low Energy (BLE) став кращим вектором для прихованих операцій Store-and-Forward завдяки низькому енергоспоживанню та повсюдному поширенню пристроїв Інтернету речей (IoT).

Революційною розробкою в галузі технологій імплантації є Interscatter (Inter-Technology Backscatter), створена дослідниками з Вашингтонського університету. Ця технологія вирішує критичне обмеження мініатюрних імплантів (наприклад, розумні контактні лінзи, нейроімпланти): відсутність достатньої потужності батареї для генерації стандартних сигналів Wi-Fi.

Пристрої Interscatter не генерують власні радіохвилі. Замість цього вони відбивають (backscatter) сигнали Bluetooth, що випромінюються пристроєм, який знаходиться поруч (наприклад, розумним годинником або телефоном), і модулюють це відбиття таким чином, щоб перетворити його на валідний пакет IEEE 802.11b (Wi-Fi).

Технічно це досягається за рахунок використання «однотонової» (single tone) передачі, створюваної шляхом реверс-інжинірингу процесу скремблювання Bluetooth. Перемикаючи антену в певному ритмі, імплант модифікує відбитий сигнал Bluetooth, створюючи сигнал з однією бічною смугою (Single Sideband — SSB), який стандартні чіпи Wi-Fi можуть декодувати як легитимний пакет.

Це дозволяє реалізувати архітектуру Store-and-Forward, де імплант глибоко всередині захищеного об'єкта (або тіла людини) збирає дані («Store») і очікує появи сигналу Bluetooth — можливо, від розумного годинника співробітника. Потім він «передає» дані («Forward»), перевідбиваючи сигнал як пакет Wi-Fi на компрометований телефон або роутер поблизу. Це забезпечує ексфільтрацію зі споживанням десятків мікроват, що на порядки менше, ніж у стандартних радіомодулів Wi-Fi , роблячи виявлення за енергоспоживанням неможливим.

Приховані Mesh-мережі та експлуатація "Find My".

Поява мереж BLE Mesh та краудсорсингових мереж локації (таких як Apple Find My) відкрила новий вектор для глобальної ексфільтрації Store-and-Forward.

Зловживання мережею "Find My".

Недавні дослідження демонструють, що шкідливе ПЗ може кодувати чутливі дані в рекламні пакети (advertisement packets) BLE, що імітують протокол Apple AirTag.

Шкідливе ПЗ на скомпрометованій (навіть ізольованій) машині транслює маяк BLE, що містить фрагменти зашифрованих даних, замасковані під ротований публічний ключ (rolling public key). Телефони iPhone, що знаходяться поблизу (які належать нічого не підозрюючим перехожим або співробітникам), виявляють цей маяк, сприймають його за втрачений AirTag і завантажують «місцезнаходження» (яке насправді є ексфільтрованими даними) на сервери Apple.

Атакуючий, знаючи алгоритм генерації ключів, опитує мережу Find My для цих конкретних ID і збирає фрагменти даних.

Це ефективно перетворює глобальну популяцію користувачів iPhone на мережу ретрансляції даних (data mules) для шкідливого ПЗ. Пряме підключення до інтернету на цільовому пристрої не потрібне. Латентність висока, але неможливість блокування цього каналу (оскільки він використовує легітимну інфраструктуру Apple) робить його стратегічно важливим.

Вразливості BlueBorne та Mesh-черв'яки.

Вразливості BlueBorne продемонстрували можливість поширення шкідливого ПЗ через Bluetooth без необхідності сполучення пристроїв. У поєднанні з Bluetooth Mesh це створює потенціал для створення «mesh-черв'яків».

У контексті Store-and-Forward mesh-мережі, імплант у захищеній серверній кімнаті може передати дані на розумну лампочку через BLE Mesh. Лампочка зберігає пакет і передає його на термостат, який передає його на торговий автомат у холі, який, нарешті, скидає дані на мобільний пристрій атакуючого на парковці. Функції Provisioning та Relay у специфікації Bluetooth Mesh надають нативну архітектуру для такої багатострибкової (multi-hop) ексфільтрації, де кожен вузол діє як тимчасовий буфер зберігання.

Атака BlueBorne використовує, зокрема, heap overflow у функції l2cap_parse_conf_rsp ядра Linux (стек BlueZ), що дозволяє віддалене виконання коду (RCE) з привілеями ядра. В Android вразливість у службі BNEP (Bluetooth Network Encapsulation Protocol) також дозволяє виконати переповнення купи та захопити контроль над пристроєм. Це дає атакуючим можливість використовувати скомпрометовані пристрої як приховані вузли ретрансляції.

GrayFish та персистентність у прошивці HDD.

Платформа GrayFish покладається на буткіт, що зберігається в реєстрі, і потенційно на перепрограмування прошивки жорстких дисків. Здатність перепрошивати контролери HDD дозволяє створювати приховані сектори на диску, які невидимі для операційної системи та не видаляються при форматуванні.

Фаза "Store": Ця прихована область слугує безпечним, персистентним буфером для зберігання ексфільтрованих даних. Дані шифруються з використанням алгоритму RC5 (специфічна реалізація Equation Group) і хешуються 1000 ітераціями SHA-256 з використанням унікального NTFS object ID системи, що прив'язує зашифровані дані до конкретного "заліза".

Фаза "Forward": Дані вилучаються, коли оркестратор GrayFish робить специфічні виклики API, або потенційно через низькорівневі тригери.

Fanny — це комп'ютерний черв'як, що використовувався Equation Group для картографування ізольованих мереж. Він використовує приховану область зберігання на USB-накопичувачах.

Коли флеш-накопичувач підключається до зараженої ізольованої машини, Fanny записує зібрані системні дані в приховану область («Store»).

А коли та ж флешка підключається до машини з доступом в інтернет, екземпляр Fanny на цій машині зчитує приховані дані та передає їх на C2-сервер («Forward»). У зворотному напрямку на флешку записуються команди C2, які переносяться назад через повітряний прошарок. Це квінтесенція архітектури Store-and-Forward на основі «sneaker-net».

DoubleFantasy та валідація цілей.

Імплант DoubleFantasy слугує первинним валідатором. Він заражає систему, перевіряє її на цікавість для атакуючих і, у разі підтвердження, завантажує складніші платформи, такі як EquationDrug або GrayFish. Взаємодія з цими імплантами часто будується на складних криптографічних протоколах, що забезпечують скритність каналу управління.

Wi-Fi Backscatter та таймінгові канали (CHAOS).

Дослідження в галузі Wi-Fi Backscatter та інструменти типу CHAOS показують, що дані можуть бути приховані в таймінгах кадрів-маяків (beacon frames) Wi-Fi. Маніпулюючи полем Timestamp у заголовку 802.11 або порядком відправки маяків, імплант може кодувати приховані біти.

Це працює завдяки тому, що імплант затримує відправку маяка на кілька мікросекунд. Приймач, що аналізує трафік, вимірює час між прибуттям кадрів (Inter-Arrival Time). Коротка затримка може означати '0', довга — '1'.

Такий трафік виглядає як нормальне мережеве перевантаження або джиттер (тремтіння фази), що робить його невидимим для стандартних брандмауерів, які аналізують IP-пакети. Використання функції синхронізації часу (TSF) стандарту 802.11 для кодування даних робить канал вкрай стійким і важким для виявлення.

Стеганографія в протоколах IoT: MQTT та CoAP.

Протоколи Інтернету речей, такі як MQTT (Message Queuing Telemetry Transport) та CoAP (Constrained Application Protocol), надають широкі можливості для стеганографії.

MQTT: Використовує модель публікації/підписки поверх TCP. Приховані дані можуть бути вбудовані в невикористовувані поля заголовків, у порядок топіків (topics) або закодовані в інтервали між повідомленнями PUBLISH. Зловмисники можуть використовувати легітимні брокери MQTT як проміжні вузли Store-and-Forward, публікуючи зашифровані дані в публічних топіках, які потім зчитуються C2-сервером.

CoAP: Працює поверх UDP і використовує семантику REST. Через відсутність суворого контролю стану з'єднання (stateless), CoAP вразливий для прихованих каналів, заснованих на маніпуляції опціями заголовків (Token, Message ID) або порядку блоків при передачі великих даних (Block-Wise Transfers). Honeypot-дослідження зафіксували підозрілі запити до серверів CoAP, що свідчать про спроби використання протоколу для розвідки або C2-комунікацій.

DNS-тунелювання через Wi-Fi.

Хоча DNS-тунелювання відоме давно , його застосування у Wi-Fi імплантах має особливості. Імплант може інкапсулювати дані в DNS-запити, що відправляються на підконтрольний зловмиснику домен.

А далі застосовується Store-and-Forward: Імплант кешує 10 МБ документів. Потім він розбиває ці дані на тисячі дрібних фрагментів, кодуючи їх у піддомени DNS-запитів (наприклад, base64chunk.attacker.com). Ці запити відправляються з великими інтервалами («Forward»), щоб уникнути спрацьовування систем обмеження швидкості (rate-limiting) і змішатися з легітимним DNS-трафіком.

Таблиця 2.2 – Порівняльна таблиця технічних характеристик ключових імплантів

Характеристика	NSA Cottonmouth-I	O.MG Cable Elite	CIA Elsa	Equation Group GrayFish
Форм-фактор	USB-A / USB-B конектор	Кабель (Lightning, USB-C)	Програмний імплант (DLL)	Програмний/Firmware (Bootkit)
Зв'язок	RF Link (власний радіоканал)	Wi-Fi (802.11b/g/n)	Wi-Fi (пасивний моніторинг)	Інтернет / Приховані сектори HDD
Подолання Air-Gap	Так, через RF міст	Так, через Wi-Fi точку доступу	Ні (вимагає вивантаження логів)	Ні (але працює з Fanny USB)
Механізм "Store"	Обмежений буфер команд	650,000 натискань (Flash)	Зашифрований лог-файл	Прихована файлова система (VFS)
Механізм "Forward"	RF-трансляція на ROC	WebUI / C2 через Wi-Fi	Ручне вилучення / Beacon	API виклики / C2 канал

Характеристика	NSA Cottonmouth-I	O.MG Cable Elite	CIA Elsa	Equation Group GrayFish
Вартість	~$20,000 (2008 р.)	~$180 (2024 р.)	Розробка ЦРУ	Розробка АНБ/Equation
Основна ціль	Розвідка високого рівня	Red Teaming / Пентест	Геолокація об'єкта	Тотальний контроль / Персистентність

2.3 Стеганографія та використання IoT-протоколів

На зміну аналоговим схемам прийшли високотехнологічні гібридні системи, які діють на стику різних фізичних доменів, експлуатують складні цифрові протоколи та інтегруються в легітимну інфраструктуру цільових об'єктів. Цей звіт присвячено всебічному аналізу феномену гібридних радіозакладних пристроїв, дослідженню їхньої архітектури, принципів дії, небезпеки, яку вони становлять для національної та корпоративної безпеки, а також розгляду передових методологій їх виявлення.

Гібридність у контексті технічної розвідки не є просто маркетинговим терміном; це фундаментальна зміна парадигми проектування шпигунського обладнання. Вона передбачає поєднання декількох технологій збору, обробки, накопичення та передачі інформації в єдиному комплексі для досягнення двох головних цілей: максимальної скритності (Low Probability of Intercept/Detection — LPI/LPD) та забезпечення стійкості каналу витоку в умовах активної протидії. Аналіз доступних технічних даних, історичних прецедентів та сучасних досліджень у сфері кіберфізичних систем дозволяє виділити три основні виміри гібридності: фізичну (мультимодальну), протокольну (cross-protocol) та операційну (часову).

Гібридний закладний пристрій можна визначити як систему, що використовує синергію різнорідних технологічних принципів для перетворення,

зберігання або передачі розвідувальної інформації, ускладнюючи тим самим її виявлення традиційними моно-сенсорними методами контролю. На відміну від класичних пристроїв, які покладаються на один канал (наприклад, радіоефір), гібридні системи динамічно адаптуються до середовища.

Мультимодальне перетворення (Multi-Modal Transduction).

В основі роботи багатьох гібридних пристроїв лежить принцип перетворення енергії з одного фізичного поля в інше без використання традиційних активних електронних компонентів, які легко виявляються детекторами нелінійних переходів. Наприклад, акустична хвиля (звук голосу) може модулювати оптичний сигнал (лазерний промінь) або змінювати параметри електромагнітного поля (імпеданс антени) у пасивному режимі. Такий підхід дозволяє створювати пристрої з "нульовим" енергоспоживанням у режимі очікування та повною відсутністю власного радіовипромінювання до моменту зовнішньої активації.

Міжпротокольна взаємодія (Cross-Protocol Bridging).

Другий аспект гібридності стосується використання вразливостей на стику різних комунікаційних стандартів. Сучасні офісні пристрої часто оснащені чіпами, що підтримують одночасно декілька протоколів (Wi-Fi, Bluetooth, ZigBee, LTE). Гібридний імплант може перехоплювати дані в захищеному сегменті дротової мережі Ethernet, але ексфільтрувати їх через бездротовий канал ZigBee або Bluetooth на скомпрометований смартфон інсайдера або дрон, що пролітає поруч. Це дозволяє обійти мережеві екрани (Firewalls) та системи запобігання витокам даних (DLP), які зазвичай моніторять лише основний інтернет-трафік.

Архітектура "Store-and-Forward": Нівелювання Фактору Часу.

Однією з найбільш небезпечних характеристик сучасних гібридних пристроїв є відмова від потокової передачі даних у реальному часі на користь архітектури "накопичення та передача" (Store-and-Forward). Ця стратегія спрямована на мінімізацію часу перебування пристрою в активному стані, що робить його практично невидимим для періодичних перевірок спектру.

Принципи ретро-рефлексії та пасивної модуляції.

Окремим класом гібридних пристроїв є системи, що базуються на принципі ретро-рефлексії (backscatter). Вони не генерують власного радіосигналу, а модулюють і відбивають зовнішнє опромінення. Це робить їх "напівпасивними" або повністю пасивними.

Фізична основа цього методу полягає у зміні ефективної площі розсіювання (RCS) антени пристрою в такт з інформаційним сигналом. Наприклад, якщо до антени підключити транзистор і змінювати його імпеданс залежно від напруги на виході мікрофона, відбитий від антени сигнал буде модульований звуком. Оскільки пристрій лише перевипромінює чужу енергію, його неможливо запеленгувати пасивними засобами радіорозвідки, якщо не знати частоту і параметри опромінюючого сигналу.

Каталог NSA ANT: Індустріалізація та мініатюризація.

Опублікований у 2013 році каталог підрозділу ANT (Advanced Network Technologies) АНБ США демонструє, як концепція гібридності була розвинена до промислового рівня. Розглянемо ключові зразки:

LOUDAUTO (Аудіо-базований RF Ретро-рефлектор) використовує мікрофон Knowles для перетворення звуку в електричний сигнал, який потім модулює зовнішній радарний сигнал (Continuous Wave) методом позиційно-імпульсної модуляції (PPM).

Пристрій є "напівпасивним" (semi-passive). Він споживає мізерний струм (15 мкА) від батареї лише для роботи мікрофона та логіки модуляції, але енергію для передачі даних у ефір бере повністю від зовнішнього опромінення.

Найбільш розповсюдженим застосуванням є прихована установка в приміщеннях, де неможливо забезпечити постійне живлення або де проводиться регулярний радіомоніторинг.

RAGEMASTER (RF-імплант у відеотракті) – це апаратний імплант, прихований у феритовому фільтрі кабелю монітора (VGA).

Гібридність (Відео -> RF) полягає в тому, що пристрій перехоплює аналоговий сигнал червоного кольору (Red video line) і використовує його для модуляції відбитого радіосигналу (backscatter). Це дозволяє відтворювати

зображення з екрана цільового комп'ютера на радарі-приймачі (наприклад, NIGHTWATCH).

Живиться від енергії самого відеосигналу або зовнішнього опромінення, не потребуючи окремого джерела живлення.

JETPLOW (Гібрид Кібер-Фізичний) Модифікація прошивки (Firmware Implant) для міжмережевих екранів Cisco PIX/ASA.

Це приклад того, як програмний код забезпечує персистентність для фізичних атак. JETPLOW перетворює мережевий пристрій на плацдарм, який може завантажувати інші модулі, здатні, наприклад, використовувати світлодіоди пристрою для оптичної передачі даних або маніпулювати апаратними ресурсами для створення побічних електромагнітних випромінювань.

Сучасні Загрози Інтернету Речей (IoT).

Еволюція побутової електроніки створила новий клас гібридних загроз, де саме середовище стає інструментом шпигунства.

Атака Lamphone (Оптико-акустична).

Дослідники продемонстрували можливість відновлення високоякісного звуку з кімнати, спостерігаючи за звичайною підвісною лампочкою через вікно за допомогою телескопа та електрооптичного сенсора. Звукові хвилі викликають мікровібрації скляної колби лампи. Ці вібрації модулюють кут відбиття або інтенсивність світла. Аналіз флуктуацій світлового потоку дозволяє відновити розмову в реальному часі.

Акустика -> Механіка -> Оптика -> Цифрова обробка. Це повністю пасивна атака, яка не вимагає проникнення в приміщення або встановлення обладнання.

Компрометація Периферії (Принтери та IP-телефони).

Сучасні офісні пристрої часто мають приховані можливості підключення. Наприклад, 3D-принтери або МФУ можуть містити LTE-модеми для віддаленої діагностики виробником. Зловмисник через кібератаку активує прихований модем або встановлює апаратний імплант у розрив ланцюгів живлення/даних принтера. Пристрій починає пересилати скани документів через стільникову мережу,

оминаючи корпоративний фаєрвол. Цей метод називається "supply chain interdiction" — перехоплення на етапі постачання.

IP-телефони: Вразливості в телефонах Cisco (наприклад, експлуатовані групою Salt Typhoon) дозволяють перетворити апарат на постійно ввімкнений мікрофон, який транслює аудіо через прихований GRE-тунель, маскуючи трафік під легітимні VoIP-пакети.

Гібридні радіозакладні пристрої представляють собою вершину еволюції засобів технічного шпигунства, поєднуючи в собі передові досягнення фізики, мікроелектроніки та програмування. Їхня головна небезпека полягає в здатності діяти в "сірих зонах" між традиційними доменами безпеки, використовуючи інфраструктуру жертви проти неї самої.

РОЗДІЛ 3
РОЗРОБКА КОМПЛЕКСУ ПОШУКУ ТА ЛОКАЛІЗАЦІЇ РАДІОЗАКЛАДНОГО ПРИСТРОЮ НА БАЗІ SDR-РАДІОПРИЙМАЧА TinySA

Тепер, коли основні види радіозакладних пристроїв та принципи їхньої роботи розглянуто, можна перейти до постановки практичного завдання та безпосередньо розробки антенного комплексу на базі SDR-Радіоприймача TinySA для пошуку даного радіозакладного пристрою.

І почати варто із постановки практичної задачі, яку й необхідно буде вирішити – а саме із створення умовного «супротивника»-радіозакладки.

3.1 Моделювання джерела загрози: розробка тестового передавача

Основою будь-якої радіозакладки є автогенератор, частота якого змінюється під впливом інформаційного сигналу. Найбільш ефективною для УКХ-діапазону є схема Колпітца, де зворотний зв'язок здійснюється через ємнісний дільник. У контексті даного дослідження ми розглядаємо транзистор не лише як підсилювач, а як реактивний елемент керування частотою.

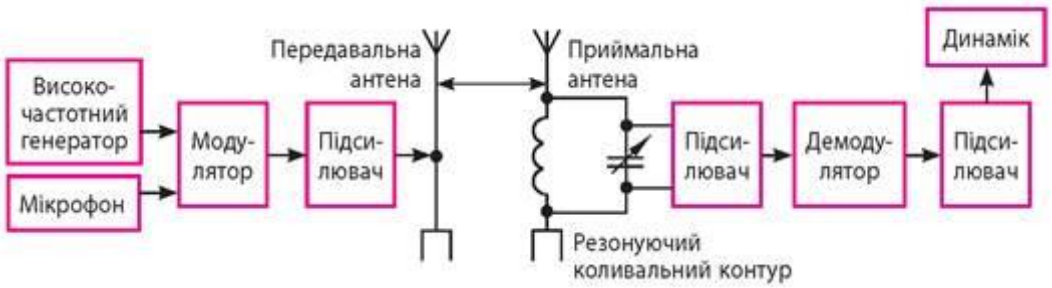

Рис. 3.1 – Приклад будови типового радіозакладного пристрою на основі принципу радіопередачі

Математична модель генерації та модуляції.

Робоча частота F_{osc} визначається параметрами коливального контуру, що складається з індуктивності L та сумарної ємності C_{tot}. У малопотужних

передавачах роль змінного конденсатора виконує бар'єрна ємність колекторного переходу транзистора C_μ.

Формула резонансної частоти контуру має вигляд:

$$f_{osc} = \frac{1}{2\pi\sqrt{L(C_{ext} + C_\mu)}}$$

де C_{ext} — зовнішні конденсатори обв'язки, а C_μ — ємність переходу, яка залежить від прикладеної напруги.

Залежність ємності переходу від напруги зміщення V_D описується рівнянням:

$$C_\mu = C_{\mu 0}(1 - \frac{V_D}{V_0})^{-n}.$$

У цій формулі $C_{\mu 0}$— ємність при нульовому зміщенні, V_0— контактна різниця потенціалів переходу, а n — коефіцієнт, що залежить від профілю легування (зазвичай $\frac{1}{2}$ для різких переходів). Коли сигнал з мікрофона $v_m(t)$ подається на базу, він змінює миттєве значення V_D що призводить до частотної модуляції (ЧМ).

Розрахунок частотної девіації.

Для визначення ефективності модуляції необхідно розрахувати девіацію частоти Δf. Якщо інформаційний сигнал $v_m(t)$ значно менший за напругу живлення V_{CC} то миттєву частоту f_i можна апроксимувати як:

$$f_i \approx f_k \left(1 - \frac{k_1}{2C_k} v_m(t)\right)$$

де f_k— центральна частота, а k_1 — крутизна зміни ємності. Це рівняння показує, що зміна частоти лінійно пропорційна амплітуді звукового сигналу, що забезпечує високу якість передачі звуку.

Для забезпечення якісного сигналу, який можна ефективно аналізувати за допомогою TinySA, ми розробимо двотранзисторну схему: задавальний генератор за схемою Колпітца та вихідний буферний каскад для ізоляції антени.

Розрахунок коливального контуру (Tank Circuit).

Основним елементом, що визначає частоту випромінювання, є паралельний коливальний контур в колекторному ланцюзі транзистора. Для роботи на частоті f_{res}= 100$ МГц ми використовуємо безкаркасну котушку індуктивності та систему ємностей.

Використовуємо емпіричну формулу для одношарової повітряної котушки:

$$L\ (mH) = \frac{d^2 * n^2}{18d + 40l}$$

де d — діаметр котушки в дюймах, l — довжина котушки в дюймах, n — кількість витків. Приймемо параметри: n = 5 витків, діаметр d = 0.236 дюйма (6 мм), довжина l = 0.315 дюйма (8 мм).

$$L \approx \frac{0.236^2 * 5^2}{18 * 0.236 + 40 * 0.315} = \frac{0.0557 * 25}{4.248 + 12.6} \approx 0.082mH\ (82\ nH)$$

Згідно з формулою Томсона для резонансу необхідна сумарна ємність C_{tot}

$$C_{tot} = \frac{1}{(2\pi f_{res})^2 L} = \frac{1}{(6.28 * 100 * 10^6)^2 * 82 * 10^{-9}} \approx 30.9\ pF$$

Ця сумарна ємність складається з постійного конденсатора, підлаштовувального тримера та внутрішньої ємності транзистора.

Математична модель частотної модуляції (ЧМ).

У нашому прикладі модуляція здійснюється безпосередньо за рахунок зміни бар'єрної ємності колекторного переходу транзистора C_μ при зміні напруги на базі. Ємність переходу C_μ залежить від напруги зміщення V_{BC} наступним чином:

$$C_\mu = \frac{C_{\mu 0}}{\sqrt{1 + \frac{V_{BC}}{V_{bi}}}}$$

де $C_{\mu 0}$— ємність при нульовій напрузі, V_{bi}— контактна різниця потенціалів (~0.7 В для кремнію).

При подачі звукового сигналу $v_m(t)$з мікрофона на базу транзистора, напруга на переході стає $V_{BC}(t) = V_{bias} + v_m(t)$

Розрахунок девіації частоти.

Миттєва частота генератора $f_i(t)$описується рівнянням:

$$f_i(t) = f_k \left(1 - \frac{k_1}{2C_k} v_m(t)\right)$$

де f_k — центральна частота (100 МГц), C_k— ємність контуру в точці спокою, k_1 — крутизна зміни ємності ΔC/ΔV

Якщо амплітуда звукового сигналу v_m= 10 мВ, а крутизна транзистора забезпечує зміну ємності на 0.5 пФ/В, то девіація частоти складе:

$$\Delta f = 100\ MHz * \frac{0.5\ pF/V\ * 0.01\ V}{2 * 30.9pF} \approx 8.1\ kHz$$

Це відповідає стандартам вузькосмугової ЧМ, яку TinySA може легко зафіксувати в режимі "Listen" або через візуальний аналіз розширення спектральної лінії.

Схемотехнічна реалізація та ізоляція.

Для стабільності частоти, що критично важливо при виявленні, ми додаємо другий транзистор (буфер).

Буферний каскад (Buffer Stage) працює в режимі класу А і забезпечує високий вхідний опір. Математично це мінімізує ефект "load pulling" (зсуву частоти під впливом навантаження).

Коефіцієнт ізоляції буфера S_{12} визначає, яка частина відбитої від антени енергії повернеться в генератор:

$$\Delta f_{pulling} \infty f_0 * \frac{1}{Q} * |S_{12}|$$

Використання буфера знижує вплив антени на частоту в 10–100 разів, що дозволяє оператору з TinySA бачити на екрані чітку несучу, яка не "стрибає" при наближенні рук до пристрою.

Індуктивність повітряної котушки змінюється при нагріванні через зміну її геометрії (d та l). Коефіцієнт температурної нестабільності частоти (TFC) для мідної котушки становить близько $\frac{15*10^{-6}}{℃}$.

На частоті 100 МГц зміна температури на 10 градусів призведе до дрейфу:

$$\Delta f_{temp} = 100MHz * 10°C * 15 * 10^{-6} = 15\ kHz$$

TinySA з налаштованим RBW (Resolution Bandwidth) 3–10 кГц дозволяє чітко відстежувати цей дрейф у реальному часі на водоспаді.

Для усунення паразитних шумів, які TinySA відобразить як бічні пелюстки (sidebands), у ланцюзі живлення необхідно використовувати блокуючий конденсатор ємністю 22 нФ. Його реактивний опір X_C на частоті 100 МГц повинен бути мінімальним:

$$X_C = \frac{1}{2\pi fC} = \frac{1}{6.28 * 100 * 10^6 * 22 * 10^{-9}} \approx 0.07\ \text{Ом}$$

Це гарантує чистий спектр випромінювання.

Таким чином, проектування радіозакладки як математично прорахованого VCO з буферною ізоляцією робить її ідеальним об'єктом для вивчення характеристик спектру за допомогою аналізатора TinySA.

TinySA (особливо версія Ultra) виступає в ролі портативного векторного аналізатора спектру. Для пошуку закладки критично важливо правильно налаштувати роздільну здатність смуги пропускання (RBW).

Математичний зв’язок між швидкістю сканування T_{sweep}та RBW визначається як:

$$T_{sweep} \approx \frac{k * \Delta F}{RBW^2}$$

де ΔF— обраний діапазон частот (span), а k — константа апаратної частини. При пошуку в широкому діапазоні (3–300 МГц) на TinySA слід використовувати більший RBW (наприклад, 100–600 кГц) для швидкого виявлення піків, а при локалізації — мінімальний (до 2.7 кГц) для точного вимірювання частоти.

Ефективність радіопеленгації безпосередньо залежить від здатності антени трансформувати параметри електромагнітної хвилі (амплітуду та фазу) у вимірювану напругу на вході TinySA. Для повного циклу операції "виявлення–локалізація" ми спроектуємо дві різні системи: широкосмуговий дискоконус для первинного сканування та спрямовану антену Ягі-Уда для фінального виходу на об'єкт.

3.2 Проектування антенних систем для радіомоніторингу

Для більш ефективного пошуку закладки, на початку, варто використовувати дискоконусний тип антен.

Дискоконусна антена є фундаментальним інструментом у радіомоніторингу, оскільки вона поєднує в собі дві критично важливі властивості для пошуку невідомих сигналів: надширокосмуговість та всеспрямованість. У контексті використання TinySA, ця антена виступає в ролі «ширококутної лінзи», яка

дозволяє бачити весь спектр одночасно без необхідності переналаштування геометрії елементів.

Дискоконусна антена (Discone) — це модифікація біконічної антени, де один із конусів замінено плоским диском. Така структура забезпечує вертикальну поляризацію та надзвичайно широкий робочий діапазон частот, що часто досягає співвідношення 10:1 між верхньою та нижньою межами.

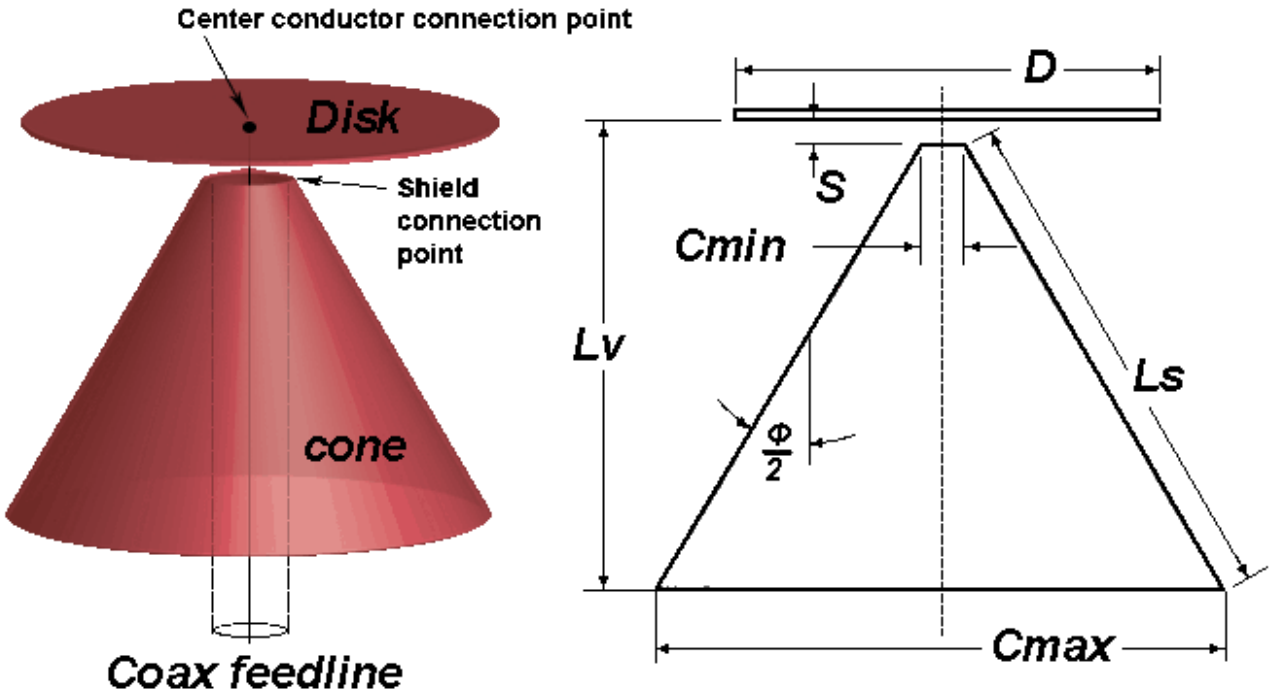

Рис. 3.2 – Приклад будови диско конусної антени

Електродинамічна теорія широкосмуговості.

Широкосмуговість дискоконуса обумовлена його геометричною формою, яка забезпечує поступову зміну хвильового опору від точки живлення до країв антени.

Принцип низької добротності (Q-factor).

На відміну від вузькосмугових диполів, де енергія накопичується у вузькому резонансному полі, конічна форма дискоконуса розосереджує електричне поле. Це значно знижує накопичену реактивну енергію, що математично виражається у низькій добротності Q:

$$Q = \frac{\omega \cdot W_{stored}}{P_{loss}}$$

Низьке значення Q безпосередньо корелює з широкою смугою пропускання оскільки смуга $\Delta \boldsymbol{f} \approx \boldsymbol{f_{res}/Q}$.

Математична модель хвильового опору (Теорія Шелккунова).

Сергій Шелккунов розробив формулу для розрахунку характеристичного опору Z_0 конічного монополя над нескінченною площиною заземлення, що є базою для розуміння дискоконуса:

$$Z_0 = 60 \ln\left(cot\left(\frac{\theta}{4}\right)\right)$$

де θ — кут розкриття конуса. Для стандартного вхідного опору 50 Ом, який необхідний для TinySA, оптимальний кут розкриття конуса зазвичай лежить у межах від 25 до 40 градусів.

Для того, щоб антена ефективно приймала сигнал нашої закладки (100 МГц), необхідно розрахувати її розміри, виходячи з найнижчої робочої частоти $\boldsymbol{F_{min}}$зрахунок довжини конуса.

Довжина твірної конуса L_c повинна дорівнювати чверті довжини хвилі на найнижчій частоті:

$$L_c = \frac{c}{4 * F_{min}} * k$$

де c ≈ 300 * 10^6 м/с, а k ≈ 0.95 – коефіцієнт скорочення. Спрощена формула для розрахунку в метрах

$$L_c(m) = \frac{75}{F_{min}(MHz)}$$

Для частоти 100 МГц: L_c = 75 / 100 = 0.75 метра.

Розрахунок діаметра диска.

Діаметр верхнього диска D_d є критичним для узгодження імпедансу і зазвичай становить 0.7 від довжини твірної конуса:

$$D_d = 0.7 * L_c = \frac{52.5}{F_{min}(MHz)}$$

Для 100 МГц: D_d = 0.7 * 0.75 = 0.525 метра.

Відстань між диском і вершиною конуса (gap) має становити близько \$1/4\$ внутрішнього діаметра конуса в точці зрізу (зазвичай 3–5 мм для УКХ). Зменшення цього зазору збільшує ємність, що може звузити смугу на високих частотах.

Діаграма спрямованості та її деформація.

Дискоконусна антена має «бубликоподібну» (toroidal) діаграму спрямованості з максимумом прийому в горизонтальній площині.

При роботі на частотах, близьких до F_{m} антена має широку основну пелюстку, спрямовану до горизонту. Однак, при значному підвищенні частоти (наприклад, у 5–10 разів від F_{min} діаграма спрямованості починає деформуватися:

- З'являються додаткові пелюстки (grating lobes).

- Основна пелюстка може відхилятися вгору від горизонту (elevation tilt).

- Gain (коефіцієнт підсилення) залишається стабільним близько 2.15 dBi (як у диполя), але його ефективність у горизонтальній площині може знижуватися через це відхилення.

Практична реалізація: Родова (Spoke) конструкція.

Для зменшення парусності (wind loading) та ваги антени, суцільні металеві поверхні диска та конуса замінюють на систему стрижнів (спиць).

Математично доведено, що для ефективної імітації суцільної поверхні в діапазоні до 300 МГц достатньо використовувати від 6 до 16 стрижнів. Чим більше стрижнів, тим краще антена наближається до теоретичної моделі суцільного конуса на високих частотах.

Відстань між кінцями стрижнів не повинна перевищувати 0.1λ на найвищій робочій частоті.

Методика роботи з TinySA.

При використанні дискоконусної антени в парі з TinySA для виявлення закладки на 100 МГц, оператор отримує наступні переваги:

1. Швидке сканування (Span): Оскільки антена не резонансна, можна встановити Span на TinySA від 30 до 300 МГц і бачити всі сигнали без втрати чутливості через неузгодженість антени.

2. Стабільність фону: Дискоконус забезпечує стабільний "Noise Floor" на екрані приладу, що дозволяє легше ідентифікувати аномальні піки випромінювання.

3. RSSI-моніторинг: Завдяки всеспрямованості, рівень сигналу на TinySA буде змінюватися тільки в залежності від відстані до джерела, а не від орієнтації антени, що корисно для початкової оцінки потужності закладки за рівнянням Фріїса.

Рис. 3.3 – Одна з моделей пристрою TinySA

Таким чином, дискоконусна антена є незамінним першим етапом у системі радіопошуку, забезпечуючи гарантоване перехоплення сигналу в надширокому діапазоні частот перед переходом до точної пеленгації за допомогою спрямованих систем.

Електродинамічне моделювання та проектування антени Ягі-Уда для точної радіолокації на частоті 100 МГц.

Якщо дискоконусна антена працює за принципом охоплення всього простору, то антена Ягі-Уда (Yagi-Uda) діє як «радіопрожектор». Її завдання — сконцентрувати прийом електромагнітної енергії у вузькому секторі, що дозволяє не тільки підвищити чутливість TinySA до слабких сигналів, а й точно визначити азимут на джерело.

Антена Ягі-Уда складається з одного активного елемента (диполя) та кількох пасивних (паразитних) елементів — рефлектора та директорів. На відміну від фазованих решіток, де кожен елемент живиться окремо, у системі Ягі струми в пасивних елементах наводяться за рахунок взаємної індукції (електромагнітного зв'язку).

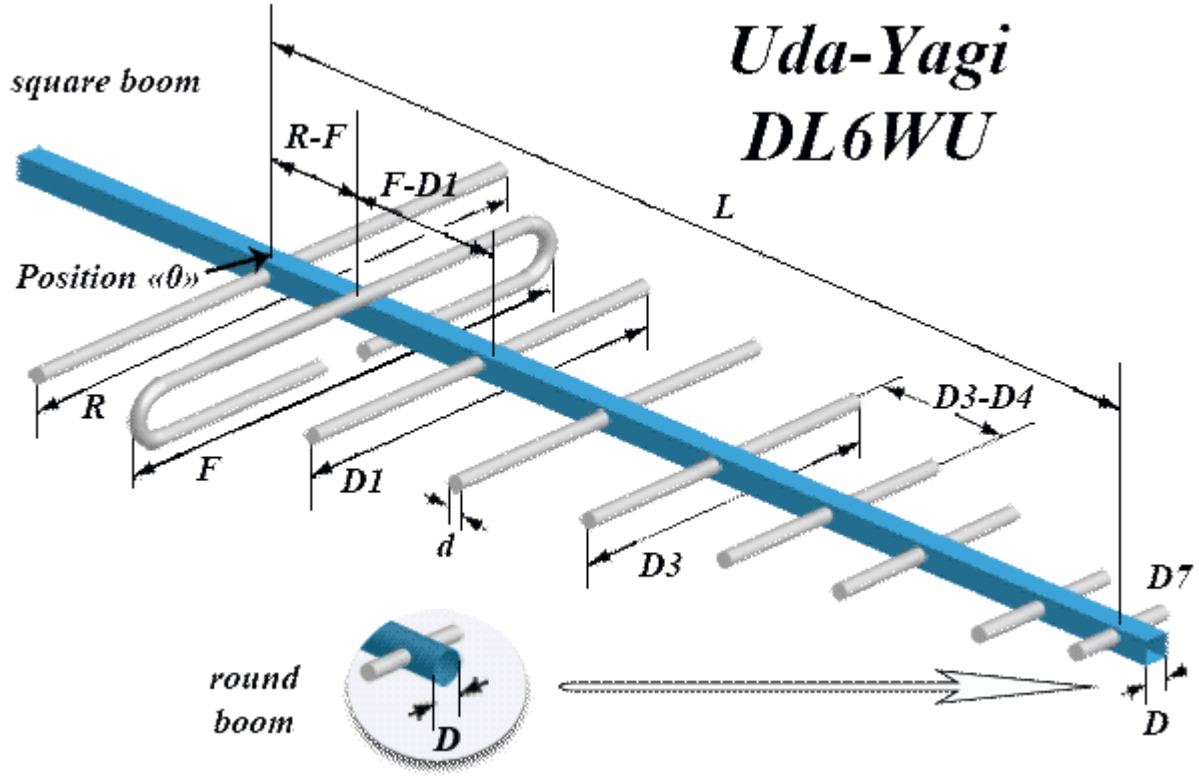

Рис. 3.4 – Загальна конструкція антени Ягі-Уда

Фазова детермінація спрямованості.

Ключ до розуміння роботи Ягі лежить у фазових зсувах наведених струмів. Рефлектор розташовується позаду активного диполя і має довжину, що трохи

перевищує резонансну (~0,5λ) Через це його імпеданс має індуктивний характер, що спричиняє затримку фази наведеного струму. Математично це призводить до того, що перевипромінювана рефлектором хвиля складається з основною хвилею синфазно у напрямку «вперед» і в протифазі у напрямку «назад», створюючи ефект відбиття.

Директори, розташовані попереду, мають довжину меншу за резонансну (~0.4-0.45 λ) Їхній імпеданс є ємнісним, що змушує фазу струму випереджати збуджуюче поле. Це створює прискорювальну фазову послідовність, яка фокусує енергію в один вузький промінь уздовж осі антени.

Розрахунок антени Ягі неможливий без врахування взаємного впливу елементів. Струм I_n у кожному пасивному елементі n визначається через систему лінійних алгебраїчних рівнянь, що базуються на матриці взаємних імпедансів Z_{mn}

$$V_1 = I_1 Z_{11} + I_2 Z_{12} + \cdots + I_n Z_{1n}$$
$$0 = I_1 Z_{21} + I_2 Z_{22} + \cdots + I_n Z_{2n}$$

де V_1 — напруга на активному диполі, Z_{nn}— власний імпеданс елемента, а Z_{mn}— взаємний імпеданс між m та n елементами.

Взаємний імпеданс розраховується за методом навведених ЕРС (EMF method). Для тонких вібраторів довжиною L на відстані d він описується через інтегральні синуси (Si) та косинуси (Ci):

$$Z_{12} = j\frac{\eta I_2}{4\pi}\int_{-L/2}^{L/2}\frac{e^{-jkr}}{r}dz$$

де η~ 120π Ом — хвильовий опір вакууму, а k = 2π/ λ — хвильове число. Саме через ці складні взаємодії зміна довжини одного директора на кілька міліметрів може радикально змінити вхідний опір та діаграму спрямованості всієї системи.

Розрахунок параметрів для локалізації 100 МГц.

Для нашого прикладу з закладкою на 100 МГц (λ = 3 метри) спроектуємо 3-елементну антену з високим відношенням вперед/назад (Front-to-Back ratio).

Геометричні розміри

1. Рефлектор (L_{ref})Повинен бути на 5% довшим за диполь. L_{ref} ~ 0.5 λ = = 1.5 м.

2. Активний диполь (L_{de}): Для резонансу в присутності пасивних елементів довжина становить ~0.475 λ = 1.425 м.

3. Директор (L_{dir}): Повинен бути на 5% коротшим за диполь L_{dir}~ 0.44 λ = 1.32 м.

4. Відстань між елементами (S): Оптимальне підсилення досягається при кроці S ~ 0.2 λ = 0.6 м.

Загальна довжина несучої траверси (буму) становитиме 1.2 метра. Така антена забезпечить підсилення близько 7.2–8.5 dBi та звуження основної пелюстки до 50–60 градусів.

TinySA надає оператору унікальну можливість бачити не лише амплітуду, а й структуру сигналу під час пеленгації.

Пошук за максимумом (Peak Tracking).

Використовуючи функцію "Peak Search" на TinySA, оператор фіксує маркер на частоті 100 МГц. При повільному обертанні антени Ягі рівень RSSI на екрані буде змінюватися згідно з діаграмою спрямованості:

$$P(\theta) = P_{max} cos^n(\theta)$$

де θ — кут відхилення від осі антени. Оскільки вершина головної пелюстки зазвичай пласка, для підвищення точності використовують метод «рівносигнальних напрямків»: оператор знаходить дві точки з однаковим рівнем сигналу ліворуч і праворуч від максимуму, а потім обчислює середнє арифметичне значення кута.

Динамічне керування рівнем (Attenuation).

При наближенні до закладки на відстань 10–15 метрів, підсилення Ягі може призвести до перевантаження входу TinySA (saturation). Це проявляється як «згладжування» верхівки піка або поява гармонік. Для відновлення точності пеленгу необхідно поступово вводити внутрішній атенюатор TinySA (меню LEVEL -> ATTENUATE).

Математично, для збереження лінійності вимірювання RSSI, рівень на вході змішувача не повинен перевищувати -20 дБм. Якщо сигнал сильніший, атенюація в 10, 20 або 30 дБ дозволить TinySA знову бачити чіткий максимум при зміні кута антени.

Ефект тіні тіла.

При ручному пошуку тіло оператора діє як додатковий рефлектор або поглинач, що може деформувати діаграму спрямованості Ягі. Для мінімізації цього ефекту антена повинна бути винесена на діелектричній штанзі довжиною не менше 1 λ (3 метри) вперед, або ж оператор повинен тримати її над головою, щоб уникнути фазових спотворень від власного тіла.

Використання антени Ягі-Уда перетворює TinySA на точний пеленгатор, дозволяючи локалізувати закладку навіть в умовах щільної забудови за рахунок високої просторової селективності та можливості відсікати відбиті сигнали.

3.3 Методика застосування аналізатора спектра TinySA Ultra

Для того, щоб антенні системи працювали коректно, TinySA має бути налаштована таким чином, щоб динамічний діапазон пристрою не перевантажувався при наближенні до закладки.

Розрахунок смуги пропускання (RBW).

Для виявлення вузькосмугового сигналу закладки (девіація ~10 кГц) необхідно встановити RBW (Resolution Bandwidth) у значення 3–10 кГц. Зв'язок між рівнем шуму (Noise Floor) та RBW визначається як:

$$P_{noise}(dBm) = -174 + 10\log(RBW) + NF$$

де NF — власний коефіцієнт шуму TinySA (~15-20 дБ). Зменшення RBW підвищує чутливість системи, дозволяючи бачити закладку на більшій відстані, але сповільнює швидкість огляду спектру.

При безпосередньому наближенні до джерела (менше 5 метрів), коли сигнал досягає рівня -20 дБм, оператор повинен активувати вбудований атенюатор TinySA (Internal Attenuator) до 30 дБ. Це запобігає появі помилкових спектральних ліній (spurs), які виникають внаслідок нелінійності першого змішувача пристрою.

Комплексне використання дискоконусної антени для початкового виявлення та Ягі-Уда (або рамки) для фінальної локалізації забезпечує повний математично обґрунтований цикл радіопошуку, роблячи TinySA професійним інструментом контррозвідки.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи мною було проведено комплексне дослідження різновидів прихованих каналів витоку інформації, що функціонують на базі сучасних SDR-технологій та телекомунікаційних протоколів. Крім того, аналітичним шляхом було визначено, що перехід від апаратної логіки радіозв'язку до програмно-визначеної архітектури докорінно змінив ландшафт загроз, зробивши засоби несанкціонованого отримання інформації (ЗНОІ) більш адаптивними, скритними та доступними.

Встановлено, що класичні методи енергетичного виявлення стають дедалі менш ефективними проти сучасних сигналів з низькою ймовірністю перехоплення (LPI). Дослідження технологій пакетної передачі (Burst Transmission) та псевдовипадкового перелаштування робочої частоти (FHSS) показало, що головним фактором захисту стає часова компресія та розподіл енергії сигналу у широкій смузі спектра. Виявлено, що для детекції таких сигналів необхідне застосування спектрального аналізу в реальному часі та візуалізації типу «водоспад», що дозволяє фіксувати короткочасні аномалії, які ігноруються традиційними скануючими приймачами. Детальний аналіз протоколів мобільного зв'язку (від GSM до 5G) та IoT продемонстрував, що легітимна мережева інфраструктура сама стає середовищем для прихованої передачі даних. Виокремлено критичні вектори атак: використання стеганографії в SMS PDU та заголовках протоколів, експлуатація вразливостей сигналізації SS7/Diameter, а також застосування гібридних апаратних імплантів (на кшталт рішень з каталогу NSA ANT), які використовують архітектуру «Store-and-Forward» для обходу систем захисту периметра.

В якості прикладу та для практичного відпрацювання методик пошуку мною було спроектовано та розраховано тестовий радіопередавач на базі автогенератора Колпітца. Шляхом математичного моделювання було доведено, що використання бар'єрної ємності переходу транзистора для частотної модуляції дозволяє отримати стабільний вузькосмуговий сигнал (NFM) з девіацією близько 10 кГц, який є

типовим для простих радіозакладок і слугує ефективним еталоном для налаштування пошукового обладнання. Також мною було обґрунтовано та розраховано параметри спеціалізованих антен для різних етапів радіомоніторингу. Доведено, що для первинного виявлення оптимальною є дискоконусна антена (розрахована на нижню частоту 100 МГц), яка забезпечує широкосмуговий огляд без необхідності перелаштування. Для точної локалізації джерела спроектовано 3-елементну антену «Хвильовий канал» (Yagi-Uda) з розрахунковим підсиленням понад 7 dBi, що дозволяє реалізувати метод пошуку за максимумом сигналу. Крім того, розроблено алгоритм використання портативного аналізатора спектра TinySA Ultra для виявлення та локалізації радіозакладок. Визначено, що критичними параметрами налаштування є смуга пропускання фільтра (RBW), яку для аналізу модуляції доцільно звужувати до 3–10 кГц, та керування вхідним атенюатором для уникнення інтермодуляційних спотворень при наближенні до джерела випромінювання.

Результати даної кваліфікаційної роботи свідчать, що ефективна протидія сучасним засобам технічної розвідки вимагає переходу від використання універсальних індикаторів поля до комплексів радіомоніторингу на базі SDR. Запропонований у роботі програмно-апаратний комплекс, що складається з доступного аналізатора TinySA та розрахованих антенних систем, дозволяє з високою ймовірністю виявляти та локалізувати як прості аналогові закладки, так і складні цифрові передавачі, за умови правильного вибору тактики пошуку та параметрів обробки сигналу.

СПИСОК ЛІТЕРАТУРИ

1. *Богуш В. М., Юдін О. К.* Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення : навчальний посібник. Київ : Ліра-К, 2023. 484 с.

2. *Дудикевич В. Б.* Основи інформаційної безпеки : навчальний посібник. Львів : Видавництво Львівської політехніки, 2018. 288 с.

3. *Бурячок В. Л., Толубко В. Б.* Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Київ : ДУТ, 2015. 288 с.

4. *Басюк Т. М., Литвин В. В.* Технології захисту інформації : навчальний посібник. Львів : Видавництво Львівської політехніки, 2025. 320 с.

5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Київ : Держстандарт України, 1996.

6. *Яцків В. В., Кулина С. В.* Технічні засоби захисту інформації : опорний конспект лекцій. Тернопіль : ЗУНУ, 2023. 88 с.

7. *Collins T., Getz R., Pu D., Wyglinski A. M.* Software-Defined Radio for Engineers. Artech House, 2018. 378 p.

8. *Balanis C. A.* Antenna Theory: Analysis and Design. 4th ed. Hoboken, NJ : Wiley, 2016. 1104p.

9. *TinySA Ultra User Guide*. URL: (дата звернення: 10.05.2026).

10. *Detection of Hopper Signals (FHSS)*. Rohde & Schwarz White Paper. Munich, 2021. URL: (дата звернення: 10.05.2026).

11. *Technical Surveillance Countermeasures (TSCM)*. U.S. Department of Energy Headquarters Facilities Master Security Plan. Chapter 9. 2024.

12. *Guri M., Zadov B., Elovici Y.* PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines. *IEEE Transactions on Information Forensics and Security*. 2019. Vol. 15. P. 1879–1890.

13. *Guri M., Kedma G., Kachlon A., Elovici Y.* AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. *9th International Conference on Malicious and Unwanted Software*. Puerto Rico, USA, 2014.

14. *Guri M., Solewicz Y., Elovici Y.* MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker Communication. *IEEE Conference on Dependable and Secure Computing*. 2018.

15. *Grover M. (MG)*. O.MG Cable: Offensive MG Kit. Technical Documentation. 2019. URL: (дата звернення: 11.05.2026).

16. *Bastille Networks*. The USB O.MG Cable: Threats and Countermeasures. Bastille Research Report, 2020.

17. *Signalling Security in Telecom SS7/Diameter/5G*. ENISA Report. European Union Agency for Cybersecurity, 2018.

18. *GTP Security: Attacks and Impact*. SecurityGen Whitepaper. 2023. URL: (дата звернення: 12.05.2026).

19. *WikiLeaks*. Vault 7: CIA Hacking Tools Revealed (CherryBlossom, Elsa projects). 2017. URL: (дата звернення: 12.05.2026).

ДОДАТКИ

Антенний комплекс для виявлення слабких радіовипромінювань на базі SDR-радіоприймача

- Магістерська робота: Георгій ЧУПРІН
- Спеціальність 125 «Кібербезпека та захист інформації»
- Освітньо-професійна програма: Технічні системи інформаційного та кібернетичного захисту
- Керівник: Юрій ПЕПА, к.т.н., доцент

Актуальність теми

- Розвиток 4G/5G, IoT та SDR змінив електромагнітну обстановку і ускладнив контроль радіоефіру.
- Сучасні радіозакладки використовують LPI/LPD, FHSS і burst-передачу, тому можуть бути малопомітними для класичних сканерів.
- Ефективний технічний захист інформації потребує доступних засобів спектрального аналізу та спеціалізованих антенних систем.
- Застосування SDR і TinySA Ultra дає змогу перейти від індикаторного пошуку до керованого радіомоніторингу.

Мета, об’єкт і предмет дослідження

- Мета: підвищення ефективності виявлення та локалізації сучасних радіозакладних пристроїв.
- Засіб досягнення мети: розробка методики застосування SDR-радіоприймача та спеціалізованих антенних систем.
- Об’єкт: процес технічного захисту інформації від витоку електромагнітними каналами зв’язку.
- Предмет: методи та апаратно-програмні засоби радіомоніторингу на базі SDR-приймачів.

Завдання кваліфікаційної роботи

- Проаналізувати технічні засоби моніторингу радіоефіру та сучасні засоби негласного отримання інформації.
- Дослідити методи розпізнавання небезпечних сигналів на фоні завад.
- Розглянути SDR як базову архітектуру програмно-апаратного комплексу радіомоніторингу.
- Виконати моделювання і розрахунок параметрів дискоконусної та спрямованої антен.
- Сформувати рекомендації щодо налаштування TinySA Ultra для виявлення LPI-сигналів.

Структура роботи

- Розділ 1: аналіз методів та засобів виявлення складних радіосигналів.
- Розділ 2: дослідження вразливостей сучасних телекомунікаційних мереж та гібридних загроз.
- Розділ 3: розробка комплексу пошуку та локалізації радіозакладного пристрою на базі TinySA.
- У роботі наведено розрахунки, схеми, практичні рекомендації та висновки.
- Обсяг: 75 сторінок, 5 рисунків, 4 таблиці, 19 джерел.

Вихідна проблема технічного захисту інформації

- Радіозакладний пристрій небезпечний не лише потужністю, а насамперед складністю його виявлення.
- Сигнал може маскуватися під легітимний Wi-Fi, IoT або мобільний трафік, ховатися в шумах чи з’являтися короткими пакетами.
- Класичні індикатори поля не завжди фіксують короткочасні або розширені по спектру сигнали.
- Потрібний пошук, який оцінює частоту, рівень, часову поведінку та спектральну структуру сигналу.

Програмно-визначене радіо SDR

- SDR переносить значну частину функцій приймача з апаратного рівня на програмний.
- Сигнал з антени проходить підсилення, цифровізацію АЦП та подальшу цифрову обробку.
- I/Q-дані містять інформацію про амплітуду і фазу, що дає змогу аналізувати різні типи модуляції.
- FFT, цифрові фільтри та waterfall-відображення формують основу сучасного радіомоніторингу.

Сигнали з низькою ймовірністю перехоплення

- Burst Transmission стискає передачу в часі та зменшує вікно виявлення джерела випромінювання.
- FHSS реалізує псевдовипадкове перелаштування робочої частоти та ускладнює пеленгацію.
- LPI/LPD-сигнали розподіляють енергію по широкій смузі й можуть виглядати як підвищений шумовий фон.
- Виявлення таких сигналів потребує спектрального аналізу в реальному часі та накопичення короткочасних аномалій.

Вразливості сучасних телекомунікаційних мереж

- У роботі розглянуто вразливості мобільних мереж 2G/3G/4G/5G, IoT-протоколів та гібридних каналів.
- Легітимна мережева інфраструктура може використовуватися як середовище прихованого передавання даних.
- Стеганографія у службових полях і використання Store-and-Forward ускладнюють пряме виявлення каналу витоку.
- Тому контроль радіоефіру має поєднувати енергетичний, спектральний і поведінковий аналіз сигналів.

Моделювання тестового радіопередавача

- Для практичного відпрацювання методики пошуку розроблено модель радіозакладки на базі автогенератора Колпітца.
- Бар’єрна ємність переходу транзистора використовується для частотної модуляції.
- Сформовано вузькосмуговий NFM-сигнал з девіацією близько 10 кГц.
- Такий сигнал є типовим еталоном для перевірки налаштувань пошукового комплексу.

Дискоконусна антена для оглядового пошуку

- Дискоконусна антена використовується для первинного широкосмугового контролю ефіру.
- Розрахунок виконано для нижньої робочої частоти 100 МГц.
- Переваги антени: широкий діапазон, відсутність потреби в перелаштуванні, зручність для виявлення аномалій.
- Її застосування доцільне на першому етапі пошуку для швидкого визначення підозрілого діапазону.

Спрямована антена Yagi-Uda

- Для етапу локалізації джерела випромінювання обґрунтовано використання 3-елементної антени Yagi-Uda.
- Розрахункове підсилення понад 7 dBi забезпечує просторову селективність.
- Антена дає змогу реалізувати пошук за максимумом рівня сигналу.
- Комбінація оглядової та спрямованої антени утворює повний цикл: виявлення – уточнення – локалізація.

Налаштування TinySA Ultra

- TinySA Ultra застосовується як портативний аналізатор спектра для контролю радіоефіру.
- Для вузькосмугових сигналів рекомендовано RBW 3–10 кГц.
- Зменшення RBW знижує шумову підлогу, але збільшує час огляду спектра.
- Під час наближення до джерела необхідно вводити атенюатор, щоб уникнути перевантаження входу та хибних спектральних ліній.

Алгоритм роботи пошукового комплексу

- 1. Початковий широкосмуговий огляд ефіру дискоконусною антеною.
- 2. Фіксація підозрілих спектральних ліній, burst-імпульсів або нестандартних змін waterfall-відображення.
- 3. Уточнення частотного діапазону та параметрів RBW, span і рівня атенюації.
- 4. Перехід до спрямованої антени Yagi-Uda та локалізація джерела за максимумом сигналу.
- 5. Повторна перевірка місця розташування джерела і документування результатів пошуку.

Практичні рекомендації

- Комплексний пошук слід проводити у два етапи: оглядовий контроль і спрямована локалізація.
- Для слабких сигналів доцільно зменшувати RBW, а для сильних – вводити атенюацію.
- Оператор має враховувати відбиття, багатопроменевість, вплив власного тіла та конструктивні особливості приміщення.
- Використання TinySA Ultra з правильно підібраними антенами дозволяє підвищити ймовірність виявлення сучасних радіозакладок.

Висновки

- Проаналізовано сучасні загрози витоку інформації через слабкі та приховані радіовипромінювання.
- Показано обмеженість класичних методів пошуку щодо LPI, FHSS і burst-сигналів.
- Обґрунтовано структуру комплексу на базі TinySA Ultra, дискоконусної антени та Yagi-Uda.
- Розроблена методика підвищує ефективність виявлення і локалізації радіозакладних пристроїв на об’єктах інформаційної діяльності.