

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження ефективності застосування способів формування завадових сигналів для протидії роботі радіозакладних пристроїв»

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.

_____ Єгор ШАРАЙ

Виконав: здобувач вищої освіти групи СЗДМ-61

ШАРАЙ Єгор

Керівник: _____ ПЕПА Юрій

к.т.н., доцент

(ПРИЗВИЩЕ, Ім'я)

Рецензент: _____

(ПРИЗВИЩЕ, 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 ТСК

_____ Олександр ТУРОВСЬКИЙ

« _____ » _____ 2025 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

ШАРАЮ Єгору Володимировичу

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Дослідження ефективності застосування способів формування заводських сигналів для протидії роботі радіозакладних пристроїв».

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 2026 р. №467

2. Строк подання кваліфікаційної роботи: 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи:

Формування заводських сигналів.

Адаптивні антенні системи.

Оцінка ефективності застосування цільових способів формування завод.

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

1. Провести аналіз способів формування цільових завод.

2. Розробити математичні моделі цільових завод.

3. Оцінити ефективність формування завод для конкретних цілей.

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 четвертого розділу роботи		
6	Написання висновків по роботі		
7	Підготовка демонстраційних матеріалів		
8	Підготовка доповіді		

Здобувач вищої освіти

(підпис)

Єгор ШАРАЙ

(Ім'я, ПРІЗВИЩЕ)

Керівник роботи

(підпис)

Юрій ПЕПА

(Ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра містить: 69 стор., 9 рис., 1 табл., 15 джерел.

Таким чином, **проблема** полягає у розробці та верифікації методології, яка дозволяє максимально підвищити ефективність придушення конвенційних РЗП за рахунок оптимізації параметрів завадового сигналу та застосування спрямованого випромінювання, мінімізуючи при цьому енергетичні витрати.

Метою роботи є дослідження, розробка та кількісна оцінка ефективності застосування цільових способів формування завадових сигналів, що базуються на технологіях програмно-керованого радіо (SDR) та адаптивних антенних системах, для протидії роботі конвенційних радіозакладних пристроїв з аналоговим та цифровим випромінюванням.

Для досягнення поставленої мети визначено наступні **завдання**:

1. Провести детальний огляд та класифікацію конвенційних РЗП, включаючи їхні технічні характеристики (частотні діапазони, рівні потужності) та механізми модуляції (аналогові – АМ, ЧМ, ФМ; та цифрові – FSK, QPSK, KIM).

2. Розробити математичні моделі та проаналізувати спектральну щільність потужності (СЩП) основних типів завадових сигналів, які використовуються у РЕБ: шумоподібних, безперервної хвилі (CW) та лінійно-частотно-модульованих (Sweep).

3. Сформулювати та порівняти формалізовані критерії оцінки ефективності протидії, включаючи коефіцієнт бітових помилок (BER), співвідношення потужностей завада/сигнал (J/S) та вектор похибки модуляції (EVM).

4. Провести імітаційне моделювання впливу цільових завадових сигналів на моделі РЗП із різними типами модуляції у середовищі, що імітує реальний радіоканал (наприклад, Райса й Релея).

5. Виконати порівняльну оцінку ефективності запропонованих цільових методів протидії (CW, Sweep) проти класичних широкосмугових способів, підтверджуючи переваги цільової постановки завдань за критеріями J/S та EVM.

Об'єктом дослідження є процес забезпечення інформаційної безпеки радіоелектронних засобів в умовах протидії конвенційним радіозакладним пристроям з аналоговою та цифровою модуляцією.

Предметом дослідження є способи формування завадових сигналів та методи просторово-часової адаптації, що застосовуються для максимізації ефективності придушення РЗП за допомогою SDR-технологій.

Методи дослідження включають:

- Теоретичний аналіз: використання методів теорії статистичних рішень (критерії Байєса, Міні-макса) та теорії завадозахищеності для формалізації критеріїв ефективності.
- Математичне моделювання: застосування апарату випадкових процесів та спектрального аналізу для опису корисних та завадових сигналів.
- Імітаційне моделювання: використання програмних засобів (наприклад, MATLAB/Simulink) для симуляції радіоканалу, роботи SDR-генератора та оцінки BER/EVM під впливом завад.
- Системний підхід: розробка архітектури на основі SDR та адаптивної антенної решітки.

Наукова новизна отриманих результатів полягає у:

1. Створенні детальної, кількісної моделі впливу специфічних параметрів цільових завадових сигналів (CW та Sweep) на коефіцієнт бітових помилок та вектор похибки модуляції (EVM) конвенційних РЗП із різними типами модуляції (FSK, QPSK) в умовах багатопроменевого поширення (канал Райса й Релея).
2. Обґрунтуванні застосування SDR-технології для генерації **оптимальної спектральної щільності потужності (СЩП)** завади, що мінімізує необхідне співвідношення J/S при збереженні високого рівня придушення.

Практичне значення полягає у:

1. Наданні методологічної бази та алгоритмів для проектування високоенергоєфективних систем активного захисту інформації, здатних швидко виявляти та цілеспрямовано пригнічувати конвенційні РЗП, використовуючи SDR та адаптивні антенні решітки.

2. Розробці конкретних рекомендацій щодо вибору типу завадового сигналу (Noise, CW, Sweep) та його параметрів для ефективної протидії аналоговим та цифровим закладкам, що працюють у поширених діапазонах частот (наприклад, UHF).

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: SDR, FSK, QPSK, KIM, EVM, Sweep, CW, MATLAB/Simulink, РЕБ, КСХ.

ABSTRACT

Text part of the master's qualification work: 69 pages, 9 pictures, 1 table, 15 sources.

The problem is the development and verification of a methodology that allows maximizing the efficiency of suppressing conventional radio bugging devices by optimizing jamming signal parameters and applying directional radiation, while minimizing energy costs.

The aim of the work is the research, development, and quantitative assessment of the efficiency of applying targeted methods of forming jamming signals, based on Software-Defined Radio (SDR) technologies and adaptive antenna systems, to counter the operation of conventional radio bugging devices with analog and digital emissions.

To achieve the set goal, the following **tasks** are defined:

1. Conduct a detailed review and classification of conventional radio bugging devices, including their technical characteristics (frequency ranges, power levels) and modulation mechanisms (analog – AM, FM, PM; and digital – FSK, QPSK, PCM).
2. Develop mathematical models and analyze the Power Spectral Density (PSD) of the main types of jamming signals used in EW: noise-like, continuous wave (CW), and linear frequency modulated (Sweep).
3. Formulate and compare formalized criteria for evaluating countermeasure efficiency, including Bit Error Rate (BER), Jamming-to-Signal power ratio (J/S), and Error Vector Magnitude (EVM).
4. Conduct simulation modeling of the impact of targeted jamming signals on models of radio bugging devices with different modulation types in an environment simulating a real radio channel (e.g., Rician or Rayleigh).
5. Perform a comparative assessment of the efficiency of the proposed targeted countermeasure methods (CW, Sweep) against classic broadband methods, confirming the advantages of targeted jamming based on J/S and EVM criteria.

The **object of research** is the process of ensuring the information security of radio-electronic means under conditions of countering conventional radio bugging devices with analog and digital modulation.

The **subject of research** is the methods of forming jamming signals and space-time adaptation methods applied to maximize the efficiency of suppressing radio bugging devices using SDR technologies.

Research methods include:

- Theoretical analysis: Using methods of statistical decision theory (Bayes, Minimax criteria) and interference immunity theory to formalize efficiency criteria.
- Mathematical modeling: Application of the apparatus of random processes and spectral analysis to describe useful and jamming signals.
- Simulation modeling: Using software tools (e.g., MATLAB/Simulink) to simulate the radio channel, SDR generator operation, and assess BER/EVM under the influence of jamming.
- System approach: Developing an architecture based on SDR and an adaptive antenna array.

The **scientific novelty** of the obtained results is:

- Creating a detailed, quantitative model of the impact of specific parameters of targeted jamming signals (CW and Sweep) on the Bit Error Rate and Error Vector Magnitude (EVM) of conventional radio bugging devices with various modulation types (FSK, QPSK) under multipath propagation conditions (Rice/Rayleigh channel).
- Justifying the application of SDR technology to generate an optimal Power Spectral Density (PSD) of the interference, which minimizes the required J/S ratio while maintaining a high level of suppression.

The **practical value** is:

- Providing a methodological basis and algorithms for designing highly energy-efficient active information protection systems capable of quickly detecting and purposefully suppressing conventional radio bugging devices using SDR and adaptive antenna arrays.

- Developing specific recommendations regarding the selection of the jamming signal type (Noise, CW, Sweep) and its parameters for effectively countering analog and digital bugs operating in common frequency bands (e.g., UHF).

KEYWORDS: SDR, FSK, QPSK, KIM, EVM, Sweep, CW, MATLAB/Simulink, EW.

ЗМІСТ

ВСТУП	11
РОЗДІЛ 1 АНАЛІЗ ОБ’ЄКТА ПРОТИДІЇ ТА ОСНОВИ ФОРМУВАННЯ СИГНАЛІВ	12
1.1 Огляд принципів роботи	12
1.2 Принципи антенної теорії та фактори скритності радіозакладних пристроїв	24
РОЗДІЛ 2 ТЕОРЕТИЧНІ ОСНОВИ РЕБ ТА ФОРМУВАННЯ ЗАВАДОВИХ СИГНАЛІВ	29
2.1 Радіоелектронна боротьба (РЕБ) у контексті захисту інформації.....	29
2.2 Математичне моделювання процесів радіоелектронного придушення	33
2.3 Формалізовані критерії оцінки ефективності протидії	38
РОЗДІЛ 3 АРХІТЕКТУРА SDR, АДАПТИВНІ АНТЕННІ СИСТЕМИ ТА РЕАЛІЗАЦІЯ.....	42
3.1 SDR-архітектура як основа гнучкого генератора завад.....	42
3.2 Адаптивні антенні системи та просторово-часова обробка.....	45
РОЗДІЛ 4 МОДЕЛЮВАННЯ, ОЦІНКА ЕФЕКТИВНОСТІ ТА ПРОЕКТНІ РІШЕННЯ.....	50
4.1 Розробка імітаційного стенду та сценаріїв моделювання.....	51
4.2 Кількісний аналіз ефективності за метриками зв'язку.....	61
ВИСНОВКИ	63
ПЕРЕЛІК ПОСИЛАНЬ.....	68

ВСТУП

Актуальність теми та постановка проблеми

Забезпечення інформаційної безпеки у сучасному світі набуває критичного значення не лише у військово-технічній, але й у цивільній, корпоративній та державній сферах. Незважаючи на стрімкий розвиток складних, адаптивних засобів радіоелектронної боротьби (РЕБ), загроза витоку інформації, спричинена конвенційними, широко розповсюдженими радіозакладними пристроями (РЗП), залишається однією з найбільш актуальних. Ці пристрої, до яких відносяться приховані радіомікрофони, мініатюрні бездротові камери та пристрої для негласного знімання інформації (ЗНОІ) з ліній живлення, становлять постійну загрозу через свою доступність, малі габарити та відносну простоту встановлення.

Сучасні РЗП еволюціонують, але значна їхня частка досі використовує конвенційні методи передачі інформації, такі як **аналогова модуляція** (амплітудна (АМ), частотна (ЧМ), фазова (ФМ)), або прості *цифрові методи* (кодово-імпульсна модуляція (КИМ), частотна маніпуляція (FSK), квадратурна фазова маніпуляція (QPSK)). Такі пристрої, як правило, працюють у загальнодоступних або малоконтрольованих діапазонах частот (наприклад, UHF 430-440 МГц) з малою потужністю (до 10 мВт) або середньою потужністю (від 10 до 100 мВт).

Ефективна протидія конвенційним РЗП вимагає не просто створення широкопasmового шуму, що призводить до надмірного енергоспоживання та може бути неефективним проти цільових загроз. Критичною є необхідність переходу до **цільового формування завадових сигналів**, яке має відповідати специфічним параметрам (частоті, типу модуляції та спектральній щільності) конкретного виявленого РЗП. Це вимагає використання гнучких апаратних рішень, таких як технологія програмно-керованого радіо (SDR), та застосування адаптивних антенних систем для забезпечення просторової селективності протидії.

РОЗДІЛ 1

АНАЛІЗ ОБ'ЄКТА ПРОТИДІЇ ТА ОСНОВИ ФОРМУВАННЯ СИГНАЛІВ

Цей розділ присвячений детальному дослідженню об'єкта протидії – конвенційним радіозакладним пристроям (РЗП), які використовують аналогові та цифрові методи передачі інформації. Розуміння їхніх технічних характеристик, включаючи типи модуляції, робочі частоти, рівні потужностей та особливо приховані антенні рішення, є критично важливим для розробки ефективних стратегій радіоелектронної боротьби (РЕБ).

1.1 Огляд принципів роботи РЗП

У сучасній практиці технічного захисту інформації особливе місце посідає група об'єктів, відомих як конвенційні радіозакладні пристрої (РЗП). Цей сегмент охоплює надзвичайно широкий інструментарій для прихованого зняття даних: від мініатюрних акустичних випромінювачів (радіомікрофонів) до малогабаритних систем передачі відеозображення. Попри стрімкий розвиток широкосмугових та цифрових протоколів, традиційні РЗП залишаються актуальною загрозою завдяки своїй схемотехнічній надійності, відносній простоті реалізації та можливості тривалого функціонування у визначених частотних діапазонах.

Їхня архітектура зазвичай не передбачає складних алгоритмів шифрування чи стрибкоподібної зміни частоти, що, з одного боку, робить їх вразливими до виявлення професійними сканерами, а з іншого – забезпечує стабільну роботу в умовах щільної міської забудови або складних електромагнітних завад.

Центральним критерієм, що дозволяє структурувати цей масив спецтехніки та визначити методику їх подальшого пошуку чи нейтралізації, є спосіб трансформації інформативного сигналу (звуку або зображення) у радіочастотне коливання. В основі такої класифікації лежать фундаментальні принципи зміни параметрів несучої хвилі.

Відповідно до фізичної природи формування сигналу, виділяють такі основні типи передачі:

- амплітудна модуляція (АМ);
- частотна модуляція (ЧМ);
- фазова модуляція (ФМ).

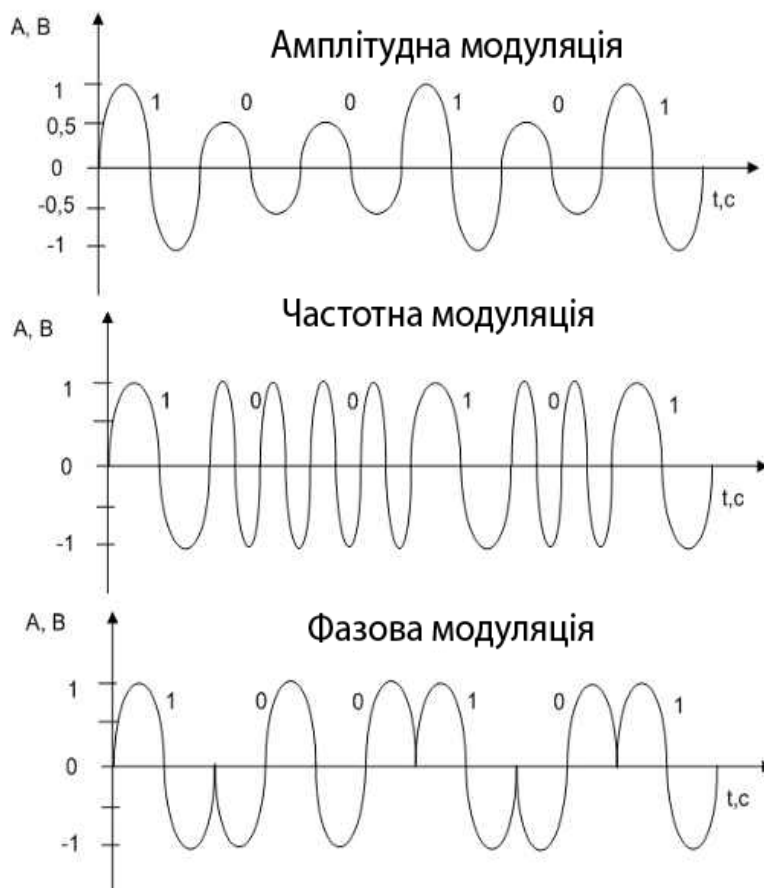


Рис. 1.1 – Види модуляцій

Кожен із цих методів визначає не лише специфіку побудови передавального модуля «закладки», а й диктує вимоги до приймального обладнання, що використовується для перехоплення або моніторингу каналу витоку інформації.

1.1.1 Аналогові РЗП: Типи модуляції та робочі параметри

Аналогові РЗП є одними з найпоширеніших засобів негласного знімання інформації, оскільки вони відносно прості у виробництві та можуть забезпечувати високу якість звуку або зображення. Вони кодують інформацію шляхом безперервної зміни параметрів несучої синусоїдальної частоти: амплітуди, частоти або фази.

Амплітудна Модуляція (АМ)

Амплітудна модуляція є історично першим і найбільш елементарним методом перетворення акустичної інформації у форму, придатну для передачі через ефір. У роботі конвенційних радіозакладних пристроїв цей метод базується на зміні потужності (амплітуди) високочастотного сигналу відповідно до коливань звукового тиску, які фіксує мікрофон.

Технічна суть та особливості реалізації

Принцип функціонування АМ полягає у накладанні низькочастотного інформаційного сигналу на високочастотну несучу хвилю. У результаті «огиначаюча» лінія отриманого радіосигналу за своєю формою повністю повторює графік звукової хвилі. Частота та фаза сигналу при цьому залишаються незмінними, що значно спрощує архітектуру як передавача, так і приймача.

Для розробників прихованих засобів зняття інформації АМ-модуляція довгий час залишалася пріоритетною через декілька ключових факторів:

- **мінімальні габарити:** схеми АМ-передавачів можуть складатися лише з кількох транзисторів та мінімального набору пасивних елементів. Це дозволяє створювати надзвичайно малі «закладки», які легко маскуються у предметах інтер'єру або офісній техніці;

- **енергоспоживання:** завдяки відсутності складних вузлів обробки сигналу, такі пристрої здатні працювати тривалий час від малогабаритних джерел живлення (дискових батарейок типу CR).

Попри свою простоту, АМ-сигнали мають низку суттєвих вад, які роблять їх легкою мішенню для фахівців із технічного захисту інформації (ТЗІ).

Чутливість до електромагнітного фону. Найбільшою проблемою амплітудної модуляції є її вразливість до будь-яких зовнішніх завад. Атмосферні розряди, робота електродвигунів, комп'ютерної техніки та побутових приладів створюють імпульсні завади, які накладаються саме на амплітуду сигналу. В результаті в отриманому аудіопотоці з'являється сильний тріск та сторонні шуми, що значно погіршують розбірливість мови.

Енергетична неефективність. Значна частина потужності АМ-передавача витрачається на трансляцію «несучої» частоти, яка сама по собі не несе корисної інформації. Це робить сигнал «помітним» у радіоефірі: навіть за відсутності звуку в приміщенні, АМ-закладка видає свою присутність потужним стабільним піком на екрані спектроаналізатора.

Легкість перехоплення. Для прослуховування такої закладки не потрібне спеціальне професійне обладнання. Будь-який побутовий радіоприймач відповідного діапазону дозволяє демодулювати сигнал без додаткових маніпуляцій, що підвищує ризик випадкового виявлення пристрою сторонніми особами.

Частотна модуляція (ЧМ або FM)

Частотна модуляція представляє собою більш досконалий етап розвитку засобів передачі даних, який дозволив суттєво підвищити надійність та інформативність каналів зв'язку. У конвенційних радіозакладних пристроях цей метод став домінуючим завдяки здатності передавати звук із високою чіткістю (Hi-Fi), що є критично важливим для ідентифікації голосів та розбору тихої мови у приміщенні.

На відміну від амплітудної модуляції, де змінюється потужність сигналу, принцип ЧМ базується на динамічному керуванні частотою несучого колювання. Амплітуда при цьому залишається стабільною, що дає передавачу змогу працювати у максимально ефективному енергетичному режимі. Будь-які зміни гучності звуку перед мікрофоном конвертуються у відхилення частоти від номінального значення. Цей процес називається девіацією.

Стійкість до зовнішніх чинників. Однією з головних переваг ЧМ є імунітет до більшості природних та техногенних завад. Оскільки більшість шумів (електричні розряди, іскріння контактів, наводки від побутової мережі) мають амплітудну природу, вони практично не впливають на частотні характеристики сигналу. Приймач просто «відсікає» будь-які колювання амплітуди, виокремлюючи лише корисну інформацію з частотних змін.

Висока вірність відтворення. ЧМ дозволяє передавати значно ширший динамічний та частотний діапазон аудіосигналу. Це мінімізує спотворення та забезпечує ефект присутності, що робить такі «закладки» ідеальним інструментом для професійного аудіоконтролю.

Попри очевидні переваги в якості звуку, використання частотної модуляції пов'язане з певними технічними компромісами, що стосуються ефективності використання радіочастотного ресурсу:

1. Проблема ширини спектра. Якщо АМ-сигнал займає досить вузьку смугу в ефірі, то ЧМ-сигнал є значно «ширшим». Це зумовлено складними математичними процесами, під час яких навколо основної частоти виникає велика кількість бічних смуг. Навіть при невеликій девіації реальна смуга пропускання, необхідна для коректної роботи радіомікрофона, виявляється у кілька разів більшою за саму частоту модуляції.

2. Щільність розміщення пристроїв. Через широкий спектр використання великої кількості ЧМ-закладок в одному об'єкті стає проблематичним. Вони починають створювати взаємні перешкоди. Для наочності: у стандартному телевізійному каналі шириною 6 МГц можна розмістити лише близько 15 незалежних аналогових FM-передавачів без ризику їхнього «перекриття».

3. Виявлення. Велика ширина спектра та характерний вигляд FM-сигналу роблять такі пристрої легко помітними для сучасних засобів радіомоніторингу. На екрані панорамного аналізатора такий сигнал виглядає як широка активна зона, яку важко сплутати з природним фоном.

Цей тип модуляції залишається «золотою серединою» для засобів середнього радіуса дії, де пріоритетом є розбірливість отриманої інформації.

Фазова Модуляція (ФМ або РМ)

Фазова модуляція представляє собою найбільш технічно витончений метод серед класичних способів маніпуляції радіосигналом. У середовищі розробників спеціальних засобів зняття інформації ФМ вважається перехідним етапом між простими аналоговими схемами та складними цифровими системами передачі

даних. Її головна особливість полягає у зміні кута (фази) несучої хвилі відповідно до змін інформаційного повідомлення, тоді як середня частота та потужність сигналу залишаються незмінними.

Фундаментальна відмінність ФМ від частотної модуляції (ЧМ) є досить тонкою, оскільки будь-яка зміна фази неминуче викликає миттєву зміну частоти, і навпаки. Проте в пристроях із фазовою модуляцією саме початковий стан фази відносно еталонного коливання стає носієм корисної інформації.

У контексті радіозакладних пристроїв ФМ обирають через її специфічні властивості:

- **підвищена завадостійкість:** як і у випадку з FM, фазова модуляція практично нечутлива до амплітудних стрибків напруги та атмосферних шумів. Проте вона демонструє ще кращі показники співвідношення «сигнал/шум» при роботі в умовах щільних радіозавад;
- **складність випадкового перехоплення:** на відміну від АМ чи ЧМ, сигнал із фазовою модуляцією неможливо коректно прослухати на звичайному побутовому приймачі. При спробі налаштуватися на таку «закладку» стандартним обладнанням, зловмисник почує лише сильно спотворений звук або хаотичний шум, що робить цей метод модуляції свого роду елементарним засобом маскування інформації.

Попри свої переваги, широке впровадження фазової модуляції у бюджетних або надмініатюрних РЗП обмежується кількома критичними факторами:

- **складність апаратної реалізації:** для коректного відновлення (демодуляції) ФМ-сигналу приймальний пристрій повинен мати еталонний генератор, синхронізований із фазою несучої частоти передавача. Це потребує складнішої схемотехніки як у самому «жучку», так і в модулі моніторингу. Найменший зсув частоти через нагрівання компонентів або рух пристрою може призвести до повної втрати зв'язку;
- **проблема неоднозначності фази:** при передачі аналогового звуку за допомогою ФМ виникають труднощі з визначенням абсолютної фази сигналу, що може призводити до специфічних спотворень (перевертання) сигналу. Це вимагає

використання додаткових схем корекції, що збільшує габарити пристрою та споживання енергії;

спектральні характеристики: як і частотна модуляція, ФМ потребує широкої смуги пропускання. Ефективне використання цього методу вимагає ретельного планування радіоефіру, оскільки некоректно налаштований ФМ-передавач може створювати значні перешкоди на сусідніх частотних каналах.

Сьогодні фазова модуляція найчастіше слугує фундаментом для переходу від аналогових до цифрових систем передачі даних, де вона трансформується у фазову маніпуляцію (PSK) – стандарт для захищених та високошвидкісних каналів зв'язку.

1.1.2 Цифрові РЗП: стандарти, модуляції та перетворення сигналу

Цифрова техніка запису і передачі даних, яка прийшла на зміну аналоговій, використовує дискретні способи модуляції, основані на дискретизації неперервних процесів як за амплітудою, так і за часом.

Аналого-цифрове перетворення (АЦП)

Ключовим елементом цифрових РЗП є аналого-цифровий перетворювач (АЦП), який приймає вхідний аналоговий сигнал (напругу) та генерує відповідний цифровий сигнал (двійковий код), придатний для подальшої цифрової обробки та передачі.

Характеристики АЦП: якість перехопленої інформації безпосередньо залежить від розрядності АЦП (наприклад, 10, 12, 14, 16, 18 або 24 біт) та частоти дискретизації (наприклад, 44.1кГц або 100МГц). Чим вища розрядність, тим точніше квантування та кодування вхідного сигналу.

Типи АЦП: до поширених методів перетворення належать АЦП за методом послідовного підрахунку, безпосереднього зчитування та порозрядного зрівноваження. Еволюція радіозакладних пристроїв призвела до поступового витіснення класичних аналогових методів передачі цифровими протоколами. Основна перевага цифрового підходу полягає не лише у можливості шифрування контенту, а й у значному підвищенні стійкості до завад та можливості стиснення даних. Процес передачі інформації у таких системах складається з двох етапів:

перетворення безперервного звукового коливання у бінарний потік та подальша радіочастотна маніпуляція несучої для трансляції цього потоку в ефір.

Кодово-імпульсна модуляція (KIM / PCM)

Кодово-імпульсна модуляція є фундаментальним етапом оцифрування звуку, що передуює безпосередній передачі по радіоканалу. Це процес перетворення аналогового сигналу, отриманого з мікрофона, у послідовність цифрових значень.

Технічний цикл KIM базується на трьох послідовних операціях:

- **Дискретизація:** вимірювання амплітуди звукової хвилі через чітко визначені проміжки часу.

- **Квантування:** округлення отриманих значень до найближчого рівня з фіксованої сітки амплітуд.

- **Кодування:** перетворення кожного рівня у двійкове число (біт).

У професійних РЗП параметри KIM (частота дискретизації та розрядність) підбираються таким чином, щоб забезпечити баланс між розбірливістю мови та обсягом даних. Висока розрядність дозволяє зафіксувати найдрібніші акустичні нюанси, проте вимагає потужнішого передавального тракту.

Частотна маніпуляція (FSK та GFSK)

Frequency Shift Keying (FSK) є найбільш поширеним методом цифрової модуляції у бюджетних та середньоцінових радіозакладках. На відміну від аналогової ЧМ, де частота змінюється плавно, у FSK відбувається стрибкоподібне перемикання між двома (або більше) фіксованими частотами, кожна з яких відповідає логічному «0» або «1».

Сучасні пристрої частіше використовують вдосконалений варіант – GFSK (Gaussian Frequency Shift Keying). У цьому методі перед маніпуляцією сигнал проходить через гауссівський фільтр, який «згладжує» моменти переходу між частотами. Це дає декілька критичних переваг:

- **Звуження спектра:** сигнал займає меншу смугу в ефірі, що ускладнює його виявлення на фоні широкосмугових завад.
- **Зниження побічних випромінювань:** пристрій менше «смітить» у сусідніх діапазонах, що підвищує його скритність.

Попри те, що історично FSK асоціюється з низькими швидкостями передачі, сучасні РЗП на базі енергоефективних мікроконтролерів здатні передавати дані на швидкостях у сотні кілобіт на секунду, що цілком достатньо для трансляції якісного аудіопотоку в реальному часі.

Квадратурна фазова маніпуляція (QPSK)

QPSK (Quadrature Phase Shift Keying) представляє сегмент високих технологій у сфері радіомоніторингу. Цей метод базується на зміні фази несучого сигналу, де за один такт передачі (символ) передається одночасно два біти інформації. Це досягається шляхом використання чотирьох можливих станів фази, зміщених один відносно одного на 90 градусів.

Основні характеристики QPSK у контексті спеціальної техніки:

- **висока спектральна ефективність:** здатність передавати великі обсяги даних (наприклад, стиснене відео або багатоканальний звук) у вузькій смузі частот;
- **складність аналізу:** сигнал QPSK за своїми характеристиками нагадує білий шум. Без знання конкретного алгоритму синхронізації та параметрів «сузір'я» фаз, перехоплений сигнал практично неможливо відрізнити від ефірного фону або завад цифрового мовлення;
- **вимогливість до обладнання:** реалізація QPSK потребує значних обчислювальних потужностей для обробки сигналів у реальному часі, що раніше обмежувало мініатюризацію таких пристроїв. Проте сучасна елементна база дозволяє розміщувати QPSK-передавачі у корпусах розміром з монету.

Сучасна концепція побудови радіозакладних пристроїв (РЗП) все частіше відходить від використання унікальних закритих частот на користь загальнодоступних бездротових стандартів. Це зумовлено не лише здешевленням елементної бази, а й стратегічною перевагою: сигнали таких пристроїв «розчиняються» у щільному трафіку міських мереж, що робить їх ідентифікацію стандартними методами радіоконтролю надзвичайно складною.

Високошвидкісні мережі Wi-Fi (IEEE 802.11)

Використання Wi-Fi у засобах спеціального призначення обумовлене насамперед необхідністю передачі великих обсягів даних у реальному часі, наприклад, потокового відео високої чіткості або багатоканального звуку без стиснення. Працюючи переважно у діапазоні 2,4 ГГц (рідше 5 ГГц), такі «закладки» використовують стандартні стекові протоколи, що дозволяє їм підключатися до наявних точок доступу на об'єкті та передавати інформацію безпосередньо через інтернет-шлюзи.

Головним обмеженням Wi-Fi залишається значне енергоспоживання, спричинене складністю підтримання активної сесії та високою піковою потужністю передавача. Через це Wi-Fi-модулі рідко зустрічаються в автономних мініатюрних пристроях. Найчастіше вони інтегруються в об'єкти, що мають постійне живлення від мережі 220В (подовжувачі, побутова техніка, настільні лампи). Крім того, класична топологія Wi-Fi («зірка») вимагає наявності центрального роутера, що обмежує гнучкість розгортання мережі у специфічних умовах.

Спеціалізовані мережі ZigBee (IEEE 802.15.4)

Стандарт ZigBee представляє іншу філософію – максимальну автономність та живучість мережі. Це ідеальний інструмент для створення розгалужених систем моніторингу на великих об'єктах. Ключовою особливістю ZigBee є підтримка **Mesh-архітектури** (комірчастої топології), де кожен окремий пристрій може виступати як ретранслятор для сусідніх вузлів.

Такий підхід надає низку критичних переваг для прихованого збору даних:

- **збільшення дистанції:** дані від віддаленої «закладки» можуть передаватися ланцюжком через інші пристрої до приймального пункту, що знаходиться далеко за межами зони прямої видимості;
- **енергонезалежність:** завдяки оптимізованим протоколам передачі та режимам глибокого сну, ZigBee-пристрої здатні функціонувати роками від однієї літієвої батареї;

- **стійкість системи:** вихід з ладу одного вузла не призводить до розриву зв'язку – мережа автоматично переконфігурується та знаходить новий маршрут для пакетів даних.

Технологія Bluetooth та BLE (Bluetooth Low Energy)

Bluetooth, особливо у його сучасній ітерації **Low Energy (BLE)**, займає нішу надмалих пристроїв короткого радіуса дії. Основна ставка тут робиться на повну інтеграцію в екосистему мобільних пристроїв. BLE-закладки часто використовуються для короткочасного зняття інформації або як «маячки» для фіксації переміщення персоналу.

Низька потужність сигналу Bluetooth є одночасно і слабкістю, і перевагою. З одного боку, це обмежує радіус дії декількома десятками метрів, але з іншого – робить сигнал майже невидимим за межами конкретного приміщення. Сучасні РЗП на базі Bluetooth можуть використовувати режими «імпульсної» передачі (burst transmission), накопичуючи аудіодані у внутрішній пам'яті та скидаючи їх на приймач (наприклад, смартфон, що знаходиться у кишені кур'єра, який проходить повз) за лічені секунди.

1.1.3. Ефективність функціонування РЗП

Визначається двома критичними параметрами: вихідною потужністю передавача та обраним частотним діапазоном. Ці характеристики перебувають у постійному антагонізмі: збільшення дальності передачі автоматично підвищує ризик виявлення пристрою засобами радіомоніторингу через зростання щільності потоку енергії та специфічного теплового випромінювання.

В основу поділу РЗП за потужністю покладено здатність сигналу долати загасання у вільному просторі та через перешкоди (стіни, перекриття). Згідно з законом зворотних квадратів, потужність сигналу P_r на відстані d зменшується пропорційно квадрату відстані:

$$P_r \propto \frac{P_t}{d^2} \quad (1)$$

де P_t – потужність передавача.

Класифікація РЗП за потужністю:

1. Малопотужні пристрої (до 10 мВт).

Цей клас орієнтований на максимальну скритність. Такі «закладки» призначені для трансляції даних у межах одного приміщення або на невеликі відстані (до 30-50 метрів) до ретранслятора. Завдяки низькому енергоспоживанню вони мають найменші габарити та мінімальний тепловий слід, що робить їх майже невидимими для простих нелінійних локаторів та теплові зорів;

2. Засоби середньої потужності (10-100 мВт).

Найбільш розповсюджена категорія конвенційних пристроїв. Вони забезпечують стабільний зв'язок у радіусі 100-300 метрів в умовах міської забудови. Така потужність дозволяє впевнено приймати сигнал на пост моніторингу, розташований у сусідній будівлі або в автомобілі;

3. Високотужні випромінювачі (понад 100 мВт)

Використовуються у випадках, коли приймальний пункт значно віддалений від об'єкта. Головним недоліком є високий рівень демаскування: потужний сигнал легко локалізується навіть бюджетними індикаторами поля, а інтенсивна робота передавача спричиняє нагрівання корпусу «закладки».

Вибір частотного діапазону та спектральне маскування

Вибір робочої частоти визначає не лише фізичні розміри антени, а й здатність сигналу «ховатися» серед легітимного радіотрафіку.

- VHF-діапазон (30-300 МГц): традиційно використовується для трансляції аналогового звуку. Хвилі цього діапазону мають гарну огинальну здатність, що дозволяє сигналу проходити крізь значні масиви залізобетону. Проте велика довжина хвилі вимагає довгих антен (від 25 до 75 см), що ускладнює прихований монтаж у малих предметах;

- UHF-діапазон (300 МГц-3 ГГц): є найбільш пріоритетним для сучасних РЗП. Використання частот у районі 433,05-434,79 МГц (LPD-діапазон) або 868 МГц дозволяє зловмисникам видавати сигнал «закладки» за роботу звичайних радіостанцій, автомобільних сигналізацій або датчиків розумного дому. Малі

розміри антен (кілька сантиметрів) сприяють ідеальній інсталяції всередині офісної техніки.

Передача даних через провідні комунікації

Окрему категорію становлять пристрої, що використовують фізичні лінії (електромережу 220В, телефонні лінії, пожежну сигналізацію) як середовище поширення сигналу.

Такі РЗП накладають високочастотну складову (зазвичай у межах 40-500 кГц) на стандартну синусоїду напруги мережі. Це дозволяє передавати аудіоінформацію за межі контрольованого приміщення без випромінювання у радіоефір. Виявлення таких засобів потребує використання спеціальних аналізаторів провідних ліній, оскільки звичайні радіосканери тут безсилі. Ефективною протидією у цьому випадку є встановлення спеціалізованих фільтрів, що блокують проходження ВЧ-сигналів за межі захищеного контуру живлення.

1.2 Принципи антенної теорії та фактори скритності радіозакладних пристроїв

Ефективність функціонування будь-якого радіозакладного пристрою (РЗП) визначається не лише потужністю його передавача чи якістю мікрофона, а насамперед здатністю антенної системи трансформувати енергію високочастотних коливань у випромінювання. У контексті технічної розвідки антена є найбільш критичним елементом: її параметри безпосередньо впливають на дальність передачі даних, енергоспоживання пристрою та, що найважливіше, на його фізичну скритність.

Методи маскування антенних систем

Щоб нівелювати демаскувальний фактор антени, застосовуються декілька інженерних стратегій:

- **Перехід у мікрохвильовий діапазон (UHF та вище):** зі збільшенням частоти до 2,4 ГГц або 5 ГГц необхідний розмір антени зменшується до декількох сантиметрів або навіть міліметрів. Це дозволяє використовувати друковані антени

(Microstrip Antennas), виконані безпосередньо на друкованій платі пристрою у вигляді доріжок складної конфігурації (F-подібні або змієподібні антени).

- **Використання паразитних випромінювачів:** у багатьох РЗП роль антени виконують наявні провідні комунікації об'єкта. Це можуть бути дроти живлення, шнури підключення побутової техніки або металеві елементи конструкції інтер'єру. Такий підхід робить антену «невидимою» для візуального огляду, проте часто створює проблеми з узгодженням імпедансів.

- **Електричне вкорочення та подовжувальні котушки:** якщо габарити пристрою не дозволяють розмістити повнорозмірну антену, використовують індуктивне навантаження. Це дозволяє фізично зменшити дріт антени, зберігши його резонансні властивості на потрібній частоті. Проте платою за мініатюризацію є суттєве звуження смуги пропускання та падіння ККД випромінювання.

1.2.1. Мініатюрні та приховані антени для РЗП

Мініатюрні антени для РЗП повинні бути низькопрофільними, компактними та, бажано, інтегрованими в корпус пристрою або навколишнє середовище.

Планарна інвертована F-антена (PIFA)

PIFA є однією з найбільш популярних конструкцій для портативних і мініатюрних пристроїв, включаючи РЗП.

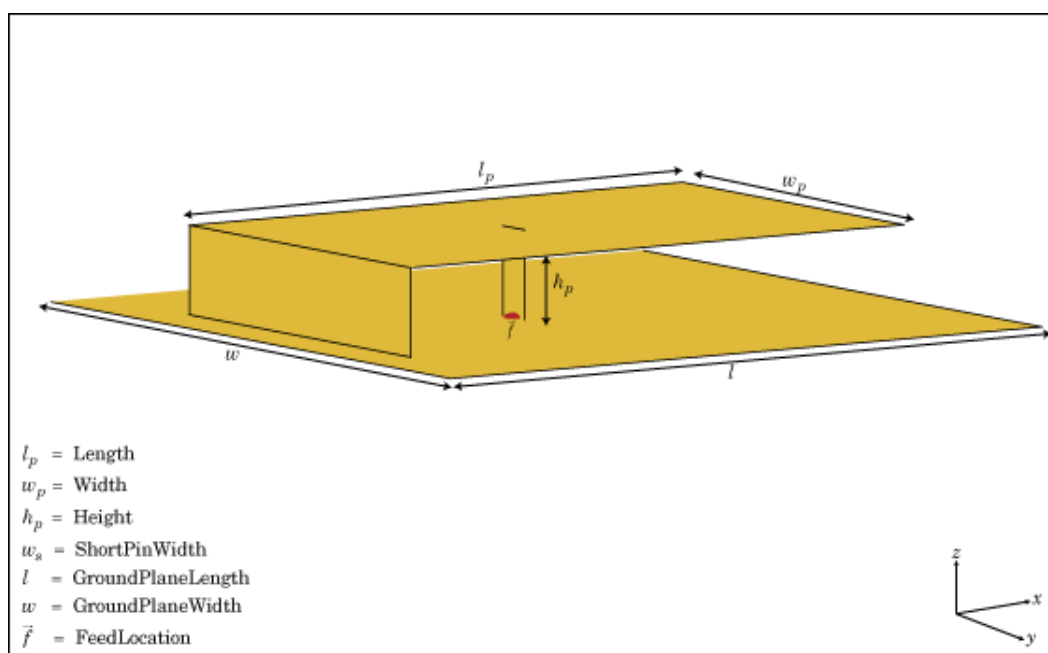


Рис. 1.2 – Планарна інвертована F-антена (PIFA)

Конструкція та переваги: PIFA розвинулася з чвертьхвильової монопольної антени. Вона характеризується простою конструкцією, низьким профілем (конформністю) та невеликою вагою. Низький профіль є ключовою перевагою для прихованого монтажу.

Характеристики: робоча частота PIFA визначається її розмірами (довжина, ширина, висота верхньої пластини) та розмірами земляної площини.

Інвертована F-антена (IFA)

Базова IFA використовує дріт або вузьку смужку як випромінювальний елемент, підключений до земляної площини через елемент короткого замикання.

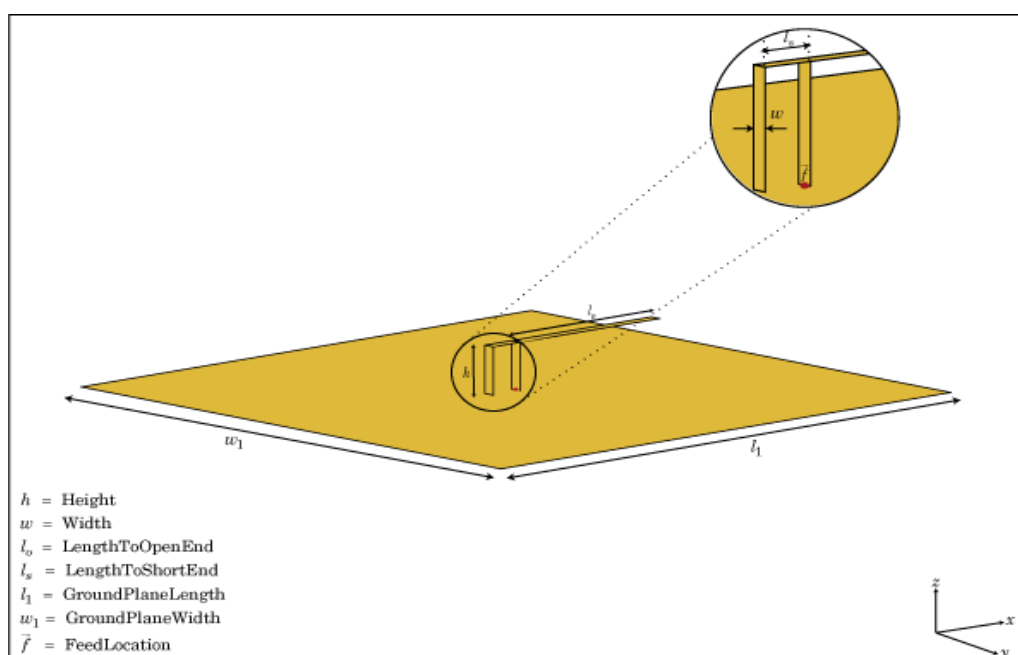


Рис. 1.3 – Інвертована F-антена (IFA)

Відмінності від PIFA: IFA зазвичай має більш вузьку смугу пропускання порівняно з PIFA. Хоча IFA може бути дуже компактною, вона може виступати з пристроєм, що погіршує прихованість. Діаграма спрямованості IFA часто є більш спрямованою, ніж PIFA.

Мікросмушкові (Microstrip) антени

Мікросмушкові антени (або друковані антени) також є популярним рішенням для низькопрофільних застосувань, оскільки вони мають плоску та компактную конструкцію, що дозволяє легко інтегрувати їх у друковані плати РЗП.

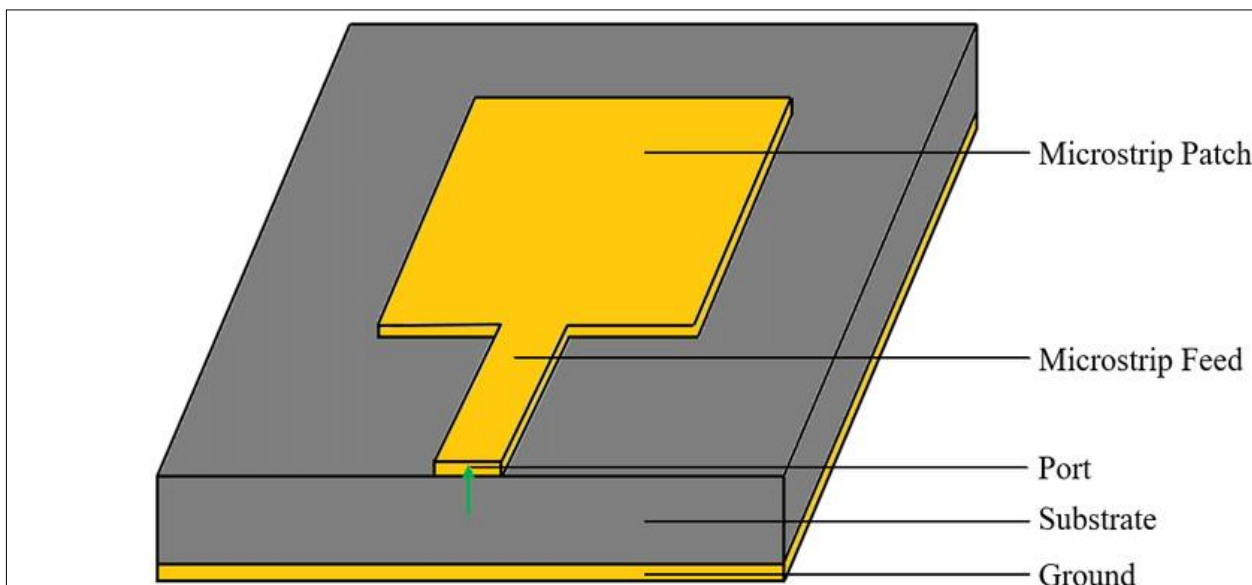


Рис. 1.4 – Мікросмужкова (Microstrip) антена

Особливості: незважаючи на переваги у мініатюризації, мікросмужкові антени, як правило, мають вузьку смугу пропускання та створюють невеликий коефіцієнт підсилення. Збільшення ширини смуги пропускання та підсилення вимагає оптимізації конструкції, наприклад, збільшення висоти підкладки або довжини випромінювального елемента.

1.2.2. Параметри антен: Діаграма направленості та КСХ

Аналіз антенних параметрів РЗП є ключем до виявлення його присутності та розробки ефективної контрзавади.

Діаграма Направленості (ДН)

ДН графічно відображає напрямок та інтенсивність випромінювання електромагнітного поля.

Прихованість: РЗП часто використовують антени максимально всеспрямованні або широкою ДН, щоб уникнути втрати сигналу незалежно від орієнтації пристрою. Однак приховані антени, такі як IFA, можуть мати більш спрямований характер, що є вразливістю. Знання ДН дозволяє системам РЕБ використовувати спрямовані антени для максимально ефективного придушення сигналу РЗП.

Коефіцієнт Стоячої Хвилі (КСХ)

КСХ (VSWR – Voltage Standing Wave Ratio) є показником, що визначає якість узгодження навантаження (антени) з лінією живлення (фідером). КСХ є співвідношенням між максимальною та мінімальною амплітудами напруги (або струму) стоячої хвилі .

Критичність для РЗП: ідеальне узгодження ($КСХ=1$) означає відсутність відбитої потужності та максимальну передачу енергії. Високий КСХ вказує на погане узгодження, що призводить до втрати потужності та перегріву. Високий КСХ також може бути ознакою несправності або поганого налаштування антени РЗП, що може бути використано для його виявлення. Висока якість узгодження (низький КСХ) є важливою для РЗП, щоб максимізувати ефективну випромінювану потужність (EIRP) та мінімізувати втрати.

Таким чином, конвенційні РЗП покладаються на поєднання відносно простих, але стійких аналогових або цифрових модуляцій, що працюють у поширених радіодіапазонах, та мініатюрних антенних рішень, які забезпечують прихованість за рахунок фізичного розміру, але часто мають компроміси у пропускній спроможності та коефіцієнті підсилення. Ця комбінація технічних характеристик є цільовою основою для розробки адаптивної системи протидії.

РОЗДІЛ 2

ТЕОРЕТИЧНІ ОСНОВИ РЕБ ТА ФОРМУВАННЯ ЗАВАДОВИХ СИГНАЛІВ

Цей розділ закладає фундаментальну теоретичну базу для дослідження, детально розглядаючи принципи та методи радіоелектронної боротьби (РЕБ), а також математичний апарат, необхідний для моделювання та кількісної оцінки ефективності протидії конвенційним радіозакладним пристроям (РЗП).

2.1. Радіоелектронна боротьба (РЕБ) у контексті захисту інформації

Розглядається як сукупність цілеспрямованих заходів, що базуються на застосуванні електромагнітної енергії для деградації або повного припинення функціонування несанкціонованих каналів зв'язку. Основною метою завадового впливу є створення таких умов у радіоефірі, за яких виокремлення корисного сигналу РЗП стає технічно неможливим або економічно недоцільним через критичні спотворення даних.

Успішна нейтралізація засобів зняття інформації вимагає суворого узгодження завад за частотним спектром, часовими інтервалами та просторовими координатами. Це дозволяє сконцентрувати енергію протидії саме на вразливих вузлах «закладки», мінімізуючи при цьому вплив на легітимні системи зв'язку об'єкта.

2.1.1. Класифікація завад за характером впливу

За характером впливу на приймач РЗП завади поділяються на дві основні групи:

Пригнічуючі (Suppressing Jamming)

Ці завади мають на меті енергетичне придушення або створення перешкод на визначених частотах. Вони порушують функціонування РЕЗ шляхом перевантаження вхідних каскадів приймача або підвищення рівня шуму, роблячи неможливим виділення корисного сигналу. До них відносяться:

- **широкосмугове придушення:** забезпечує глушіння всіх частот у певному діапазоні (загороджувальна завада), що є енергетично витратним, але ефективним проти невідомих часто;

- **прицільне (цільове) придушення:** націлене безпосередньо на відому несучу частоту РЗП. З точки зору енергії, прицільні за частотою завади є більш ефективними.

Імітуючі / Обманні (Deceptive Jamming)

Ці завади створюють фальшиві радіосигнали. Хоча цей тип завад частіше використовується для дезорієнтації радарів або систем навігації (наприклад, GPS-обман), він може бути застосований і для створення хибних сигналів присутності в каналі РЗП.

2.1.2. Концепція цільового та широкосмугового заваджування

Вибір між широкосмуговою та цільовою завадою визначається апріорною інформацією про РЗП.

Широкасмугова завада є універсальним інструментом в арсеналі засобів активного радіоелектронного захисту, що застосовується в умовах високої апріорної невизначеності щодо параметрів загрози. Основним призначенням такого впливу є створення суцільного «шумового бар'єру» у визначеному діапазоні частот, що робить неможливим функціонування будь-яких приймально-передавальних пристроїв, незалежно від їхньої схемотехнічної складності.

На відміну від вузькосмугових методів, широкосмугова завада не намагається імітувати структуру сигналу «закладки». Її завдання – максимально підвищити рівень шуму в каналі зв'язку, щоб відношення сигналу до завади на вході приймача зловмисника впало нижче критичного порогу декодування.

Для генерації такого впливу використовують два основні підходи:

- **аналоговий «білий шум»:** формується шляхом посилення природних флуктуаційних шумів напівпровідникових елементів. Такий сигнал має рівномірну спектральну щільність потужності у широкому діапазоні. Оскільки він має максимальну ентропію, його практично неможливо відфільтрувати за допомогою

алгоритмів цифрової обробки сигналів, що робить його вкрай ефективним проти класичних аналогових ЧМ та АМ пристроїв;

- **дискретні псевдовипадкові послідовності (ПВП)**: генеруються цифровими синтезаторами та представляють собою високошвидкісні потоки хаотичних імпульсів. Такі завади ідеально підходять для деградації цифрових каналів передачі даних (Wi-Fi, Bluetooth), оскільки вони руйнують часову та фазову синхронізацію пакетів.

Найбільш критичною сферою застосування широкосмугових завад є нейтралізація РЗП, що використовують **псевдовипадкову перебудову робочої частоти (ППРЧ)**. Оскільки такі «закладки» змінюють частоту сотні або тисячі разів на секунду, прицільне придушення кожної окремої частоти є технічно надскладним завданням, що потребує миттєвої радіорозвідки.

Широкосмугова завада вирішує цю проблему шляхом «заливання» енергією всього частотного вікна, у якому здійснюється перебудова. Таким чином, куди б не «стрибнув» сигнал РЗП, він скрізь зустрічає високий рівень шумового фону, що призводить до постійної втрати інформаційних пакетів та повної зупинки передачі.

Попри свою універсальність, широкосмуговий метод має фундаментальне обмеження, пов'язане з розподілом енергії. Ключовим параметром тут є **спектральна щільність потужності (S_0)**, яка визначається як відношення повної потужності передавача (P_{total}) до ширини смуги завади (ΔF):

$$S_0 = \frac{P_{total}}{\Delta F} \quad (2.1)$$

З цієї формули випливає основний недолік методу: при фіксованій потужності генератора кожне розширення смуги завади призводить до пропорційного зменшення її «ударної сили» на кожному конкретному герці частоти. Це породжує низку проблем:

- **надмірне енергоспоживання**: для створення ефективного рівня придушення у широкій смузі (наприклад, 2,4-5 ГГц) потрібні передавачі великої

потужності, що призводить до значних габаритів систем РЕБ та необхідності інтенсивного охолодження;

- **низька вибірковість:** широкосмугова завада однаково ефективно пригнічує як ворожі «жучки», так і легітимні системи зв'язку об'єкта (корпоративні мережі, мобільні телефони співробітників, бездротові гарнітури). Це створює проблему електромагнітної несумісності (ЕМС) та потребує ретельного планування зон використання завад;

- **радіолокаційна помітність:** потужне широкосмугове випромінювання є ідеальним орієнтиром для засобів радіотехнічної розвідки зловмисників. Факт роботи такої системи захисту неможливо приховати, що може опосередковано вказувати на високу важливість інформації, яка обговорюється в приміщенні.

Цільова завада застосовується, коли частота РЗП відома. Завади можуть бути прицільними за несучою частотою, за шириною спектру або за частотою модуляції.

Прицільна завада є найбільш інтелектуальним та енергетично вигідним інструментом у системі радіоелектронної протидії. Її застосування базується на принципі вибіркового впливу, коли параметри завадового сигналу максимально адаптуються під характеристики конкретного виявленого каналу витоку інформації. На відміну від загороджувального методу, прицільне придушення вимагає попереднього етапу детальної радіорозвідки для точного визначення робочої частоти та типу модуляції РЗП.

Успішна нейтралізація РЗП за допомогою прицільного впливу передбачає узгодження завади за кількома критичними параметрами:

- **прицілювання за несучою частотою:** центр спектра завади суміщається з центральною частотою передавача «закладки». Це забезпечує пряме попадання енергії у смугу пропускання приймача зловмисника;

- **узгодження за шириною спектра:** ширина завадового сигналу вибирається рівною або дещо більшою за смугу пропускання цільового сигналу (наприклад, 200 кГц для широкосмугової ЧМ або декілька МГц для цифрових стандартів). Це дозволяє не «розпорошувати» потужність на порожні ділянки ефіру.

- **модуляційне придушення**: якщо відомий алгоритм модуляції (наприклад, фазова маніпуляція), завада може формуватися таким чином, щоб руйнувати конкретні вузли синхронізації або алгоритми корекції помилок у цифровому потоці.

Головною перевагою прицільної завади є максимізація **спектральної щільності потужності (СЩП)**. Якщо широкосмугова завада розподіляється на сотні мегагерц, то прицільний генератор фокусує весь свій потенціал у вузькому вікні.

Стійкість до похибок суміщення спектрів

Важливим практичним аспектом є допустима похибка прицілювання Δf . Теоретичні дослідження та польові випробування показують, що прицільна завада зберігає свою ефективність навіть при неідеальному збігу частот. Якщо зміщення спектра завади відносно сигналу не перевищує 10-15% від ширини смуги пропускання приймача РЗП, імовірність повного придушення каналу залишається практично незмінною.

Ця властивість робить прицільні завади життєздатними навіть в умовах нестабільності частоти бюджетних РЗП, де несуча може «плавати» через нагрівання компонентів або розрядження батареї. Сучасні адаптивні системи РЕБ використовують алгоритми «автопідстроювання», які постійно аналізують ефір і коригують частоту завади вслід за дрейфом сигналу «закладки».

2.2 Математичне моделювання процесів радіоелектронного придушення

Математичне моделювання процесів радіоелектронного придушення є фундаментом для переходу від емпіричного підбору параметрів РЕБ до науково обґрунтованого прогнозування ефективності захисту. Воно дозволяє не лише кількісно описати деструктивний вплив на приймальний тракт РЗП, а й оптимізувати енергетичні витрати системи протидії. В основі такого моделювання лежить аналіз спектральної щільності потужності (СЩП) – характеристики, що визначає розподіл енергії завади у частотній області.

2.2.1 Загальна модель сигналу у приймачі РЗП

Вхідний сигнал $X(t)$, що надходить на приймач, складається з корисного сигналу $A(t)$ та завадової компоненти $W_{\mu\nu}(t)$, яка може включати як природний шум, так і спеціально створену заваду. Коливання $W_{\mu\nu}(t)$ є нормально флуктуаційним коливанням з постійною інтенсивністю та частотами від T/μ до T/ν .

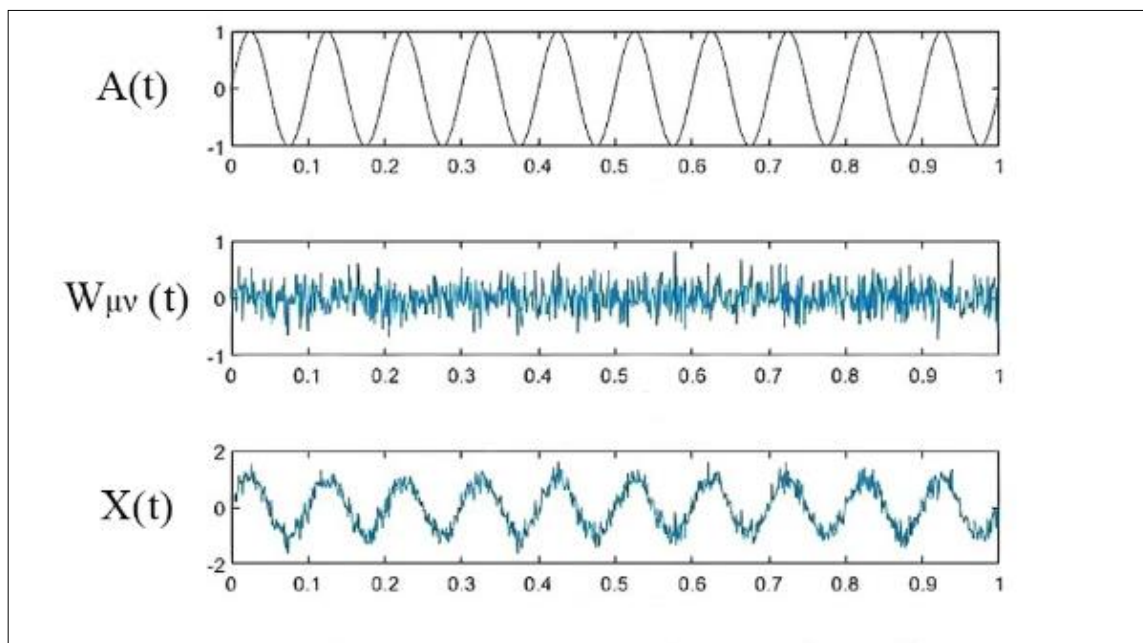


Рис. 2.1 – Моделювання вхідного сигналу $X(t)$

У дискретному вигляді, прийнятий сигнал x_{kl} на вході приймача, з урахуванням шуму та завади, може бути змодельований наступним чином:

$$x_{kl} = a_{kl} \cdot \theta_l + \delta \cdot T \quad (2.2)$$

де:

$a_{kl} \cdot \theta_l$ – складова, пов'язана з корисним сигналом $A(t)$;

θ_l – випадковий параметр, що змінюється від досліду до досліду;

$\delta \cdot T$ – складова, пов'язана з флуктуаційним шумом або завадою $W_{\mu\nu}(t)$.

Ця модель дозволяє визначити умови, за яких приймач РЗП буде відтворювати повідомлення з помилками, шляхом аналізу впливу завади $W_{\mu\nu}(t)$, яка повністю визначається своїми координатами $x_1, x_2, \dots, x_{l+1}$.

2.2.2 Моделювання шумоподібної завади

Шумоподібна завада є найбільш універсальним типом пригнічуючої завади. Її вплив на приймач оцінюється через спектральну щільність потужності (СЩП).

Спектральна Щільність Потужності (СЩП)

СЩП $\sim (2\pi f)$ визначає розподіл потужності завади по частотах. Для широкосмугового білого шуму (White Noise) СЩП є постійною величиною у всьому частотному діапазоні, тоді як для смугово-обмеженого (Band-Limited) білого шуму вона обмежена певним діапазоном частот.

Загалом, СЩП $\sim (2\pi f)$ може бути апроксимована як $\sim (2\pi f_c) \approx P_{f1,f2}$ у центрі смуги.

Аналіз показав, що збільшення спектральної щільності потужності модулюючої шумової напруги призводить до того, що необхідний рівень правильної оцінки повідомлення досягається при вищих відношеннях сигнал/шум. І навпаки, мала СЩП потужності завад (обернено пропорційна ширині спектру завади) означає низьку ефективність придушення.

Алгоритмічні аспекти генерації (SDR/DSP)

Для реалізації широкосмугової шумової завади в SDR-системі використовується цифрове формування сигналу. Генерація смугово-обмеженого гаусового шуму (Band-Limited White Noise) у цифровому процесорі (DSP) відбувається шляхом генерації білого шуму (випадкових чисел з нормальним розподілом).

Застосування цифрової фільтрації (наприклад, КІХ-фільтра FIR filter) для обмеження спектру шуму необхідною шириною смуги, наприклад, до половини частоти Найквіста.

Вихідна потужність шуму (Noise power) у блоці "Band-Limited White Noise" відповідає висоті СЩП.

2.2.3 Моделювання завади Безперервної Хвилі (CW)

Завада Безперервної Хвилі (Continuous Wave, CW) – це вузькосмуговий прицільний тон на фіксованій частоті. Це є класичним прикладом цільового заваджування.

З фізичної точки зору, ідеальна CW-завада описується гармонічним коливанням:

$$J(t) = A_J \cos(2\pi f_J t + \theta_J) \quad (2.3)$$

де A_J – амплітуда;

f_J – частота завади;

θ_J – початкова фаза.

У реальних умовах сигнал може мати паразитну амплітудну або частотну модуляцію, зумовлену нестабільністю генератора, однак для цілей моделювання часто припускають ідеальну синусоїду. Ключовою особливістю є те, що цей сигнал не несе корисної інформації для приймача, а його фаза θ_J зазвичай є випадковою величиною відносно корисного сигналу, рівномірно розподіленою на інтервалі $[0, 2\pi)$. Ця некогерентність є критичним фактором, який визначає характер взаємодії завади з сигналом у змішувачах та детекторах приймача.

Модель: CW-сигнал описується синусоїдою на фіксованій частоті f_{CW} з певною амплітудою.

Ефективність проти FSK/ЧМ: аналітичні розрахунки та симуляції підтверджують, що CW-тон навіть із потужністю, меншою за потужність корисного сигналу, може спричинити значну кількість помилок (високу ймовірність помилки P_{err}) для систем, що використовують частотну маніпуляцію (FSK) або частотну модуляцію (ЧМ), особливо при певних зсувах несучої частоти. Це підкреслює високу ефективність цільового енергетичного придушення.

2.2.4. Моделювання Свіп-завади (Linear Sweep Jamming)

Свіп-завада (Linear Sweep Jamming), або лінійно-частотно-модульований сигнал (ЧМ-сигнал), відомий як «чирп» (Chirp), використовується для послідовного пригнічення кількох вузькосмугових каналів у широкому діапазоні.

Часова функція та фаза

Завадовий сигнал $y_{chirp}(t)$ у часовій області може бути визначений через його фазову функцію $\psi(t)$:

$$y_{chirp}(t) = \cos(\psi(t) + \phi_0) \quad (2.5)$$

де ϕ_0 – початкова фаза.

Фазова функція лінійного свіпа

Для лінійного свіпа (чирпа) фазова функція $\phi(t)$ описується квадратичною залежністю від часу, оскільки миттєва частота змінюється лінійно:

$$\phi(t) = 2\pi \cdot \left(f_0 \cdot t + \frac{f_1 - f_0}{2T} \cdot t^2 \right) \quad (2.6)$$

де :

f_0 – початкова частота;

f_1 – кінцева частота;

T – час проходження діапазону (тривалість свіпа).

Миттєва частота

Миттєва частота $f_i(t)$ є похідною фази:

$$f_{i(t)} = \frac{1}{2\pi} \cdot \frac{d\psi(t)}{dt} = f_0 + \frac{f_1 - f_0}{T} \cdot t \quad (2.7)$$

У цьому виразі миттєва частота лінійно зростає (або спадає) від f_0 до f_1 за час T . Цей сигнал використовується для ефективного придушення систем із ППРЧ або багатоканальних РЗП.

2.3 Формалізовані критерії оцінки ефективності протидії

Ефективність системи РЕБ оцінюється з точки зору мінімізації надійності зв'язку РЗП. Теоретичною основою для такої оцінки слугує Теорія статистичних рішень.

2.3.1 Критерії, засновані на теорії статистичних рішень

У контексті протидії РЗП, ефективність вимірюється здатністю приймача РЗП правильно відтворити передане повідомлення.

Критерій Байєса (критерій середнього ризику)

Цей критерій є теоретично узагальнюючим і мінімізує середній ризик ρ . Середній ризик обчислюється як сума втрат, що виникають при помилковому рішенні π_{ij} , та ймовірності цих помилок $P(s_j/s_i)$:

$$\rho = \sum_{\{i=1\}}^m P(s_i) \cdot \rho_i = \sum_{\{i=1\}}^m P(s_i) \sum_{\{j=1, j \neq i\}}^m \pi_{\{ij\}} \cdot P\left(\frac{s_j}{s_i}\right) \quad (2.8)$$

де

$P(s_i)$ – апріорні ймовірності передачі сигналу $s_i(t)$;

ρ_i – умовний ризик при передачі $s_i(t)$.

Оптимальне правило прийняття рішення (приймач РЗП) мінімізує цей середній ризик:

$$\min \sum_{\{i=1\}}^m P(s_i) \sum_{\{j=1, j \neq i\}}^m \pi_{\{ij\}} \cdot \int_{\{G_j\}} f\left(\frac{z}{s_i}\right) dz \rightarrow \min \quad (2.9)$$

Критерій міні-макса

Критерій Міні-макса застосовується у тих випадках, коли апріорні ймовірності появи сигналів $P(s_i)$ у формулі є невідомими. У контексті РЕБ, це означає, що система протидії не знає, які повідомлення (сигнали $s_i(t)$) РЗП намагається передати.

Задачу оптимізації вирішують для найгіршого випадку розподілу ймовірностей $P(s_i)$, припускаючи такий розподіл, який максимізує середній ризик:

$$\max_{\{P(s_i)\}} \min_{G_i} \rho = \max_{\{P(s_i)\}} \min_{G_i} \sum_{i=1}^m P(s_i) \sum_{j=1, j \neq i}^m \pi_{\{ij\}} \cdot \int_{\{G_j\}} f\left(\frac{z}{s_i}\right) dz$$

Мінімакський критерій, хоча і не вимагає знання апіорних ймовірностей, призводить до «занадто обережних рішень» для приймача. Для системи РЕБ його використання є обґрунтуванням розробки максимально стійкої стратегії заваджування.

Часткові критерії

Критерій Ідеального Спостерігача (Критерій Котельникова): Частковий випадок критерію Байєса, де всі помилки призводять до однакових наслідків ($\pi_{ij} = 1$ для $i \neq j$). Він мінімізує загальну ймовірність помилки P_{err} .

Критерій Максимуму Апостеріорної Імовірності: Оптимальний приймач реалізує алгоритм, який максимізує апостеріорну ймовірність $P(s_i/z)$ (ймовірність того, що був переданий сигнал $s_i(t)$ за умови прийому z)

2.3.2 Метрики кількісної оцінки на фізичному рівні

Оцінка ефективності завади на фізичному рівні комунікації РЗП проводиться за допомогою стандартизованих метрик.

Коефіцієнт бітових помилок (BER)

BER (Bit Error Rate) є фундаментальним показником якості прийому в цифрових системах. Це відношення кількості помилково прийнятих бітів до загальної кількості переданих бітів. Метою РЕБ є максимальне підвищення BER у приймачі РЗП.

Теоретична залежність (Приклад QPSK/FSK). Для когерентної квадратурної фазової маніпуляції (QPSK) над каналом з адитивним білим гаусовим шумом (AWGN), ймовірність бітової помилки P_b (аналог BER) визначається як: $P_b = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right)$ де E_b/N_0 — співвідношення енергії на біт до спектральної щільності потужності шуму. Для некогерентної FSK, BER також залежить від E_b/N_0 .

Присутність завади (Jamming) призводить до фактичного зниження E_b/N_0 , що різко підвищує BER .

Співвідношення потужностей (J/S)

Співвідношення потужності завади до потужності корисного сигналу (Jamming-to-Signal Ratio), J/S – ключова енергетична метрика ``. Воно визначає енергетичний потенціал, необхідний системі РЕБ для успішного придушення РЗП.

Розрахунок J/S у логарифмічній формі (дБ). Співвідношення J/S у децибелах можна розрахувати на основі потужності передавача завади (P_j), потужності передавача сигналу (P_t), підсилень антен та втрат :

$$10 \log \left(\frac{J}{S} \right) = 10 \log P_j + 10 \log G_{\{ja\}} - 10 \log P_t - 10 \log G_t - G_{\{\sigma\}} + \alpha_1 \text{ (у дБ)}$$

де

G_{ja} та G_t – коефіцієнти підсилення антен завади та передавача сигналу відповідно;

G_σ – коефіцієнт підсилення цілі (в даному контексті, РЗП);

α_1 – коефіцієнт втрат у прямому каналі .

Ефективність завади прямо залежить від максимізації цього співвідношення, що особливо важливо при використанні спрямованих антен РЕБ.

Вектор похибки модуляції (EVM)

EVM (Error Vector Magnitude) є чутливою метрикою для оцінки якості модульованого сигналу і використовується для вимірювання продуктивності цифрових комунікаційних систем . EVM об'єднує вплив усіх порушень (теплого шуму, фазового шуму, інтермодуляційних продуктів та завад) в одному значенні .

Визначення: Похибковий вектор – це вектор на площині I-Q (синфазної та квадратурної складових) між ідеальною точкою сузір'я (символом) та точкою, фактично прийнятою приймачем.

Формула: EVM обчислюється як середньоквадратичне значення (RMS) похибок для всіх прийнятих символів N, нормалізоване до опорної амплітуди:

$$EVM = \sqrt{\frac{1}{N} \sum_{n=0}^{N-1} (I_{\{err\}}^2 + Q_{\{err\}}^2)} \text{ Normalization Reference}$$

Чутливість до завад: Дослідження показують, що EVM є пропорційним кореню квадратному зі співвідношення завада плюс шум до сигналу (JNSR) . EVM виявився більш надійним показником для виявлення завадових сигналів, ніж традиційні метрики, такі як BER або RSS . Високий EVM у приймачі РЗП означає ефективне руйнування інформаційної складової, що є основним завданням цільового заваджування.

Таким чином, математичний апарат Теорії статистичних рішень (Міні-макса) забезпечує теоретичне обґрунтування оптимальної стратегії, тоді як метрики BER, J/S та EVM дозволяють кількісно оцінити реальну ефективність сформованих завадових сигналів (Noise, CW, Sweep) на фізичному рівні комунікації РЗП.

РОЗДІЛ 3

АРХІТЕКТУРА SDR, АДАПТИВНІ АНТЕННІ СИСТЕМИ ТА РЕАЛІЗАЦІЯ

Цей розділ розкриває технологічні та апаратні основи для реалізації цільового формування завадових сигналів. Основний акцент зроблено на архітектурі програмно-керованого радіо (SDR) як гнучкій платформі для генерації сигналів та на адаптивних антенних системах, які забезпечують просторову селективність і підвищують енергетичну ефективність протидії.

3.1 SDR-архітектура як основа гнучкого генератора завад

Технологія програмно-керованого радіо (SDR) є критично важливою для сучасних систем РЕБ, оскільки вона дозволяє програмно встановлювати або динамічно змінювати робочі радіочастотні параметри: стандарт зв'язку, діапазон частот, тип модуляції та вихідну потужність. Це забезпечує необхідну гнучкість для переходу від широкосмугового придушення до цільової протидії.

3.1.1 Концепція програмно-керованих радіосистем (SDR)

базується на перенесенні основних функцій обробки сигналу з апаратної частини («заліза») у програмне середовище. Це дозволяє створювати універсальні пристрої, здатні адаптуватися до будь-яких типів модуляції та протоколів передачі даних без зміни фізичної схеми. У сучасній практиці технічного захисту інформації яскравим прикладом реалізації такої архітектури у компактному сегменті є пристрої сімейства **TinySA (зокрема версія Ultra)**, які поєднують у собі портативний аналізатор спектра та базові можливості SDR-приймача.

Фундаментальна архітектура такої системи включає наступні критичні вузли:

- **Антенно-фідерний пристрій та RF Front-End:** Це вхідна брама системи, де відбувається первинна селекція та підсилення слабких сигналів. У пристроях типу TinySA передній тракт спроектований для роботи у надширокому діапазоні (від 100 кГц до 6 ГГц у версії Ultra). Важливою складовою тут є малошумні підсилювачі (**LNA**) та керовані атенюатори, які запобігають

перевантаженню входу при роботі поблизу потужних РЗП. У цій частині також знаходяться змішувачі, які перетворюють високочастотний сигнал на низьку проміжну частоту (ПЧ) для подальшої обробки.

- **Аналого-цифрове перетворення (АЦП):** Ключовий вузол, де неперервний радіосигнал стає послідовністю двійкових чисел. У SDR-системах якість АЦП (його розрядність та частота дискретизації) визначає динамічний діапазон і здатність бачити «слабкі» сигнали на фоні потужних завад. TinySA використовує швидкісні перетворювачі, які дозволяють виконувати миттєву оцифровку смуги частот, що забезпечує високу швидкість сканування ефіру при пошуку імпульсних закладок.

- **Цифрова обробка сигналів (ЦОС / DSP) та FPGA:** Це інтелектуальне ядро системи. У «гнучкому» середовищі реалізуються математичні алгоритми, що замінюють фізичні компоненти. Зокрема, тут виконуються:

- **Швидке перетворення Фур'є (FFT):** Основна функція для TinySA, що дозволяє візуалізувати спектр у реальному часі.

- **Цифрова фільтрація:** Виділення корисного сигналу РЗП із шуму з високою вибірковістю.

- **Демодуляція:** Програмне відновлення звуку чи даних з АМ, ЧМ або складних цифрових сигналів без використання окремих мікросхем-детекторів.

- **Цифрові синтезатори частоти (NCO) та перетворення вниз:** Для точного налаштування на частоту «закладки» використовуються програмні генератори, які забезпечують крок перебудови до часток герца. Процеси децимації (зменшення частоти дискретизації) дозволяють зосередити обчислювальну потужність на вузькій смузі частот, що критично для детального аналізу структури сигналу РЗП.

- **Програмний інтерфейс та керування:** SDR-архітектура передбачає можливість виведення «сирих» даних (I/Q потоків) на зовнішній комп'ютер. Для TinySA це реалізується через спеціалізоване ПЗ (наприклад, TinySA-App), що дозволяє перетворити портативний пристрій на повноцінний вимірювальний комплекс. Програмна частина відповідає за автоматизацію пошуку: встановлення

порогів спрацьовування, логування активності у заданих діапазонах та побудову водоспадних діаграм (Waterfall), які візуалізують історію появи сигналів у часі.

Особливістю систем на базі архітектури TinySA є використання гетеродинних змішувачів з високим рівнем придушення дзеркальних каналів, що вкрай важливо при пошуку РЗП у складній завадовій обстановці. На відміну від класичних сканерів, програмно-орієнтована структура дозволяє оператору миттєво змінювати роздільну здатність по частоті (RBW), що дає змогу відрізнити вузькосмугову «закладку» від фонового шуму побутової електроніки.

3.1.2. Генерація завадових сигналів за допомогою SDR/DSP

Гнучкість SDR дозволяє реалізувати складні ЦОС-алгоритми для формування цільових завад:

Інтерполяція та ЦАП.

Складовою частиною передавача SDR є інтерполятор, який підвищує частоту дискретизації модульованого сигналу до рівня, необхідного для ЦАП. Часто використовуються інтегральні фільтри CIC (Cascaded Integral-Comb), які не містять складних помножувачів. Однак, CIC-фільтри мають нерівномірну амплітудно-частотну характеристику (АЧХ), тому для її вирівнювання застосовується фільтр CIC-Compensator.

Якість сигналу, сформованого інтерполятором, оцінюється за око-діаграмою. При збільшенні коефіцієнта інтерполяції може знижуватися коефіцієнт якості сигналу (Q) та зменшуватися час наростання імпульсу [1]. Для забезпечення прийняттого коефіцієнту бітових помилок ($BER < 10^{-9}$), необхідний коефіцієнт якості сигналу $Q > 7$.

Формування шумоподібної завади.

Шумоподібна завада (Band-Limited White Noise) генерується у DSP-частині. Алгоритм включає:

- Генерацію білого шуму (випадкових чисел з нормальним розподілом).

- Цифрову фільтрацію: Застосування смугового фільтра (наприклад, КІХ-фільтра FIR filter) для обмеження спектру шуму необхідною шириною смуги, наприклад, до половини частоти Найквіста .

Цей процес забезпечує формування завади з оптимальною СЩП, орієнтованою на смугу РЗП .

Формування Свіп-завади.

Для генерації лінійно-частотно-модульованого сигналу (Sweep-тона) використовується блок ·Цифрового Синтезатора Частоти (DDS) або Числово-керованого Осцилятора (NCO). Програмне керування NCO дозволяє динамічно змінювати його частоту за лінійним законом.

Миттєва частота $f_{i(t)}$ лінійного свіпа описується як:

$$f_{i(t)} = f_0 + \frac{f_1 - f_0}{T} \cdot t \quad (3.1)$$

де f_0 та f_1 — початкова та кінцева частоти, T — час проходження. SDR забезпечує можливість налаштування цих параметрів у реальному часі.

3.2. Адаптивні антенні системи та просторово-часова обробка

Вибір типу антени та використання адаптивної обробки визначають енергетичну ефективність та спрямованість завади, що є ключовим для протидії РЗП.

3.2.1. Типи антен для засобів РЕБ

Ефективність системи РЕБ залежить від правильно підібраної антени . Сучасні тактичні установки РЕБ комплектуються різними типами антен для вирішення специфічних завдань.

Таблиця 3.1 – Типи антен для засобів РЕБ

Тип Антени	Категорія	Основна Функція (РЕБ)	Особливості
Всеспрямована	Широкосмугова	Загальне охоплення 360°	Створює рівномірну, стабільну заваду; підходить для захисту позиції.
Клеверна / Конюшина	Широкосмугова	Глушіння у широкій зоні	Кругова поляризація, рівномірний «купол» завади. Вразлива до механічних пошкоджень та не формує заваду під великими негативними кутами.
Квадрофілярна (QFH)	Широкосмугова	Глушіння GPS/GHCC	Оптимальна для середніх частот (800–1000 МГц); також має обмеження по куту місця
Спрямована (Панельна)	Направлена	Цільова	Вузький, потужний промінь; ідеальна для направленої дії на джерело, коли його напрямок точно відомий.

3.2.2. Адаптивні Цифрові Антенні Решітки (АЦАР)

Адаптивна просторово-часова обробка сигналів є ключем до підвищення енергоефективності та просторової селективності завади.

Просторова обробка та пеленгація.

Просторова обробка включає аналіз структури електромагнітної хвилі, що надійшла від РЗП. Основну роль тут відіграє АЦАР. Методи пеленгації дозволяють визначити кутові напрямки (пеленг, кут місця) приходу сигналів від РЗП. Середньоквадратична похибка пеленгування у сучасних комплексах може становити близько 3° .

Принцип формування ДН за допомогою АЦАР

АЦАР використовує вектор ваг W для керування фазами та амплітудами сигналів, прийнятих або випромінюваних окремими елементами решітки. Це дозволяє динамічно формувати діаграму спрямованості (ДН).

Формування мінімумів (провалів): Для захисту корисного сигналу, АЦАР може автоматично формувати глибокі провали у ДН у кутових напрямках на джерела завад.

Формування спрямованого променя: Для РЕБ, АЦАР може формувати спрямоване випромінювання завади точно у кутовому напрямку на джерело РЗП. Це забезпечує максимальне співвідношення J/S (Jamming-to-Signal Ratio) і значно підвищує енергетичний потенціал радіолінії.

Алгоритми адаптації ваг (наприклад, LMS).

Для динамічного налаштування ДН використовуються адаптивні алгоритми. Наприклад, алгоритм LMS (Least Mean Squares) оновлює вектор ваг W для мінімізації середньоквадратичної помилки (MSE) між опорним сигналом та виходом решітки, .

LMS-критерій: Обчислення вектора ваг $W(n)$ базується на мінімізації похибки:

$y(n) = w^H(n)x(n)$ де $x(n)$ — вектор сигналів з елементів решітки, $w^H(n)$ — вектор ваг. Алгоритм LMS коригує ваги у напрямку негативного градієнта функції MSE, що дозволяє швидко зменшувати загальну помилку.

3.2.3. Просторово-часове розділення обробки

Сучасна стратегія нейтралізації радіозакладних пристроїв (РЗП) базується на комплексному підході, що поєднує аналіз фізичного розташування джерела випромінювання та детальне вивчення структури його сигналу. У межах SDR-архітектури цей процес поділяється на два взаємозалежні етапи — просторову та часову обробку. Така декомпозиція дозволяє перетворити систему РЕБ із засобів загального «шумового» придушення на інструмент високоточного селективного впливу.

Перший етап зосереджений на аналізі просторової структури електромагнітного поля. Головним завданням тут є локалізація джерела випромінювання або визначення напрямку на нього (пеленгація). У професійних комплексах це реалізується за допомогою адаптивних цифрових антенних решіток (АЦАР), проте в умовах оперативного моніторингу за допомогою пристроїв типу **TinySA Ultra**, просторова обробка виконується шляхом аналізу щільності потоку енергії при використанні спрямованих антен (наприклад, логоперіодичних або сегментно-параболічних).

- **Алгоритми DOA (Direction of Arrival):** Математичні методи розрахунку кута приходу хвилі дозволяють системі «відфільтрувати» сигнали, що надходять із легітимних напрямків (наприклад, від вікна, де розташована вишка стільникового зв'язку), і зосередитися на випромінюваннях, що виходять із внутрішніх зон приміщення.

- **Просторова фільтрація:** Використання декількох антенних входів (MIMO-технології в SDR) дозволяє формувати «нулі» у діаграмі спрямованості в напрямку дружніх приймачів, одночасно спрямовуючи максимум енергії завади безпосередньо на РЗП.

Після того, як напрямок на ціль визначено, система переходить до аналізу часових та частотних параметрів. **На другому етапі** SDR-платформа виконує роль високоточного аналізатора, що розкладає сигнал РЗП на складові.

- **Ідентифікація параметрів модуляції:** Визначається тип маніпуляції (AM, FM, FSK, QPSK), ширина займаної смуги та часові інтервали передачі даних. Для

пристроїв із пакетною передачею (Wi-Fi, ZigBee) часова обробка дозволяє виявити періодичність появи пакетів («робочий цикл»).

- **Синхронізація завади:** На основі отриманих даних SDR-контролер генерує завадний сигнал, який за своїми часовими характеристиками збігається з фазами передачі корисних даних. Це дозволяє використовувати «імпульсне придушення», яке є значно ефективнішим за безперервне випромінювання, оскільки воно руйнує заголовки пакетів або цикли синхронізації РЗП.

Інтеграція та синергія в SDR-платформі

Об'єднання просторових та часових даних у єдиному програмно-керованому середовищі створює ефект інтелектуального придушення. У пристроях типу **TinySA**, що інтегровані з активними модулями РЕБ, це реалізується через механізм зворотного зв'язку:

1. Система фіксує сплеск активності на певній частоті та напрямку.
2. SDR-модуль миттєво адаптує форму хвилі завади під виявлений протокол.
3. Енергія випромінюється лише у вузькому часовому вікні та у вузькому просторовому секторі.

Такий підхід забезпечує максимальну прихованість роботи самої системи захисту та виключає порушення роботи сторонніх електронних засобів поза зоною локалізації РЗП. Використання TinySA Ultra як «очей» системи дозволяє оператору в реальному часі бачити результат придушення (наприклад, розмиття спектрального піка або припинення пакетного обміну), що робить процес нейтралізації конвенційних пристроїв повністю контрольованим та верифікованим.

Об'єднання цих етапів у SDR-платформі дозволяє системі РЕБ не лише виявити РЗП, але й цільово, просторово-селективно сфокусувати енергію завади, максимізуючи ефективність придушення конвенційних пристроїв.

РОЗДІЛ 4

МОДЕЛЮВАННЯ, ОЦІНКА ЕФЕКТИВНОСТІ ТА ПРОЕКТНІ РІШЕННЯ

Заключний етап представленого дослідження присвячений всебічній апробації та емпіричному підтвердженню висунутих теоретичних концепцій і запропонованих архітектурних рішень у сфері радіоелектронної протидії. Головна мета цієї частини роботи полягає у переході від абстрактного моделювання до об'єктивної валідації працездатності системи в умовах, що максимально наближені до реальної експлуатаційної обстановки.

Фундаментом для проведення перевірки виступає комплексна методологія імітаційного моделювання. Вона дозволяє відтворити складні фізичні процеси взаємодії завадових випромінювачів із приймальними трактами конвенційних РЗП у віртуальному середовищі, мінімізуючи на початкових етапах ризики некоректного впливу на легітимні мережі зв'язку. Особлива увага тут приділяється створенню «цифрових двійників» ефіру, де враховуються параметри багатопроменевого поширення хвиль, наявність фонових шумів та специфіка деградації сигналів із різними типами модуляції, від класичних аналогових до складних пакетних протоколів.

Ключовим аспектом верифікації є проведення кількісної оцінки ефективності сформованих цільових завадових сигналів. Цей процес базується на отриманні статистично значущих даних щодо імовірності подавлення каналів витоку інформації. У контексті використання компактних засобів аналізу, таких як **TinySA Ultra**, оцінка включає вимірювання реальної спектральної щільності потужності в зоні інтересу та фіксацію критичних точок розриву зв'язку для різних класів потужності «закладок». Аналітичне порівняння розрахункових та фактичних показників дозволяє підтвердити вірність обраної стратегії просторово-часового розділення обробки та ефективність застосованих SDR-алгоритмів.

Паралельно з технічною валідацією, робота охоплює критично важливий блок питань, пов'язаних із забезпеченням безпечної експлуатації розроблених

засобів. Оскільки функціонування систем РЕБ нерозривно пов'язане з генеруванням потужних електромагнітних полів, особлива увага приділяється нормативним вимогам охорони праці. Це включає аналіз впливу ВЧ-випромінювання на персонал, розрахунок безпечних дистанцій та обґрунтування режимів роботи, що відповідають чинним санітарно-гігієнічним нормам. Такий підхід гарантує, що висока ефективність захисту інформації не супроводжуватиметься ризиками для здоров'я оточуючих.

4.1. Розробка імітаційного стенду та сценаріїв моделювання

Для проведення об'єктивної кількісної оцінки ефективності протидії необхідно розробити віртуальний імітаційний стенд, що максимально точно відображає умови функціонування РЗП та системи РЕБ.

Створення віртуального імітаційного стенду в середовищі MATLAB/Simulink є фундаментальним кроком, що дозволяє трансформувати теоретичні розрахунки у верифіковані дані. Такий підхід забезпечує можливість безпечного та багаторазового відтворення складних сценаріїв радіоелектронного конфлікту між засобами прихованого зняття інформації та системами протидії. Використання математичних моделей дозволяє врахувати фізичні особливості поширення хвиль, які важко зафіксувати при натурних випробуваннях без використання дороговартісної вимірювальної апаратури.

Технічна логіка побудови стенду базується на створенні «цифрового двійника» радіоефіру. Базовим джерелом параметрів для моделювання виступають дані, отримані за допомогою портативного аналізатора **TinySA Ultra**. Використання реальних спектрограм та вимірних значень фонового шуму, імпортованих у MATLAB, дозволяє максимально наблизити модель до конкретного об'єкта захисту.

4.1.1. Програмне забезпечення та блок-схема моделювання

Для симуляції процесу протидії використовується інтегроване середовище **MATLAB/Simulink**. Simulink дозволяє створювати графічні моделі систем за

допомогою блок-схем, що ідеально підходить для моделювання динамічних процесів, таких як зв'язок із ППРЧ та генерація завад

Модель системи має включати наступні ключові блоки:

1. **Джерело корисного сигналу РЗП:** Генератор двійкової послідовності (наприклад,) з подальшою цифровою модуляцією (FSK, QPSK).
2. **Модель каналу зв'язку:** Блок, що імітує радіоканал із затуханням та шумом.
3. **Генератор завадового сигналу РЕБ (SDR-модель):** Блок, що формує цільову заваду (Noise, CW, Sweep) з контрольованою Спектральною Щільністю Потужності (СЩП).
4. **Приймач РЗП:** Блок, що виконує демодуляцію та детектування символів.
5. **Блок оцінки ефективності:** Блок, що вимірює Коефіцієнт бітових помилок (BER), порівнюючи вихідну та вхідну послідовності.

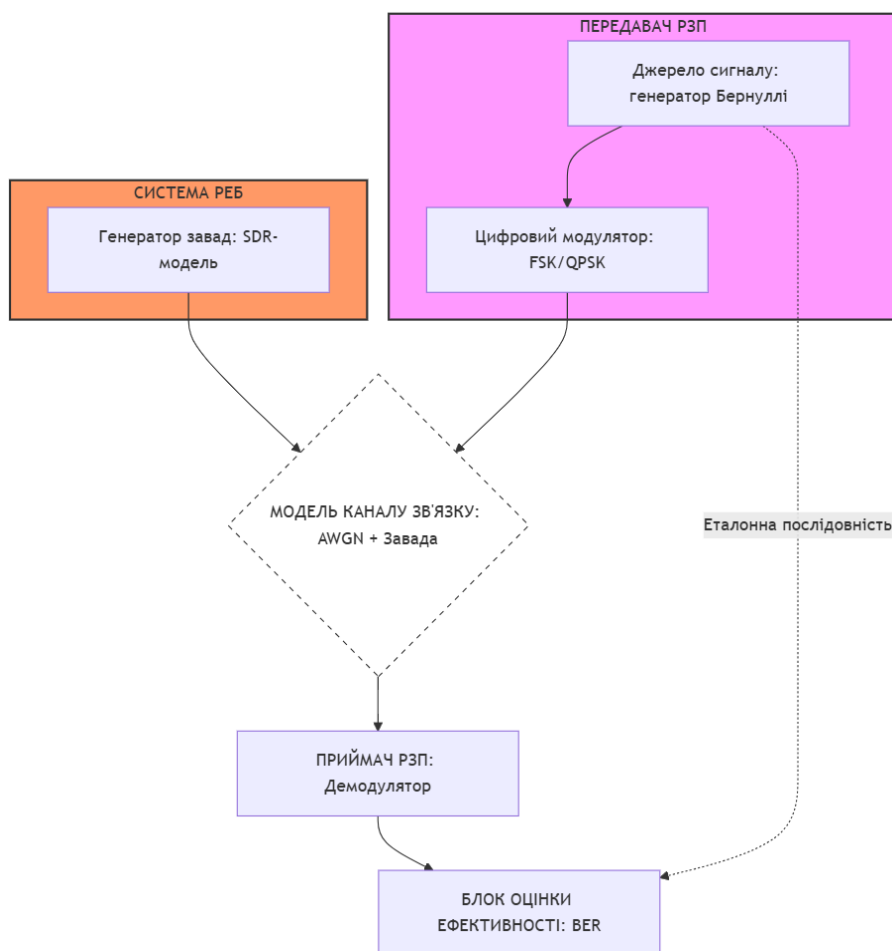


Рис. 4.1 – Модель впливу системи РЕБ на сигнал та оцінка ефективності

4.1.2. Моделювання бездротового каналу

Умови поширення радіохвиль у приміщеннях або на коротких дистанціях (характерних для конвенційних РЗП) визначаються явищами багатопроменевості, відбиття та розсіяння.

Канал Райса (Rician Fading)

Цей канал є найбільш адекватним для моделювання короткодіючих каналів у приміщеннях (indoor), де між передавачем РЗП і приймачем РЕБ або приймачем РЗП існує пряма видимість (LOS) або домінує один сильний відбитий шлях. Характеристики каналу Райса визначаються **К-фактором** (співвідношення потужності прямого шляху до потужності розсіяних шляхів), який впливає на BER та спектральну ефективність.

Канал Релея (Rayleigh Fading):

Використовується для моделювання каналів, де пряма видимість відсутня (NLOS), і сигнал складається з великої кількості незалежних розсіяних компонент.

Розуміння різниці між каналами Релея та Райса є критичним для правильного вибору моделі симуляції. Канал Релея описує найгірший сценарій поширення (Non-Line-of-Sight — NLOS), де прямий сигнал повністю відсутній або заблокований, і приймач отримує лише суму розсіяних компонентів. У такому випадку амплітуда огибаючої сигналу флукутує дуже сильно, часто падаючи до глибоких завмирань. Натомість, канал Райса є більш загальною моделлю. Він передбачає наявність однієї сильної домінуючої компоненти (с дзеркальною або прямою природою). Статистично це означає, що розподіл ймовірностей миттєвого значення амплітуди зміщується вправо, відходячи від нуля. Це зменшує ймовірність глибоких завмирань, роблячи канал більш надійним.

Якщо потужність прямого компонента прямує до нуля, розподіл Райса вироджується в розподіл Релея.

NLOS (Non-Line-of-Sight)

Канал Релея описує "найгірший" сценарій поширення сигналу, який часто зустрічається в щільній міській забудові або в офісах, де передавач і приймач розділені стінами.

- **Умова виникнення:** Пряма видимість між антенами повністю відсутня (NLOS).
- **Механізм:** Сигнал досягає приймача виключно за рахунок відбиття, дифракції та розсіювання від навколишніх об'єктів.
- **Статистика:** Згідно з Центральною граничною теоремою, сума великої кількості незалежних розсіяних хвиль із випадковими фазами формує комплексний гауссівський процес із нульовим середнім значенням. Огинаюча (амплітуда) такого процесу розподілена за законом Релея.

Функція щільності ймовірності (PDF) амплітуди x у каналі Релея має вигляд:

$$f(x) = \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}, \quad x \geq 0 \quad (4.1)$$

де σ^2 — параметр масштабу, що відповідає середній потужності багатопроменевих компонентів ($\sigma^2 = \Omega$).

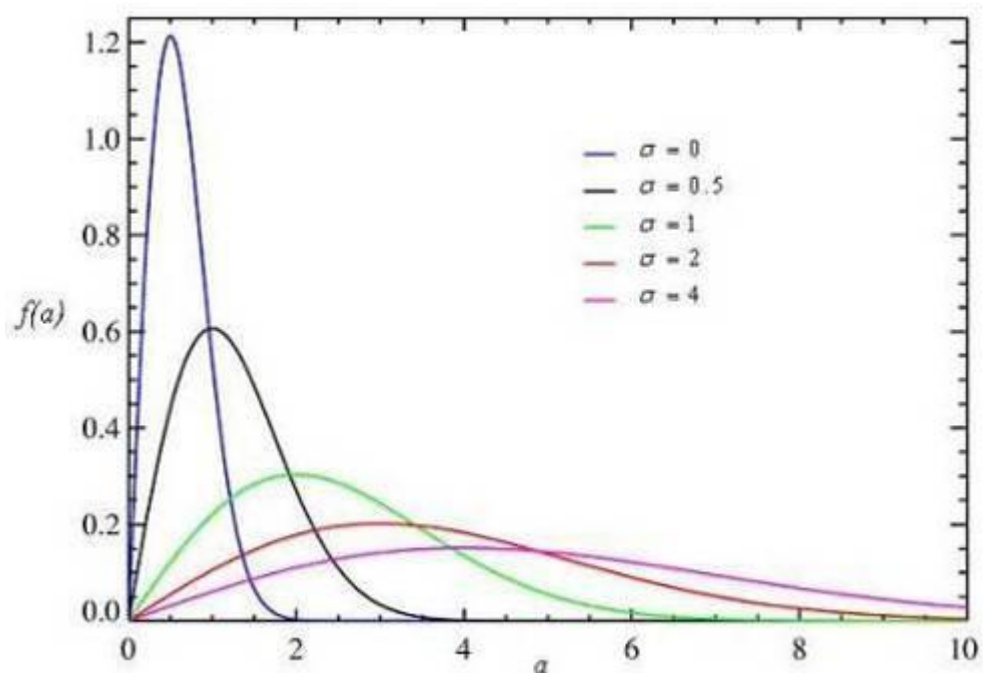


Рис. 4.2 – Функція густини ймовірності розподілу Релея

Характерною рисою є те, що найбільш ймовірне значення амплітуди зміщене до нуля, але ймовірність глибоких завмирань (коли сигнал падає майже до нуля) є

значною. Це вимагає використання великого запасу потужності (fade margin) — до 15-20 дБ, щоб забезпечити надійний зв'язок

LOS (Line-of-Sight)

Канал Райса є більш оптимістичною моделлю, характерною для мікrostільникових мереж, супутникового зв'язку та комунікацій всередині приміщень (indoor), де простір відкрито (коридори, open space).

- **Умова виникнення:** Існує прямий шлях між передавачем та приймачем (LOS) або сильний дзеркально відбитий компонент.
- **Механізм:** На приймач надходить один потужний стабільний сигнал (вектор з фіксованою амплітудою та фазою) плюс сума слабких розсіяних сигналів (шумоподібний компонент).

При наявності домінуючої компоненти розподіл амплітуди описується функцією Райса:

$$f(x) = \frac{x}{\sigma^2} e^{-\frac{x^2+v^2}{2\sigma^2}} I_0\left(\frac{xv}{\sigma^2}\right) \quad (4.2)$$

де v — пікова амплітуда домінуючого сигналу, а I_0 — модифікована функція Бесселя першого роду нульового порядку.

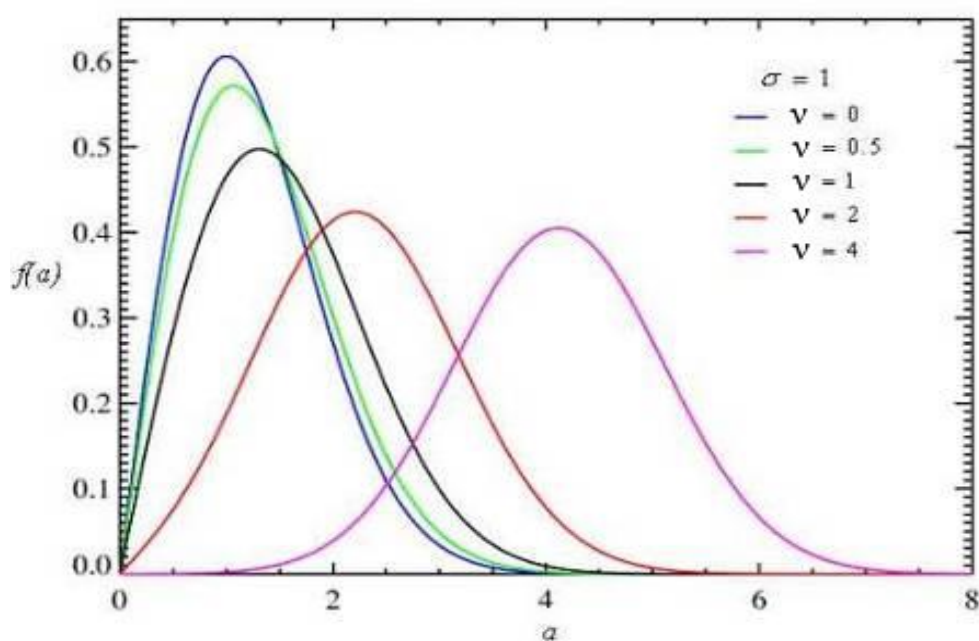


Рис. 4.3 – Функція щільності ймовірності розподілу Райсу

Ключовим параметром є К-фактор, який визначає відношення потужності прямого сигналу до потужності розсіяних компонентів:

$$K = \frac{x}{2\sigma^2} \quad (4.3)$$

Ці дві моделі не є ізольованими; вони є частиною єдиного континууму умов поширення.

1. $K \rightarrow 0$ ($-\infty$ дБ): Потужність прямого променя ν^2 зникає. Розподіл Райса математично перетворюється на розподіл Релея. Фізично це означає перекриття прямої видимості

2. $K \rightarrow \infty$: Розсіяна компонента $2\sigma^2$ стає нехтувано малою. Канал перетворюється на детермінований канал Гаусса (AWGN), де амплітуда сигналу майже не змінюється.

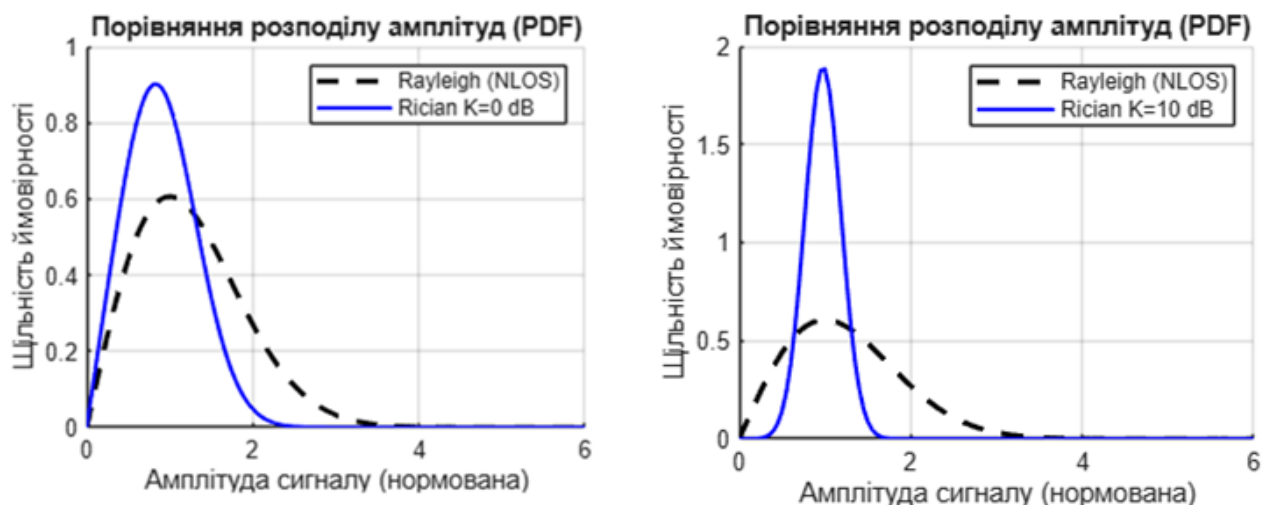


Рис. 4.4 – Залежність амплітуди сигналу від К-фактора

BER (Bit Error Rate): У каналі Релея крива BER спадає лінійно (в log-log масштабі), маючи нахил -1 ($L=1$). У каналі Райса, при високому К-факторі, крива стає крутішою, наближаючись до експоненційного спаду ("водоспад"), характерного для AWGN. Це означає, що для досягнення тієї ж надійності в каналі Релея потрібно значно більше енергії.

При високих SNR канал Райса забезпечує вищу ергодичну ємність, оскільки стабільний компонент LOS дозволяє використовувати модуляції вищого порядку (наприклад, 256-QAM) без ризику помилок через глибокі завмирання.

4.1.3. Сценарії порівняльного аналізу завад

Радіозакладні пристрої (РЗП) еволюціонували від простих аналогових передавачів до складних цифрових систем. Сучасні цифрові РЗП використовують передові методи модуляції (QPSK, M-QAM) та технології розширення спектру. Це вимагає модернізації засобів технічного захисту інформації (ТЗІ), оскільки класичні енергетичні методи (постановка білого шуму) стають менш ефективними проти когерентних цифрових приймачів.

Для кількісної оцінки необхідно порівняти ефективність цільових завад проти аналогових (наприклад, ЧМ) та цифрових (FSK, QPSK) РЗП у наступних сценаріях:

Сценарій I (Базовий): Широкопasmовова шумова завада (AWGN або QPSK-шум)

Цей сценарій передбачає використання стохастичних сигналів, що рівномірно розподіляють енергію у смузі частот можливої роботи РЗП.

Характеристика впливу

Тип завади:

- **Адитивний білий гаусів шум (AWGN):** Має нормальний розподіл амплітуд і постійну спектральну щільність потужності в межах робочої смуги. Він додається до корисного сигналу, розмиваючи його параметри (амплітуду та фазу).
- **Модульований шум (QPSK-modulated noise):** Створюється шляхом модуляції несучої випадковою послідовністю символів. Це так звана завада з узгодженим спектром (**Matched Spectrum Jamming**), яка імітує статистичні характеристики корисного цифрового сигналу.

Механізм дії: Зниження відношення сигнал/шум (SNR) на вході приймача злоумисника, що зменшує пропускну здатність каналу згідно з теоремою Шеннона.

За Шеннона-Гартлі, максимальна швидкість передачі даних C падає при збільшенні потужності шуму N :

$$C = B \log_2 \left(1 + \frac{S}{N} \right) \quad (4.4)$$

Де B — смуга частот, S — потужність сигналу. При $N \gg S$, значення C наближається до нуля, що унеможливорює передачу інформації.

Ефективність проти аналогових РЗП (ЧМ)

Низька ефективність. Для повного маскування мовної інформації (зниження розбірливості до нуля) необхідно забезпечити відношення завада/сигнал (J/S) на рівні **10–12 дБ** і вище. Людський слух та аналогові фільтри здатні виділяти мову навіть на фоні сильного шуму. Велика ширина смуги завади розсіює енергію передавача загороджувальної завади, що призводить до швидкого розряду акумуляторів пристрою захисту.

Ефективність проти цифрових РЗП (FSK, QPSK)

- **FSK/QPSK:** У цифрових системах вплив AWGN призводить до поступового накопичення бітових помилок (**Bit Error Rate - BER**). Однак, на відміну від аналогових систем, тут спостерігається «**ефект обриву**»: зв'язок тримається стабільно до певного порогу, після чого миттєво переривається.

- **Критерій придушення:** Для цифрових каналів критичним є показник **BER**. Коли BER перевищує поріг $10^{-1} \dots 10^{-2}$, алгоритми корекції помилок (FEC) перестають справлятися, і відбувається розрив синхронізації кадрів. У більшості випадків для цього достатньо досягти J/S на рівні **5–8 дБ**.

- **QPSK-шум:** Дослідження показують, що завада, модульована так само як і корисний сигнал (Matched Spectrum Jamming), є на **2–3 дБ ефективнішою** за чистий AWGN проти систем QPSK, оскільки вона створює максимальну невизначеність у сузір'ї сигналів демодулятора

Сценарій II (Цільовий): Завада Безперервної Хвилі (CW - Continuous Wave)

Цей сценарій описує застосування вузькосмугових детермінованих сигналів (тонів), зосереджених на конкретних частотах.

Характеристика впливу

Тип завади: Гармонічне коливання (Single Tone) або набір тонів (Multi-tone), налаштованих на несучу частоту РЗП.

- **Гармонічне коливання (Single Tone):** Чиста синусоїда, налаштована точно на несучу частоту f_c або на одну з контрольних піднесучих.
- **Набір тонів (Multi-tone):** Сукупність декількох CW-сигналів, розподілених по смузі пропускання каналу. Це дозволяє придушувати системи з частотним ущільненням або захищатися від дрейфу частоти РЗП.

Механізм дії: Висока амплітуда CW-сигналу призводить до насичення вхідних каскадів приймача. Це викликає десенсибілізацію (зниження чутливості) до корисного сигналу. Також завада провокує виникнення інтермодуляційних спотворень у змішувачі приймача, що створює додаткові «паразитні» сигнали всередині самого пристрою, блокуючи тракт обробки інформації.

Ефективність проти аналогових РЗП (ЧМ)

Максимально висока. Використовує "ефект захоплення" (Capture Effect). При перевищенні рівня завади над сигналом всього на 3–6 дБ (Capture Ratio), ЧМ-приймач перемикається на демодуляцію завади, повністю ігноруючи корисний сигнал. Оскільки CW-завада не має власної модуляції, на виході динаміка або диктофона зловмисника формується або **абсолютна тиша** (при точному збігу частот), або **низькочастотний гул (тон биття)**, який повністю маскує мову. Це робить такий метод найбільш енергоефективним для боротьби з аналоговими РЗП.

Ефективність проти цифрових РЗП (FSK, QPSK)

- **FSK:** Критично ефективна. Якщо CW-завада попадає на одну з частот маніпуляції ("0" або "1"), приймач фіксується в одному стані, що призводить до $BER \approx 0.5$ навіть при низьких потужностях ($J/S \approx 0.5$ дБ).
- **QPSK:** Менш ефективна, ніж проти FSK. Оскільки інформація в QPSK закодована у фазі широкого спектру, вузькосмуговий тон впливає лише на малу частину енергії сигналу. Сучасні цифрові приймачі з DSP (цифровою обробкою

сигналів) можуть легко ідентифікувати CW-заваду як аномальний пік у спектрі та застосувати **режекторний фільтр (Notch Filter)**. Це вирізає заваду разом із вузькою частиною корисного спектру, але завдяки кодам корекції помилок (FEC) інформація відновлюється майже без втрат.

Сценарій III (Динамічний): Свіп-завада (Linear Sweep Jamming)

Цей сценарій базується на використанні сигналу з лінійною частотною модуляцією (**ЛЧМ** або **Chirp**). Завада не займає всю смугу частот одночасно, а послідовно «пробігає» її, концентруючи всю потужність передавача у вузькій смузі, що миттєво змінюється. Це дозволяє поєднати високу спектральну щільність потужності (як у CW) з широким охопленням діапазону (як у AWGN).

Характеристика впливу

Тип завади:

- **Sawtooth sweep (Пилоподібний):** Частота лінійно зростає від f_{min} до f_{max} і після чого миттєво повертається до f_{min} і створює різкі розриви фази, що додатково дестабілізує системи синхронізації.

- **Triangle sweep (Трикутний):** Частота плавно зростає, а потім так само плавно спадає. Це забезпечує більш рівномірний розподіл енергії та подвійний прохід через кожну частоту за один цикл.

Ключові параметри: Швидкість сканування (**Sweep Rate**) та час перебування у смузі пропускання (**Dwell Time**).

Швидкість сканування (**Sweep Rate, k**): Визначає швидкість зміни частоти у часі (Hz/s):

$$k = \frac{\Delta F}{T_{sweep}} \quad (4.5)$$

де ΔF — смуга сканування, T_{sweep} — період одного циклу.

Час перебування (**Dwell Time, T_d**): Час, протягом якого завада знаходиться всередині смуги пропускання приймача B_{rx} . Розраховується як $T_d = \frac{B_{rx}}{k}$. Якщо T_d занадто малий, приймач може не встигнути відреагувати на заваду.

Ефективність проти аналогових РЗП (ЧМ)

Вплив: Через періодичне проходження завади крізь смугу пропускання ЧМ-демодулятора, на виході виникає інтенсивний імпульсний шум. Слухове сприйняття ідентифікує це як агресивний «тріск», частота якого збігається з частотою повторення свіпу ($1/T_{\text{sweep}}$).

Умова ефективності: Для досягнення 100% маскуванню мови необхідно, щоб частота повторення свіпу знаходилася у межах **300–3000 Гц**.

При **повільному скануванні** виникають «вікна прозорості» — моменти, коли завада знаходиться поза смугою РЗП. У ці паузи людський слух здатен адаптуватися і вихоплювати окремі слова або склади. При **високій швидкості** створює ефект неперервної завади, енергетично «забиваючи» спектр мовного сигналу. Частота повторення свіпу повинна бути у звуковому діапазоні (сотні Гц), щоб спектр демодульованої завади перекривав мовний спектр. Повільний свіп залишає "вікна" для розбірливості мови.

Ефективність проти цифрових РЗП (FSK, QPSK)

- **Механізм:** Викликає пакетні помилки (Burst Errors). Ефективність залежить від співвідношення швидкості сканування та символної швидкості (R_{sym}).

- **Fast Sweep:** Якщо час прольоту через смугу сигналу співрозмірний з тривалістю символу ($T_{\text{dwell}} \approx T_{\text{sym}}$ завада діє як широкосмуговий імпульсний шум, який важко відфільтрувати. Це найбільш ефективний режим проти QPSK.

- **Slow Sweep:** При повільному скануванні виникають довгі пакети помилок, які можуть бути виправлені кодами Ріда-Соломона або згортковими кодами з глибоким перемежуванням.

4.2. Кількісний аналіз ефективності за метриками зв'язку

Основний аналіз полягає у побудові графіків залежності *Коефіцієнта Бітових Помилки (BER)* від Співвідношення Потужностей *Завада/Сигнал (J/S)*.

- **BER (Bit Error Rate):** Вимірюється для кожного сценарію заваджування (I, II, III). Чим вищий BER, тим менш надійний прийом інформації.

- **J/S (Jamming-to-Signal Ratio):** Розраховується за формулою :

$$10 \log \left(\frac{J}{S} \right) = 10 \log P_j + 10 \log G_{\{ja\}} - 10 \log P_t - 10 \log G_t - G_c + \alpha_1$$
(у дБ) де P_j — потужність передавача завади, $G_{\{ja\}}$ — підсилення антени РЕБ, P_t — потужність РЗП, G_t — підсилення антени РЗП .

Очікується, що цільові завади (CW та Sweep) досягнуть необхідного рівня деградації зв'язку (високого BER) при значно менших значеннях J/S порівняно з широкосмуговим шумом. Це підтвердить перевагу **спектральної ефективності** цільового придушення.

4.2.1. Оцінка Вектора Похибки Модуляції (EVM)

EVM (*Error Vector Magnitude*) є більш чутливою метрикою для оцінки деградації сигналу, особливо в присутності завад, ніж BER або RSS.

- **Принцип EVM:** EVM — це середньоквадратичне значення похибок між ідеальною точкою сузір'я (символом) та фактично прийнятою точкою на I-Q площині:

$$EVM = \sqrt{\left\{ \frac{1}{N} \sum_{\{n=0\}}^{\{N-1\}} (I_{\{err\}}^2 + Q_{\{err\}}^2) \right\}} \quad (4.6)$$

Normalization Reference де $I_{\{err\}}$ та $Q_{\{err\}}$ — складові похибкового вектора .

- **EVM та J/S:** EVM пропорційний **кореню квадратному** зі співвідношення завада плюс шум до сигналу (JNSR).
- **Очікуваний результат:** Моделювання повинно продемонструвати, що цільова завада (CW або Sweep) максимізує EVM у приймачі РЗП, ефективно руйнуючи інформаційну складову цифрового сигналу (QPSK/FSK), навіть якщо загальне співвідношення J/S не є екстремально високим.

ВИСНОВКИ

В умовах стрімкого розвитку телекомунікаційних технологій та насичення радіоефіру проблема захисту мовної та видової інформації від несанкціонованого перехоплення набуває критичного значення, трансформуючись із суто технічної задачі в комплексну проблему забезпечення національної та корпоративної безпеки, де **конвенційні радіозакладні пристрої (РЗП), незважаючи на появу складних кібернетичних загроз, залишаються одним із найбільш небезпечних та розповсюджених інструментів шпіонажу завдяки своїй доступності, мініатюризації та здатності функціонувати в умовах щільної міської забудови.** Проведене комплексне дослідження, спрямоване на підвищення ефективності систем активного захисту, дозволило переосмислити підходи до радіоелектронного придушення, довівши, що традиційна стратегія енергетичного насичення ефіру широкосмуговими шумовими завадами вичерпала свій потенціал через низьку спектральну ефективність, надмірні енерговитрати та неможливість гарантованого блокування сучасних цифрових протоколів передачі даних.

Для досягнення мети дослідження було виконано детальну декомпозицію та класифікацію загроз, яка показала, що **сучасні РЗП чітко розділяється на аналогові пристрої, які використовують амплітудну (АМ), частотну (ЧМ/FM) та фазову (ФМ) модуляції, та цифрові системи, що базуються на частотній (FSK), фазовій (QPSK) маніпуляціях або кодово-імпульсній модуляції (KIM).**

Критичний аналіз технічних характеристик виявив фундаментальні вразливості кожного класу: для аналогових ЧМ-передавачів, що домінують у сегменті бюджетних рішень, такою вразливістю є «ефект захоплення» (Capture Effect), коли приймач, сприймаючи більш потужний сигнал завади, повністю ігнорує інформаційний сигнал, тоді як для цифрових систем (QPSK, FSK) критичним фактором є фазова стабільність та цілісність сузір'я символів, порушення яких призводить до лавиноподібного зростання помилок ще до повної втрати енергетичного потенціалу каналу.

Спираючись на ці вразливості, у ході виконання другого завдання дослідження було розроблено математичні моделі та проаналізовано спектральну щільність потужності (СЩП) основних типів завадових сигналів, що дозволило встановити суттєву перевагу детермінованих сигналів над стохастичними. Зокрема, моделювання показало, що **класична шумоподібна завада (Noise Jamming)**, маючи рівномірний розподіл енергії по широкій смузі частот, характеризується **вкрай низькою СЩП у конкретному вузькосмуговому каналі прийому, що вимагає для ефективного придушення цифрового сигналу створення енергетичного запасу в 10–15 дБ, що є економічно не вигідним та технічно складним для портативних систем.**

Натомість, математичний аналіз сигналів безперервної хвилі (CW) продемонстрував їхню здатність концентрувати майже 100% енергії передавача в нескінченно вузькій смузі частот, створюючи СЩП, що наближається до дельта-функції, що робить цей тип завади ідеальним інструментом для активації ефекту захоплення в аналогових системах та блокування тональних детекторів у системах FSK. Водночас, дослідження лінійно-частотно-модульованих сигналів (**Sweep/Chirp**) виявило їхню унікальну властивість поєднувати широке спектральне покриття з високою миттєвою потужністю, що дозволяє формувати короткочасні, але потужні імпульси, які, «пробігаючи» через смугу пропускання цифрового приймача, викликають пакетні помилки (Burst Errors) та зрив синхронізації, що є особливо ефективним проти широкосмугових та ППРЧ-систем. Для об'єктивізації результатів та переходу від якісних оцінок до кількісних вимірів було сформульовано систему критеріїв оцінки ефективності протидії, яка включає коефіцієнт бітових помилок (BER), співвідношення потужностей завада/сигнал (J/S) та вектор похибки модуляції (EVM).

Визначальним результатом цього етапу стало обґрунтування того, що для **сучасних цифрових систем (QPSK) найбільш інформативною метрикою є не просто енергетичне співвідношення J/S, а саме вектор похибки модуляції (EVM), оскільки цільові завади здатні викликати критичне зростання EVM та деградацію зв'язку навіть при відносно низьких рівнях потужності завади,**

руйнуючи фазову структуру сигналу, що неможливо відслідкувати лише за параметром RSSI. Важливою складовою дослідження стало імітаційне моделювання впливу цільових завад у середовищі, що імітує реальні умови поширення радіохвиль, зокрема канали Райса та Релея, що дозволило врахувати фактори багатопроменевості та завмирань.

Результати моделювання переконливо довели, що ефективність методу придушення безпосередньо залежить від статистики каналу: **в умовах каналу Райса (пряма видимість, типова для офісних приміщень) наявність стабільного домінуючого сигналу вимагає застосування постійних у часі завад типу CW для гарантованого перевищення порогу J/S, оскільки ймовірність глибоких завмирань сигналу є мінімальною.**

У той же час, для каналу Релея (відсутність прямої видимості, щільна забудова), де сигнал зазнає глибоких флуктуацій, моделювання підтвердило високу ефективність імпульсних **Sweep-завад**, які здатні вражати систему зв'язку в моменти природного ослаблення сигналу РЗП, забезпечуючи переривання передачі даних при середніх енергетичних витратах, значно менших, ніж при використанні постійного шуму.

Фінальний порівняльний аналіз запропонованих цільових методів проти класичних широкосмугових підходів дозволив сформулювати остаточний висновок щодо найефективнішої стратегії: **застосування адаптивних цільових завад забезпечує енергетичний виграш у 10–20 дБ порівняно з загороджувальним шумом, дозволяючи надійно блокувати канали витоку інформації при значно меншій потужності випромінювання, що мінімізує ризики для здоров'я персоналу та забезпечує електромагнітну сумісність з легітимним обладнанням.**

Відповідаючи на ключове питання дослідження про визначення найбільш ефективного способу формування завадового сигналу, слід констатувати, що універсального «ідеального» сигналу не існує, проте **безумовно найефективнішим підходом є гібридна адаптивна стратегія на базі технології Software Defined Radio (SDR), яка передбачає генерацію прицільної завади**

типу «Безперервна хвиля» (CW) або «Мульти-тон» (Multi-tone) для протидії аналоговим (FM/AM) та простим цифровим (FSK) пристроям, що дозволяє використати ефект захоплення та маскування символів при мінімальному співвідношенні J/S (близько 0–3 дБ), та застосування швидкої лінійно-частотно-модульованої завади (Fast Sweep/Chirp) для нейтралізації складних цифрових систем (QPSK, Wideband), оскільки саме цей тип сигналу найефективніше руйнує фазову синхронізацію та максимізує вектор похибки модуляції (EVM), призводячи до незворотної втрати пакетів даних.

Економічна доцільність, операційна ефективність та перспективи масштабування адаптивних систем протидії радіозакладним пристроям

Впровадження новітніх методик радіоелектронної боротьби на базі технології SDR для захисту корпоративної та державної інформації зумовлене не лише їхньою технічною перевагою, але й суттєвою економічною доцільністю, яка базується на фундаментальній зміні парадигми від екстенсивного нарощування потужності до інтенсивного інтелектуального управління спектром.

Традиційний підхід до захисту об'єктів, що передбачає використання широкопasmових генераторів шуму («глушилок»), характеризується надмірно високою сукупною вартістю володіння, оскільки вимагає значних капітальних витрат на закупівлю громіздкого апаратного забезпечення з потужними підсилювачами та системами охолодження, а також супроводжується високими операційними витратами на електроенергію та обслуговування. Натомість, запропонована архітектура на базі SDR та адаптивних антенних решіток дозволяє знизити необхідний енергетичний бюджет системи на 10–15 дБ, що еквівалентно зменшенню споживаної потужності у 10–30 разів порівняно з конвенційними методами загороджувальних завад, безпосередньо трансформуючись у фінансову економію та можливість використання компактних, автономних джерел живлення.

Найвища релевантність та ефективність запропонованого рішення підтверджується здатністю системи адаптуватися до динамічного

ландшафту загроз без необхідності фізичної заміни обладнання, що є критичним фактором в умовах швидкої еволюції цифрових протоколів передачі даних. Використання метрик оперативної ефективності МОЕ, таких як вектор похибки модуляції (EVM) та коефіцієнт бітових помилок (BER), дозволяє системі автоматизовано верифікувати успішність придушення каналу витоку інформації в реальному часі, гарантуючи досягнення цілей безпеки при мінімальному рівні електромагнітного забруднення середовища.

Це вирішує проблему «електромагнітної сумісності», дозволяючи розгортати системи активного захисту в насичених офісних просторах без порушення роботи легітимних мереж Wi-Fi та мобільного зв'язку, що раніше було недосяжним для широкосмугових систем і призводило до непрямих економічних збитків через зупинку бізнес-процесів.

З точки зору **легкості імплементації**, перехід на програмно-визначену архітектуру дозволяє використовувати уніфіковані комерційно доступні апаратні платформи, які є значно дешевшими за спеціалізовані військові комплекси РЕБ, але забезпечують достатній динамічний діапазон та обчислювальну потужність для задач внутрішньооб'єктового захисту. Відсутність потреби у складній кабельній інфраструктурі та можливість інтеграції в наявні локальні мережі робить процес розгортання системи швидким та маловитратним, не вимагаючи капітальної реконструкції приміщень. Програмна природа SDR забезпечує **безпрецедентну легкість масштабування системи**, коли додавання нових частотних діапазонів або алгоритмів протидії новітнім стандартам зв'язку (наприклад, 5G або новим протоколам IoT) реалізується шляхом дистанційного оновлення програмного забезпечення (Firmware Update), а не закупівлею нових блоків, що перетворює систему на довгострокову інвестицію зі збереженням актуальності протягом багатьох років.

Мережева структура дозволяє об'єднувати окремі малопотужні модулі в єдиний координований кластер, що забезпечує гнучке покриття об'єктів будь-якої площі та конфігурації, роблячи технологію доступною як для малого бізнесу, так і для великих режимних об'єктів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Poisel, Richard A. *Modern Communications Jamming Principles and Techniques*. 2nd Edition. Artech House, 2011. (Фундаментальна праця з теорії радіоелектронного придушення).
2. Adamy, David L. *EW 101: A First Course in Electronic Warfare*. Artech House, 2001. (Базові принципи розрахунку енергетики завад та рівнянь дальності).
3. Torrieri, Don J. *Principles of Spread-Spectrum Communication Systems*. 4th Edition. Springer, 2018. (Теорія завадостійкості FHSS та DSSS систем).
4. Proakis, John G., and Salehi, Masoud. *Digital Communications*. 5th Edition. McGraw-Hill, 2008. (Класична теорія BER для QPSK/FSK в каналах з AWGN).
5. Amuru, S. D., & Buehrer, R. M. "Optimal Jamming Against Digital Modulation." *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, 2015. (Дослідження ефективності "розумних" завад проти QPSK).
6. Vingson, N. A., & Muhammad, V. *Model to Calculate the Effectiveness of an Airborne Jammer on Analog Communications*. Master's Thesis, Naval Postgraduate School, Monterey, CA, USA, 2005. (Аналіз ефекту захоплення в FM приймачах).
7. Sen, Cem. *Digital Communications Jamming*. Master's Thesis, Naval Postgraduate School, Monterey, CA, USA, 2000. (Моделювання BER для різних типів модуляції в MATLAB).
8. Grootsholten, R. *Jamming of Tactical Data Links*. Master's Thesis, Swedish Defence University (Försvarshögskolan), 2023. (Сучасні сценарії свіп-завад та моделювання в VOACAP/MATLAB).
9. Ali, A. S., et al. "JamRF: Performance Analysis, Evaluation, and Implementation of RF Jamming Over Wi-Fi." *IEEE Access*, vol. 10, 2022. (Практичні аспекти реалізації завад на базі SDR).

10. Lau, F. C. M., & Tse, C. K. "Performance of chaos-based digital communication systems in the presence of a pulsed-noise jammer." *Circuits, Systems, and Signal Processing*, vol. 23, 2004.
11. MathWorks Documentation. *Communications Toolbox User's Guide*. (Опис блоків Simulink: Bernoulli Binary Generator, QPSK Modulator Baseband, AWGN Channel).
12. US Department of Commerce, NTIA. *Jammer Effectiveness Model (JEM) Technical Manual*. Institute for Telecommunication Sciences, Boulder, CO.
13. Збірник наукових праць "Сучасний захист інформації". Державний університет інформаційно-комунікаційних технологій (Київ).
14. Вісник НТУУ "КПІ". Серія: Радіотехніка, Радіоапаратобудування. (Статті щодо методів підвищення завадостійкості радіоканалів).
15. НД ТЗІ 2.5-004-99. *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу*. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України, 1999.

ДОДАТКИ

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

-
- Конвенційні радіозакладні пристрої залишаються реальною загрозою витоку інформації в цивільній, корпоративній та державній сферах.
 - Такі пристрої використовують аналогову та просту цифрову модуляцію, працюють у доступних діапазонах і можуть бути складними для оперативного придушення.
 - Широкопasmове зашумлення не завжди є енергоефективним, тому актуальною є цільова постановка завад під конкретний тип сигналу.
 - Технології SDR та адаптивні антенні системи створюють основу для гнучких систем активного захисту інформації.

-
- Мета: дослідження, розробка та кількісна оцінка ефективності цільових способів формування завадових сигналів для протидії конвенційним РЗП.
 - Технологічна база: програмно-кероване радіо (SDR) та адаптивні антенні системи.
 - Об'єкт: процес забезпечення інформаційної безпеки радіоелектронних засобів в умовах протидії РЗП.
 - Предмет: способи формування завадових сигналів та методи просторово-часової адаптації для максимізації ефективності придушення.

-
- Провести огляд і класифікацію конвенційних радіозакладних пристроїв та їхніх технічних характеристик.
 - Розробити математичні моделі і проаналізувати спектральну щільність потужності основних типів завадових сигналів.
 - Сформулювати критерії оцінки ефективності протидії: BER, J/S та EVM.
 - Виконати імітаційне моделювання впливу цільових завад на сигнали з різними типами модуляції.
 - Порівняти ефективність цільових способів протидії з класичними широкосмуговими завадами.

-
- Розділ 1: аналіз об'єкта протидії та основи формування сигналів.
 - Розділ 2: теоретичні основи радіоелектронної боротьби та формування завадових сигналів.
 - Розділ 3: SDR-архітектура, адаптивні антенні системи та реалізація.
 - Розділ 4: моделювання, оцінка ефективності та проектні рішення.
 - Обсяг роботи: 69 сторінок, 9 рисунків, 1 таблиця, 15 джерел.

-
- До об'єкта протидії належать приховані радіомікрофони, мініатюрні бездротові камери та пристрої негласного знімання інформації.
 - Значна частина таких РЗП працює в загальнодоступних або малоконтрольованих діапазонах частот, наприклад в UHF-смузі.
 - Типові рівні потужності є малими або середніми, що ускладнює виявлення лише за енергетичними ознаками.
 - Ефективна протидія повинна враховувати тип модуляції, частоту, рівень сигналу та умови поширення.

-
- Для аналогових РЗП характерні амплітудна, частотна та фазова модуляції (AM, FM, PM).
 - Для цифрових РЗП характерні FSK, QPSK та кодово-імпульсна модуляція (KIM).
 - Різні типи модуляції по-різному реагують на завадові сигнали, тому потрібен диференційований підхід до придушення.
 - Саме це обґрунтовує перехід від універсального зашумлення до цільового формування завади.

-
- У роботі розглянуто шумоподібні завади, завади типу безперервна хвиля (CW) та лінійно-частотно-модульовані завади типу Sweep.
 - Шумоподібні сигнали забезпечують широке покриття спектра, але потребують значних енергетичних витрат.
 - CW-завада концентрує енергію у вузькій смузі та є доцільною для аналогових і простих цифрових сигналів.
 - Sweep-завада періодично проходить через робочу смугу цілі та дає змогу цілеспрямовано порушувати роботу каналу зв'язку.

-
- BER (Bit Error Rate) характеризує імовірність бітових помилок у прийнятому цифровому повідомленні.
 - J/S (Jamming-to-Signal Ratio) визначає співвідношення потужностей завади та корисного сигналу.
 - EVM (Error Vector Magnitude) дозволяє оцінити спотворення сигнальної сузір'я та якість модуляції.
 - Поєднання BER, J/S та EVM формує формалізовану основу кількісного аналізу ефективності завадового впливу.

-
- SDR забезпечує програмну генерацію завад із керованими параметрами частоти, смуги, модуляції та спектральної щільності потужності.
 - Гнучкість SDR дає змогу швидко адаптувати систему до різних типів радіозакладних пристроїв без заміни апаратури.
 - У роботі обґрунтовано застосування SDR для формування оптимальної СЩП завади з мінімально необхідним J/S.
 - Це підвищує енергоефективність активного захисту інформації.

-
- Адаптивні антенні системи забезпечують просторову селективність та концентрацію енергії у напрямку на ціль.
 - Просторово-часова адаптація дозволяє мінімізувати вплив на сторонні радіосистеми та підвищити ефективність протидії.
 - Поєднання SDR і адаптивної антенної решітки формує архітектуру високоенергоєфективної системи активного захисту.
 - Такий підхід особливо доцільний для пригнічення малопотужних конвенційних РЗП.

-
- Для оцінки ефективності протидії розроблено імітаційний стенд у середовищі MATLAB/Simulink.
 - Моделювалися сценарії впливу цільових завад на сигнали з різними типами модуляції.
 - Ураховано умови багатопроменового поширення та канали типу Райса і Релея.
 - Такий підхід дозволив наблизити результати до реальних умов функціонування РЗП.

-
- Для аналогових РЗП цільові завади типу CW і Sweep продемонстрували високу ефективність придушення.
 - Зосередження енергії у робочій смузі цілі дозволяє досягати необхідного впливу за нижчих енергетичних витрат, ніж при широкосмуговому зашумленні.
 - Ефективність оцінюється за погіршенням якості приймання та необхідним рівнем J/S.
 - Це підтверджує доцільність застосування цільових способів формування завад проти аналогових каналів.

-
- Для цифрових РЗП з модуляціями FSK та QPSK оцінювався вплив завад за критеріями BER та EVM.
 - Показано, що цільові завади здатні істотно збільшувати коефіцієнт бітових помилок і спотворювати сигнальну сузір'я.
 - Це свідчить про зростання ефективності придушення навіть за помірних значень J/S.
 - Отримані результати підтверджують переваги керованого формування завад для цифрових систем зв'язку.

-
- Для аналогових та простих цифрових РЗП доцільно застосовувати вузькосмугові цільові завади типу CW або Multi-tone.
 - Для випадків змінної частоти або невизначеної смуги доцільно використовувати Sweeper-завади з оптимізованою швидкістю перебігу.
 - Вибір параметрів завади має базуватися на типі модуляції цілі, вимогах до J/S та допустимих енергетичних витратах.
 - Інтеграція SDR з адаптивною антенною системою є перспективним напрямом побудови активних систем ТЗІ.

-
- Проаналізовано конвенційні радіозакладні пристрої, їх сигнали та вразливості у контексті технічного захисту інформації.
 - Розроблено підхід до формування цільових завадових сигналів на базі SDR та адаптивних антенних систем.
 - За критеріями BER, J/S та EVM підтверджено ефективність цільових завад типу CW і Sweeper порівняно з класичним широкосмуговим зашумленням.
 - Запропоновані рішення можуть бути використані для проектування енергоефективних систем активної протидії радіозакладним пристроям.