НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО

Декан факультету
Інформаційних технологій

_____ / Болбот І.М., д.т.н., проф. /
підпис ПІБ, вчене звання і ступінь

«___» _____ 2025 р.

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри
Комп'ютерних систем, мереж
та кібербезпеки

_____ / Касаткін Д.Ю., к.пед.н., доц. /
підпис ПІБ, вчене звання і ступінь

«___» _____ 2025 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

На тему «Дослідження стійкості БПЛА до електромагнітних перешкод»

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерні системи та мережі

Орієнтація освітньої програми Освітньо-професійна

Гарант освітньої програми

к. фіз.-мат. н., доц. _____ Нікітенко Є. В.
(науковий ступінь та вчене звання) (підпис) (ПІБ)

Керівник магістерської кваліфікаційної роботи

к. фіз.-мат. н., доц. _____ Нікітенко Є. В.
(науковий ступінь та вчене звання) (підпис) (ПІБ)

Виконав _____ Левченко Р. Р.
(підпис) (ПІБ студента)

КИЇВ – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж і кібербезпеки
_____ / Касаткін Д.Ю., к.пед.н., доц. /
підпис ПІБ, вчене звання і ступінь
«___» _____20___р.

З А В Д А Н Н Я
до виконання магістерської кваліфікаційної роботи здобувачу

Левченко Родіону Руслановичу
(прізвище, ім'я, по батькові)

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма Комп'ютерні системи та мережі

Орієнтація освітньої програми Освітньо-професійна

Тема магістерської кваліфікаційної роботи Дослідження стійкості БПЛА до електромагнітних перешкод

Затверджена наказом ректора НУБіП України від "29" жовтня 2024р. № 1941 «С»

Термін подання завершеної роботи на кафедру 14. 11. 2025р.

Вихідні дані до магістерської кваліфікаційної роботи _____

Перелік питань, що підлягають дослідженню:
1. _____
2. _____
3. _____

Перелік графічних документів (за потреби) Презентація виконаної роботи.

Дата видачі завдання " 29 **"** жовтня 2025р.

Керівник магістерської кваліфікаційної роботи _____ Нікітенко Є. В.
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Левченко Р.Р.
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Опрацювання вихідних матеріалів та аналіз сучасних досліджень у сфері БПЛА	31.10.2025	Виконано
2	Аналіз класифікацій джерел електромагнітних перешкод, типів БПЛА та каналів передавання керування й телеметрії	03.11.2025	Виконано
3	Дослідження типів електромагнітних перешкод та визначення механізмів їх впливу на радіоканал керування й телеметрії БПЛА	05.11.2025	Виконано
4	Дослідження моделей каналів зв’язку БПЛА для оцінювання стійкості до перешкод	08.11.2025	Виконано
5	Порівняльний аналіз результатів моделювання та визначення критичних режимів, за яких відбувається втрата стійкості БПЛА	10.11.2025	Виконано
6	Оформлення пояснювальної записки	12.11.2025	Виконано
7	Підготовка графічного матеріалу та презентації	13.11.2025	Виконано
8	Подання завершеної роботи на кафедру	14.11.2025	Виконано

Студент _____ Левченко Р.Р.
(підпис) (ініціали та прізвище)

Керівник роботи _____ Нікітенко Є. В.
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка: 79 сторінок, 14 рисунків, 6 таблиць, 23 джерела.

БЕСПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ, ЕЛЕКТРОМАГНІТНІ ПЕРЕШКОДИ, ЗАВАДОСТІЙКІСТЬ, РАДІОЗВ’ЯЗОК, РЕБ, НАВІГАЦІЙНІ СИСТЕМИ, EMC, FPV-ДРОН.

Об'єкт дослідження – безпілотний літальний апарат як радіоелектронна система, що піддається впливу електромагнітних завад.

Мета роботи – дослідити процес функціонування безпілотного літально го апарата в умовах дії електромагнітних перешкод.

Робота складається з чотирьох розділів.

Перший розділ надає базові відомості про принципи роботи радіозв’язку. Описано фізичну архітектуру БПЛА, основні типи каналів зв’язку та сучасні технології комунікації, що використовуються під час керування безпілотними платформами.

Другий розділ розглядає природу електромагнітних перешкод, їх класифікацію, механізми впливу на радіоелектронні системи та канали зв’язку. Проаналізовано ризики для БПЛА, що виникають у завадному середовищі, включаючи зниження якості сигналу, втрату керування.

Третій розділ присвячено технічним і програмним методам підвищення стійкості каналів зв’язку БПЛА. Розглянуто підходи до зниження дії завад. Наведено приклади рішень, що підвищують завадостійкість радіоканалів.

Четвертий розділ надає практичну складову дослідження. Подано графічні залежності, розрахунки наведеної напруги, оцінку ефективності фільтраційних засобів та визначення критичних частотних діапазонів.

ABSTRACT

Explanatory note: 79 pages, 14 figures, 6 tables, 23 sources.

UNMANNED AERIAL VEHICLES, ELECTROMAGNETIC INTERFERENCE, INTERFERENCE IMMUNITY, RADIO COMMUNICATION, ELECTRONIC WARFARE, NAVIGATION SYSTEMS, EMC, FPV-DRONE.

Object of research – an unmanned aerial vehicle as a radio-electronic system exposed to electromagnetic interference.

Purpose of the work – to study the operation of an unmanned aerial vehicle under the influence of electromagnetic disturbances.

The work consists of four chapters.

The first chapter provides fundamental information on radio communication principles. It describes the physical architecture of UAVs, the main types of communication channels, and modern technologies used to control unmanned platforms.

The second chapter examines the nature of electromagnetic interference, its classification, and the mechanisms by which it affects radio-electronic systems and communication channels. It analyzes risks for UAVs operating in an interference-rich environment, including signal degradation and loss of control.

The third chapter is devoted to technical and software methods for increasing the resilience of UAV communication channels. It considers approaches to reducing the impact of interference and provides examples of solutions that enhance the interference immunity of radio channels.

The fourth chapter presents the practical component of the research. It includes graphical dependencies, calculations of induced voltage, evaluation of filtering efficiency, and identification of critical frequency ranges.

ЗМІСТ

ВСТУП

Упродовж останніх десятиліть безпілотні літальні апарати (БПЛА) перетворилися на один із найдинамічніших напрямів розвитку сучасної авіаційної техніки. Їхня універсальність, відносна дешевизна та можливість виконання завдань без участі пілота роблять такі системи незамінними у цивільних, наукових і військових сферах. Водночас із розширенням сфер застосування підвищуються вимоги до надійності функціонування БПЛА в умовах дії різноманітних зовнішніх факторів, серед яких ключову роль відіграють електромагнітні завади.

Електромагнітне середовище, у якому працює безпілотник, є насиченим безліччю джерел випромінювання. До них належать лінії електропередач, базові станції мобільного зв’язку, радіолокатори, радіостанції, промислові установки, а також цілеспрямовані системи радіоелектронної боротьби. Усі ці джерела здатні створювати завади різного типу:

широкосмугові (імпульсні) — короткі електромагнітні сплески, що спричиняють тимчасові збої в роботі електроніки;

вузькосмугові (періодичні) — випромінювання на певних частотах, яке заважає прийому або передачі сигналів;

індукові та кондуктивні — струми, що потрапляють у провідники через наведення або прямий контакт;

високоенергетичні впливи — потужні імпульси, здатні вивести з ладу мікросхеми та контролери.

Такі впливи можуть спричинити втрату стійкого каналу зв’язку між оператором і літальним апаратом, порушення навігації, некоректну роботу сенсорних систем, або навіть повну втрату керованості. Особливо небезпечними є ситуації, коли безпілотник діє у зоні потужних радіопередавачів чи військових систем радіоелектронного придушення.

Таким чином аналіз впливу цілеспрямованих електромагнітних перешкод на канали зв’язку безпілотних літальних апаратів становить суттєвий етап у підвищенні рівня їхньої надійності та ефективності застосування. Це має

особливе значення для таких сфер, як медична логістика, моніторинг стану довкілля, управління техногенними ризиками у нафтогазовій промисловості, а також у військових та розвідувальних операціях.

У даному дослідженні буде продемонстровано, що підвищення стійкості каналів зв’язку безпілотних літальних апаратів до навмисних завад можливе за рахунок використання сучасних технічних і програмних рішень — зокрема методів протидії інтерференції, систем криптографічного захисту, механізмів виявлення атак та алгоритмів виправлення помилок у переданих даних.

Метою даної роботи є всебічне дослідження впливу електромагнітних завад на системи керування безпілотних літальних апаратів, а також розроблення підходів до підвищення їх завадостійкості. У межах цієї мети передбачається:

– вивчити фізичну природу та класифікацію електромагнітних перешкод;

– проаналізувати чутливість основних вузлів БПЛА (контролера, приймача, системи живлення) до дії ЕМ-поля;

– виконати моделювання впливу електромагнітного випромінювання різної інтенсивності на роботу електронних компонентів;

– розробити рекомендації щодо підвищення стійкості системи управління за допомогою екранування, фільтрації та резервування сигналів.

Практична цінність дослідження полягає у можливості застосування отриманих результатів під час проектування та випробувань БПЛА, що використовуються у складних радіоелектронних умовах. Запропоновані методи підвищення стійкості можуть бути використані для вдосконалення захисту каналів зв’язку, стабілізації контролерів і підвищення загальної надійності систем безпілотних платформ.

РОЗДІЛ 1
ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО РАДІОЗВ'ЯЗОК ТА БПЛА

1.1 Що таке радіохвиля

Радіохвилі (раніше їх називали герцовими) є видами електромагнітного випромінювання, що характеризуються найнижчими частотами та найбільшими довжинами хвиль у всьому електромагнітному спектрі. Зазвичай їх частота становить менше 300 гігагерц (ГГц), а довжина хвилі перевищує 1 міліметр — приблизно як товщина зернини рису. Радіохвилі з частотами понад 1 ГГц і довжиною хвилі менше 30 сантиметрів належать до діапазону мікрохвиль.

Як і всі електромагнітні хвилі, радіохвилі у вакуумі поширюються зі швидкістю світла, а в атмосфері Землі — трохи повільніше. Їхнє утворення відбувається внаслідок прискореного руху заряджених частинок, наприклад під час змінних електричних струмів. У природі радіохвилі випромінюються блискавками, різними космічними об’єктами, а також входять до складу теплового (або «чорного тілового») випромінювання, яке випускають усі нагріті тіла. [1]

Радіохвилі штучно створюються за допомогою електронного пристрою — передавача, який з’єднаний з антеною, що випромінює ці хвилі. Для прийому сигналу використовується інша антена, під’єднана до приймача, який обробляє отримане випромінювання.

У сучасних технологіях радіохвилі мають надзвичайно широке застосування: від стаціонарного й мобільного радіозв’язку до мовлення, радарів, навігаційних систем, супутникового зв’язку та бездротових комп’ютерних мереж.

Різні діапазони частот мають свої особливості поширення в атмосфері Землі:

- Довгі хвилі здатні огинати перешкоди, такі як гори, і слідувати за кривизною поверхні Землі — це так звані поверхневі хвилі.

- Середні та коротші хвилі можуть відбиватися від іоносфери та повертатися на поверхню далеко за горизонт — утворюючи небесні хвилі.

- Дуже короткі хвилі (дециметрові та сантиметрові) поширюються майже прямолінійно, майже не огинаючи об’єкти, тому їх дальність обмежена межами прямої видимості.

1.2 Дизайн БПЛА та будова систем управлінь

Пілотовані та безпілотні літальні апарати одного типу зазвичай мають схожу конструкцію та базові компоненти. Основна різниця полягає у відсутності кабіни екіпажу й систем життєзабезпечення в безпілотних моделях. Деякі БПЛА несуть корисне навантаження (наприклад, камеру), маса якого значно менша за вагу людини, тому їхні розміри можуть бути суттєво меншими. Навіть озброєні військові дрони, попри вагомі корисні навантаження, зазвичай легші за свої пілотовані аналоги з подібним арсеналом.

Цивільні малі БПЛА не мають життєво важливих систем, тому їх можна виготовляти з легших і менш міцних матеріалів, застосовуючи спрощені електронні схеми керування. Серед малих дронів особливо поширена конфігурація квадрокоптера, яка майже не використовується у пілотованій авіації. Завдяки мініатюризації для таких апаратів можна застосовувати малопотужні, але ефективні рушійні системи — наприклад, електродвигуни з живленням від акумуляторів. [2]

БПЛА використовують радіозв’язок для керування, передавання відео та обміну іншими видами даних. Перші моделі мали лише вузькосмуговий канал для передачі команд (uplink), а згодом було додано і зворотній (downlink). Такі двонапрямні вузькосмугові канали забезпечували передачу команд управління (C&C) і телеметрії — даних про стан систем апарата до оператора.

У сучасних безпілотних системах зазвичай необхідна передача відеопотоку, тому замість кількох окремих каналів для команд, телеметрії та відео використовується широкосмуговий зв’язок, який здатен передавати всі типи даних одночасно. Такі канали підтримують якісне обслуговування (QoS) і працюють з трафіком TCP/IP, що дозволяє маршрутизувати сигнали навіть через Інтернет.

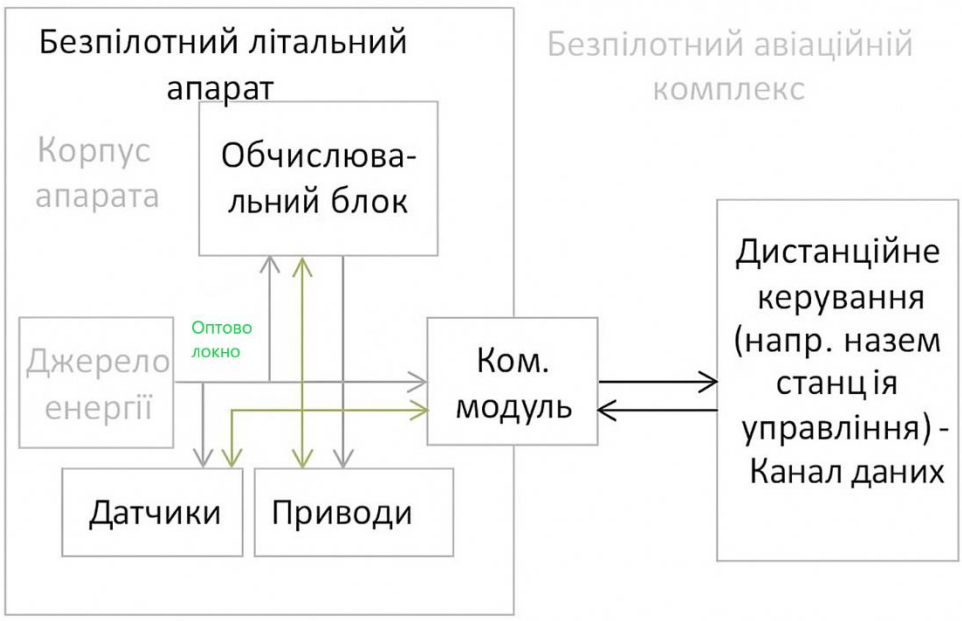

Рис 1.1 - Загальна фізична структура БПЛА

Сигнал керування з боку оператора може надходити з різних джерел:

- Наземна станція керування (GCS) — оператор із радіопередавачем, комп’ютером, смартфоном або планшетом, який безпосередньо контролює політ.

- Віддалені мережеві системи, наприклад двосторонній супутниковий зв’язок, який застосовують у військових системах. У цивільному секторі вже використовується передача відео через мобільні мережі, а також експериментується пряме керування дроном через стільникову мережу LTE або 5G.

- Інший літальний апарат, що виконує роль ретранслятора або мобільної станції управління — концепція взаємодії пілотованих і безпілотних платформ (MUM-T).

Сучасні стандарти зв’язку враховують потреби БПЛА: у стандарті 5G передбачено зменшену затримку до 1 мс і підвищену надійність у режимі ultra-reliable low-latency communications (URLLC).

Також активно розвивається технологія Remote ID, яка забезпечує координацію між безпілотниками: апарати транслюють свої координати, що дозволяє іншим дронам уникати зіткнень і здійснювати безпечну навігацію. [3]

1.3 Радіопротоколи зв’язку БПЛА

У сучасних системах безпілотних літальних апаратів (БПЛА) радіозв’язок відіграє критичну роль — він забезпечує передавання команд від наземної станції до апарата, а також надходження телеметрії, даних сенсорів, відеопотоку та стану системи. Вибір протоколу зв’язку безпосередньо впливає на затримку, надійність, просторово-частотну стійкість, пробивну здатність у середовищі з перешкодами, можливість двонапрямленої комунікації та безпеку. У цьому розділі розглянуто як застарілі, так і актуальні радіопротоколи, що застосовуються у БПЛА, їхню архітектуру, переваги, недоліки та практичні аспекти використання.

Для ефективного зв’язку БПЛА важливо, щоб протокол відповідав таким вимогам:

- Низька затримка (latency) — необхідна для оперативного управління в реальному часі.
- Висока надійність — мінімальна кількість втрат пакетів, стабільне з’єднання у високодинамічному середовищі.
- Здатність працювати у завадному середовищі — багатошляхове поширення сигналу, зміни орієнтації антен, рух апарата.
- Двонаправлена передача (або хоча б зворотний канал) — для

телеметрії, стану системи, зворотного зв’язку.

- Масштабованість каналів і інтеграція з контролерами — підтримка багатьох каналів керування, додаткових датчиків.
- Безпека — автентифікація, шифрування, захист від підслуховування та перехоплення команд (особливо важливо у військових/розвідувальних застосуваннях).
- Інтеграція з апаратною платформою і автопілотом — зручність підключення, підтримка контролерів, прошивок.

Нижче — огляд та порівняльна таблиця кількох протоколів: застарілих та сучасних.

PPM (Pulse Position Modulation) - іноді відомий як CPPM або PPMSUM, використовує один провід для багатьох каналів, передаючи імпульси підставного сигналу. Переваги: одна лінія сигналу замість кількох, простота реалізації. Недоліки: аналоговий формат, більші ймовірності джиттера, обмежена кількість каналів/швидкість передавання. У контексті сучасних БПЛА — застарілий вибір, більше використовувався у хобі-моделізмі. Наприклад, типовий кадр PPM має довжину ~22,5 мс, далі декодування каналів.

CRSF (Crossfire Serial Protocol) - Протокол CRSF, розроблений TBS (Team Black Sheep) для їхньої системи Crossfire, використовується й у системах ExpressLRS. Він забезпечує двонаправлену передачу: як команди керування, так і телеметрій. Переваги: висока швидкість оновлення каналів, інтегрований зворотний канал для телеметрії, надійність. Недоліки: вимагає сумісного приймача/передавача, налаштування UART та підтримки з боку прошивки автопілота.

ELRS (ExpressLRS) - відкритий протокол радіозв’язку з акцентом на низьку затримку та велику дальність, що використовує LoRa або FSK-модуляцію. У межах ELRS часто використовується CRSF-канал на фізичному рівні, або ж можливість взаємодії з протоколом MAVLink через UART-інтерфейс. Переваги: дуже мала затримка, великі дальності (> 100 км в деяких конфігураціях), гнучкість під різні частоти. Недоліки: іноді складніша

конфігурація, потребує актуальної прошивки та апаратури.

MAVLink - протокол прикладного рівня, широко застосований у середовищі БПЛА, зокрема у системах автопілота (наприклад, ArduPilot, PX4). Цей протокол описує набір повідомлень між апаратом і станцією керування (GCS). Основний акцент — на семантиці даних, а не на специфіках радіозв'язку фізичного рівня. Переваги: стандартність, інтеграція з програмним забезпеченням, можливість підключення до GCS. Недоліки: сам по собі не охоплює фізичний канал радіозв'язку, не завжди оптимізований для наднизької затримки чи завадостійкості. У деяких середовищах критичними є питання безпеки (наприклад, вразливості повідомляються).

Таблиця 1.1

Порівняльна таблиця протоколів зв'язку

Протокол	**Сфера застосування**	**Основні характеристики**	**Переваги**	**Недоліки**
PPM	Хобі-моделі, прості БПЛА	Аналогова мультиканальна передача імпульсів	Простота, низька вартість	Вища затримка, велика кількість проводів/каналів, обмежена швидкість
CRSF	Сучасні FPV/БПЛА, дальній радіозв'язок	Двонаправлений цифровий протокол, телеметрія	Низька затримка, телеметрія, висока надійність	Потрібна сумісна апаратура та налаштування
ELRS	Дальній зв'язок, FPV, аматорські та напівпрофесійні БПЛА	LoRa/FSK фізичний рівень + цифровий протокол	Велика дальність, відкритий протокол, низька затримка	Конфігурація, потребує актуальної прошивки
MAVLink	Автопілоти, наземні станції, обмін повідомленнями між системами	Протокол обміну даними прикладного рівня	Стандарт, велика підтримка, гнучкість	Не визначає фізичний канал, може вимагати додаткових модулів

Тому вибір радіопротоколу для БПЛА — це не тільки питання сучасності або «новизни», це питання масштабування, середовища застосування, вимог до затримки, надійності та безпеки. У практичних умовах (особливо у військово-

цивільному контексті України) пріоритетами стають протоколи, які дозволяють працювати із двонаправленою телеметрією, мають високу завадостійкість та можуть бути інтегровані з автопілотами. Протоколи типу PPM, хоча й історично важливі, вже поступаються у складніших сценаріях. Сучасні рішення (CRSF, ELRS, MAVLink) забезпечують такий рівень можливостей, який відповідає викликам сучасного повітроплавання безпілотних систем.

1.4 Принцип функціонування каналу зв'язку

БПЛА застосовуються для широкого спектра завдань, що зумовлює потребу у використанні різних типів каналів зв'язку. Нижче наведено основні варіанти каналів, які можуть використовуватися для передавання інформації між дроном і наземною інфраструктурою.

RF-канали — це канали зв'язку, що передають дані за допомогою радіохвиль між БПЛА та наземним пунктом управління. Вони можуть функціонувати в різних частотних діапазонах, залежно від особливостей застосування та необхідної пропускної здатності.

Основні характеристики RF-каналів:

- робочий частотний діапазон;
- доступна пропускна здатність каналу;
- швидкість передавання інформації;
- максимальна дальність стабільного зв'язку;
- мінімальний рівень сигналу, що здатний розпізнати приймач.

RF-канали мають свої переваги та недоліки.

Переваги таких каналів полягають у значній зоні покриття, високій швидкості передавання інформації та великій пропускній спроможності.

Серед недоліків варто відзначити підвищену чутливість до електромагнітних перешкод, можливість блокування або спотворення сигналу, а також порівняно високе енергоспоживання апаратури.

Оптичні канали зв’язку є різновидом систем передавання даних, у яких інформація переноситься світловими сигналами. Такі канали забезпечують роботу на значних дистанціях і характеризуються високою пропускною здатністю.

Основними параметрами оптичних каналів зв’язку є:

- робоча довжина хвилі випромінювання;
- пропускна здатність лінії;
- швидкість передавання інформації;
- максимально можлива дальність роботи.

Обмін даними між БПЛА та наземною станцією здебільшого здійснюється через радіочастотні канали, до складу яких входять приймальні та передавальні модулі. Радіочастотний канал БПЛА може використовувати різні схеми модуляції та методи кодування — зокрема амплітудну (АМ), частотну (ЧМ) або фазову (ФМ) модуляції. Такі підходи дають змогу підвищити стійкість системи до завад, оскільки застосовуються розширені засоби виправлення та відновлення сигналу. Водночас складність таких методів робить канал більш чутливим до навмисних радіоперешкод, коли зловмисник може сформувати спеціальні сигнали, здатні погіршити роботу зв’язку або повністю його порушити. Дальність дії радіоканалу БПЛА визначається комплексом факторів: вихідною потужністю передавачів, висотою польоту апарата, рельєфом місцевості, наявністю або відсутністю завад, а також характеристиками застосованих частотних діапазонів і типом антен, встановлених на борту та на наземному пункті управління [4]

У таблиці 1.2 наведено технічні характеристики каналів зв’язку безпілотних повітряних апаратів. До переліку параметрів включено швидкість передавання даних, робочий частотний діапазон, максимальну дальність сигналу, тип застосованої антени та інші ключові показники.

Таблиця 1.2

Основні технічні параметри каналів зв’язку БПЛА

Технічна характеристика	Опис
Робочий частотний діапазон	Частотний діапазон, у межах якого працює канал зв’язку БПЛА.
Швидкість обміну даними	Максимальна швидкість передавання інформації через канал.
Дальність каналу зв’язку	Найбільша відстань, на якій забезпечується стабільний зв’язок.
Маса та габарити обладнання	Розміри й вага антен та інших елементів системи зв’язку.
Тип передавального модуля	Вид передавача, що використовується для формування сигналу.
Перешкодозахищеність	Стійкість каналу до впливу зовнішніх радіоперешкод.
Буферизація даних	Обсяг даних, який система може тимчасово зберігати під час передачі.
Метод модуляції сигналу	Алгоритм, за яким здійснюється модуляція інформаційного сигналу.
Тип антени	Конструкція та формат антени, що застосовується у каналах зв’язку БПЛА.
Стійкість приймального тракту	Здатність приймача працювати коректно за наявності завад.

Пряма видимість між БПЛА та наземним пунктом керування забезпечується шляхом збільшення висоти польоту апарата та оптимального налаштування кута підйому антени наземної станції. Передавання даних на дистанцію понад 300 км можливе лише за застосування ретрансляторів, систем супутникового зв’язку або стаціонарної інфраструктури передачі інформації.

Більшість комерційних дронів використовують стандартну схему прямого зв’язку «земна станція — БПЛА», коли обмін даними відбувається без посередників. Для збільшення зони надійного зв’язку було створено спеціальну архітектуру передачі телеметрії, у якій наземна станція отримує дані та формує корекційні команди. Проте радіус дії такої системи залишається обмеженим можливостями наземного обладнання, і один з дронів у групі може виходити за межі стабільного прийому.

Оскільки радіоканал зв’язку БПЛА завжди обмежений дальністю, а також може погіршуватися через рельєф місцевості чи забудову, неможливо збільшити його до фізичної межі радіогоризонту. Тому для передачі даних на більші відстані застосовуються додаткові системи ретрансляції. Система зв’язку може працювати у двох основних режимах:

Режим ретрансляції - система діє як проміжна ланка між дроном та наземною станцією. Ретранслятор розширює ефективну дальність каналу на власний радіус дії, дозволяючи БПЛА працювати на значно більших дистанціях порівняно з прямим зв’язком. Цей режим активується, коли система не бачить підключення до автопілота дрона чи наземної станції, або коли вона працює від автономного живлення.

Режим прямого зв’язку - у цьому випадку обмін даними відбувається безпосередньо між БПЛА та наземним обладнанням. Дальність роботи обмежується потужністю радіомодуля, проте затримка передачі мінімальна. Режим активний тоді, коли система під’єднана одночасно до обох вузлів — і до дрона, і до станції керування.

Для розширення радіуса зв’язку може застосовуватися технологія LoRa (Long Range), розроблена компанією Semtech. Вона є основою багатьох IoT-рішень і забезпечує передачу даних на великі відстані при низькому енергоспоживанні. Пристрої LoRa працюють у мережах LPWAN, а відкритий протокол LoRaWAN дає змогу створювати масштабовані IoT-системи, у яких використовується енергоефективний та захищений канал зв’язку. Модуляція LoRa ґрунтується на методі розширення спектра (SSM) та варіації частотної модуляції CSS (chirp spread spectrum), із вбудованою прямою корекцією помилок FEC. Дані передаються у вигляді широкосмугових імпульсів із частотою, що змінюється в часі. На відміну від прямого розширення спектра, технологія LoRa зменшує вимоги до стабільності частоти та дозволяє використовувати недорогі кварцові резонатори, підвищуючи стійкість приймача до частотних відхилень.

1.5 Принцип дії ЕМ завад та їх вплив на радіоелектричні пристрої

У сучасному світі, де бездротові системи й радіоелектроніка складають основу багатьох критично важливих інфраструктур, проблема електромагнітних завад (EMI — electromagnetic interference) та навмисного радіозаглушення (jamming) набуває особливого значення. Сам по собі термін «електромагнітна завада» охоплює будь-яке небажане електромагнітне випромінювання, яке порушує нормальну роботу електронних пристроїв. Згідно з літературою, EMI «є явищем, в якому електромагнітне випромінювання одного пристрою порушує роботу іншого сусіднього електронного ланцюга шляхом кондукційної чи радіаційної передачі». [5]

Пристрій, який навмисно або ненавмисно створює значну кількість ЕМ-випромінювання, може викликати зниження співвідношення корисного сигналу до шуму (SNR — signal-to-noise ratio) у приймачі і, як наслідок, погіршення демодуляції, підвищення кількості помилок, втрату зв’язку або навіть пошкодження електроніки. У публікації про вплив ЕМ-завад на системи зв’язку й радарів зазначено, що «у сучасних умовах бойових дій ефективність систем зв’язку, радіонавігації й розвідки значною мірою залежить від здатності протидіяти електромагнітним перешкодам».

Коли розглянути пристрої зв’язку, безпілотні літальні апарати, радари чи телекомунікаційні системи, то їхня стійкість до ЕМ-завад визначається такими факторами: рівень завадового сигналу (джерело), співвідношення «сигнал/завада», спектральне перекриття, затримка системи, механізми модуляції, а також наявність заходів протидії (екранування, фільтрація, алгоритми опору). Наприклад, у роботі з залізничними системами було встановлено, що при співвідношенні потужності завад до корисного сигналу (JSR — Jammer-to-Signal Ratio) лише на рівні -6 дБ починаються серйозні порушення, а при -2 дБ або 1 дБ – зв’язок може бути повністю втрачено. [6]

Радіозавади (або електромагнітні завади — EMI) можуть суттєво погіршувати або й повністю блокувати роботу радіоприймальних та радіопередавальних пристроїв. Нижче наведено основні механізми такого впливу:

Підвищення рівня шуму / зменшення співвідношення сигнал/шум - коли зовнішні завадні сигнали чи хвилі потрапляють у ланцюг приймача, вони підвищують фон шуму. Внаслідок чого слабкий корисний сигнал може стати непридатним для демодуляції або бути «загубленим». Наприклад: у радіоприймачі, якщо рівень завади росте до рівня корисного сигналу, пристрій стає нездатним виділити потрібну інформацію.

Перевантаження (блокування) приймача / зниження чутливості - Сильний радіосигнал у тій самій або сусідній частотній смузі може “заблокувати” або “заглушити” приймач, підвищуючи мінімально дієвий рівень прийому (MDS — Minimum Detectable Signal). Це явище іноді називають «desensitization» (зниження чутливості приймача). Наприклад: приймач, розрахований на взаємодію із слабкими сигналами, розташований поряд із потужним передавачем — може перестати сприймати слабкі сигнали взагалі.

Інтермодуляція і спрощення спектру через нелінійності приймача чи антени - нелінійні елементи в приймачі чи в антенной системі можуть змішувати завадні сигнали з корисними, генерувати гармоніки або побічні продукти змішування, які потрапляють у смугу прийому. Наприклад: два завадних сигнали на різних частотах можуть створити продукт суміш-різниця частот, який лежатиме в смузі корисного сигналу і спричинятиме помилки. [7]

Мультипроміжне (multipath) та фазові збурення - При багатошляховому поширенні сигналу (відбитки, віддзеркалення, рефракція) корисний сигнал може надходити в приймач із декількох шляхів із різною затримкою та фазою, що призводить до інтерференції, «затухання» або викривлень. Це не завжди саме «завада» в класичному розумінні, але ефект дуже схожий: приймач «бачить» неправильний сигнал або слабший, ніж мав би.

Втрати даних, помилки демодуляції, зниження якості зв’язку - через

завади можуть зростати помилки в пакеті, знижуватися швидкість, відбуватися втрати зв’язку, зниження точності навігаційних/телеметричних систем. Наприклад: цифровий радіоканал може працювати на межі, і заява «cliff effect» означає, що невелике збільшення завади призводить до різкого падіння якості прийому

Таким чином, електромагнітні завади є одним із головних факторів, що впливають на стабільність роботи радіоелектронних систем. Для забезпечення їх стійкості слід застосовувати комплексні технічні рішення: екранізацію компонентів, використання фільтрів на вході й виході сигналів, частотне рознесення каналів, адаптивні методи модуляції та алгоритми виправлення помилок, здатні компенсувати вплив зовнішніх перешкод.

РОЗДІЛ 2

ПРОБЛЕМАТИКА ВПЛИВУ ЕМ ПЕРЕШКОД НА КАНАЛИ ЗВ'ЯЗКУ БПЛА

2.1 Загальний опис ЕМ перешкод

Теоретичний принцип електромагнітних (ЕМ) перешкод полягає у порушенні процесу передачі даних між передавачем і приймачем. На практиці ж основний вплив спрямований безпосередньо на приймальний пристрій, оскільки саме на цьому етапі сигнал має найменшу потужність і є найбільш вразливим до зовнішніх впливів.

Існує кілька підходів до реалізації впливу на обмін даними між двома бездротово з'єднаними вузлами. Ці методи відрізняються за типом випромінювання, способом модуляції та спектральним охопленням, проте всі вони мають спільну мету — знизити якість прийому або повністю зірвати передавання інформації.

Першим типом дій є пасивне спостереження, коли зловмисник лише приймає сигнал і намагається отримати інформацію про передані дані, не втручаючись у сам процес передачі.

Другий варіант — активне випромінювання енергії, метою якого є створення електромагнітних перешкод, що знижують якість або повністю блокують передавання даних між передавачем і приймачем.

Третій рівень загрози пов'язаний із втручанням у цілісність і конфіденційність даних, коли атака відбувається на більш високому рівні комунікаційного протоколу. Такі дії можуть включати зміну або підміну інформації в каналі зв'язку.

Завади можуть мати як мирне, так і військове призначення. У цивільному секторі вони проявляються у вигляді глушіння радіостанцій, супутникових каналів, мобільного зв'язку чи мережі Інтернет. У військовій сфері завади використовуються для пригнічення роботи радарів, систем управління БПЛА або

ліній зв’язку противника. Радіочастотне глушіння належить до навмисних завад і полягає у створенні штучних сигналів, які перекривають робочу частоту системи зв’язку, зменшуючи співвідношення сигнал/шум і унеможливлюючи нормальну передачу даних. Такі завади цілеспрямовано зривають обмін інформацією між передавачем і приймачем, особливо в бездротових мережах. Подібна технологія часто використовується як інструмент контролю інформації — наприклад, у державах із жорсткою цензурою, де глушіння застосовується для блокування іноземного мовлення або обмеження доступу населення до незалежних джерел інформації. Необхідно розрізняти навмисні завади від ненавмисних, що виникають через технічні несправності або неправильну роботу обладнання. Ненавмисні завади можуть з’являтися, коли оператор випадково використовує зайняту частоту або коли електронний пристрій генерує сторонні випромінювання, наприклад телевізійна станція, сигнал якої потрапляє в аварійний діапазон авіаційного зв’язку. Головна відмінність полягає в тому, що ненавмисні завади є побічним ефектом роботи техніки, тоді як радіочастотне глушіння — це навмисно створений шум, метою якого є позбавлення приймача можливості приймати та обробляти корисний сигнал.

Радіочастотне глушіння — це процес, під час якого приймальний пристрій перевантажується потужним сигналом завад, створеним спеціальним джерелом випромінювання. У цьому випадку сама завада виступає передавачем, який генерує сигнали у робочій частотній смузі, щоб ускладнити або зробити неможливою обробку корисного сигналу. Такий вид впливу має часову природу — він не завжди повністю зупиняє обмін даними, але здатний суттєво сповільнити передачу інформації. Це особливо критично у випадках, коли для прийняття рішень потрібні актуальні та своєчасні дані, наприклад, у тактичних або бойових операціях. Суть глушіння полягає у порушенні роботи каналу зв’язку певного об’єкта чи супутника з метою унеможливлення прийому або декодування сигналу на приймачі. Теоретичні основи цього методу з’явилися одночасно з розвитком радіозв’язку, а практичне застосування почалося у військових умовах — для запобігання перехопленню або зриву передач

противником. Мета використання глушіння полягає у тому, щоб позбавити супротивника можливості безперешкодно користуватися своїми засобами зв’язку. Радіочастотні глушники активно застосовувались біля кордонів і на стратегічних ділянках. У період Другої світової війни нацистська Німеччина використовувала глушіння для блокування трансляцій союзних радіостанцій до окупованої Європи. Згодом цей метод набув подальшого розвитку під час Холодної війни, конфлікту у В’єтнамі та арабо-ізраїльських воєн, ставши одним із ключових інструментів радіоелектронної боротьби. У сфері безпеки бездротових мереж глушіння розглядається як процес штучного порушення стабільної передачі або прийому сигналу через навмисне зменшення співвідношення сигнал/шум (SNR) на приймальному боці. Це досягається передаванням заважаючих радіохвиль, які перекривають або маскують корисний сигнал, що призводить до зниження якості зв’язку або повного його зриву. Показник співвідношення сигнал/шум (SNR або S/N) характеризує різницю між рівнем корисного сигналу та рівнем фонових електромагнітних завад. Коли SNR падає нижче критичного порогу, приймач втрачає можливість коректно декодувати інформацію, навіть якщо передавання технічно триває.

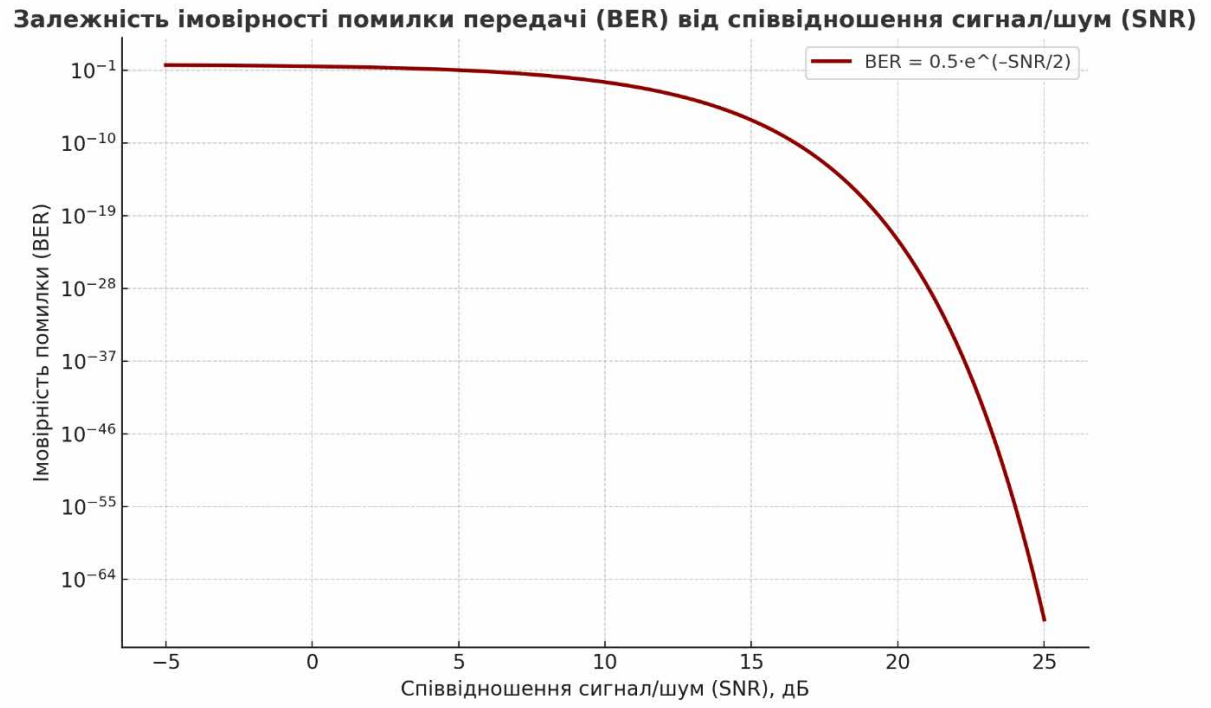

Рис 2.1 - Залежність співвідношення сигнал/шум (SNR) від рівня потужності електромагнітної завади.

На рисунку видно, що зі зменшенням співвідношення сигнал/шум (SNR) імовірність помилки передачі даних (BER) різко зростає. Це свідчить про зниження завадостійкості каналу зв'язку. При досягненні критичного рівня шуму система зв'язку БПЛА втрачає здатність до коректної передачі команд і телеметрії.

Для розуміння природи навмисного глушіння необхідно враховувати різновиди завад, які можуть впливати на бездротову інфраструктуру. Сучасна класифікація виділяє такі типи:

- проактивні завади — працюють постійно, незалежно від активності цілі;
- реактивні завади — активуються лише при виявленні сигналу або передачі даних;
- функціонально-специфічні — спрямовані на певний тип сигналу чи протоколу;
- смарт-гібридні — комбінують кілька підходів і адаптуються до

характеристик мережі.

Навмисні завади, на відміну від випадкових електромагнітних шумів, мають цільову спрямованість — вони перевантажують передавач або блокують його активність, утримуючи канал зв’язку постійно зайнятим. Коли система виявляє активний об’єкт або пошкоджений пакет даних, вона автоматично зупиняє передавання, що призводить до деградації каналу.

Ефективність глушіння залежить від потужності випромінювання завади, її розташування відносно цільового вузла, а також від топології мережі. За характером дії завада може бути примітивним постійним джерелом безперервного шуму або інтелектуальним адаптивним пристроєм, здатним аналізувати спектр і підлаштовуватися під зміну параметрів сигналу.

Таким чином, глушіння є однією з найнебезпечніших форм впливу на бездротові системи, оскільки воно не лише порушує роботу каналу зв’язку, а й може використовуватись як елемент електронної війни або засіб кібератаки на мережеву інфраструктуру. [8]

2.2 Типи перешкод

У сучасних бездротових комунікаційних системах, зокрема в каналах управління та передачі даних безпілотних літальних апаратів (БПЛА), ключову роль відіграє стійкість до різних типів перешкод. Цей аспект набув особливої актуальності в умовах сучасної війни, де Україна широко використовує FPV-дрони (First Person View) як високоточний елемент тактичних дій. Такі дрони, оснащені системами передачі відео в реальному часі, є надзвичайно ефективними у веденні розвідки та ураженні цілей, проте їхня робота повністю залежить від стабільності каналів зв’язку та відеосигналу. Будь-які радіочастотні або електромагнітні завади можуть призвести до втрати керування, зниження точності наведення або навіть повного виходу апарата з ладу.

Перешкоди є одним із головних чинників, що обмежують пропускну

здатність, дальність дії та надійність систем зв’язку. Вони можуть мати природне або штучне походження, бути навмисними (створеними засобами радіоелектронної боротьби) чи випадковими. Їхній вплив проявляється у зменшенні співвідношення сигнал/шум (SNR), спотворенні або зсуві частоти сигналу, втраті синхронізації між передавачем і приймачем. Класифікація перешкод здійснюється за кількома критеріями — за розташуванням джерела, типом сигналу, фізичною природою або способом впливу на систему. Відповідно, виділяють внутрішньоканальні, суміжноканальні, міжканальні, міжсимвольні, електромагнітні, акустичні, оптичні та інші типи завад. Кожен із них чинить власний вплив на роботу каналу зв’язку, знижуючи якість прийому або порушуючи передавання даних. Завади виступають головним обмежувальним чинником у розвитку бездротових технологій, оскільки саме вони визначають реальні межі пропускної здатності та стабільності каналу. Для FPV-дронів це означає, що навіть короткочасний вплив потужних електромагнітних сигналів може повністю вивести систему управління з ладу або унеможливити виконання завдання.

Отже, аналіз типів перешкод і механізмів їхньої дії є критично важливим для розуміння стійкості БПЛА до електромагнітного впливу. Усвідомлення різновидів завад дозволяє визначити потенційні вразливості системи зв’язку FPV-дронів та розробити ефективні методи протидії — фільтрацію, частотне рознесення, адаптивну модуляцію, екранування та впровадження резервних каналів управління. [9]

Знизу представлена класифікація завад за розташуванням джерела, типом сигналу та системою передачі.

За розташуванням джерела перешкод відносно корисного сигналу:

Внутрішньоканальна перешкода (ВКП). Виникає, коли дві або більше бездротові системи одночасно передають дані в межах однієї частоти. Це поширене явище у стільникових мережах, де частоти повторно використовуються в різних зонах покриття. Для мінімізації ВКП необхідно дотримуватись просторового рознесення комірок із однаковими частотами та

забезпечувати мінімально можливу потужність передавання, достатню для стабільного зв’язку.

Суміжноканальна перешкода (СКП). Виникає через вплив сигналів, що працюють у сусідніх частотних діапазонах, на корисний канал. Причиною можуть бути недосконалі фільтри приймача, які пропускають небажані частоти, або ефект «ближній-далекий», коли потужні сигнали від близьких передавачів заглушують слабші. Зменшення СКП досягається за рахунок оптимального частотного планування та якісної фільтрації.

За типом сигналу, що створює перешкоду:

Електромагнітна перешкода (ЕМП). Виникає, коли електромагнітне випромінювання однієї системи впливає на сигнал іншої, що працює в тій самій або суміжній частотній області. ЕМП може порушувати роботу як одночастотних, так і різночастотних систем зв’язку.

Акустична (звукова) перешкода. Формується внаслідок накладання звукових хвиль, які можуть взаємно посилюватися або знищувати одна одну залежно від їхньої фази.

Світлова перешкода. Виникає при взаємодії світлових потоків різних або однакових довжин хвиль. Оптичні сигнали здатні створювати перешкоди також для систем, що використовують інші типи середовищ передавання — наприклад, у змішаних оптико-радіочастотних системах.

За типом системи передавання:

Міжканальна перешкода (МКП) у системах OFDM. Виникає, коли піднесучі OFDM-сигнали втрачають ортогональність. Це може бути спричинено затримками поширення сигналу, які перевищують тривалість циклічного префікса (CP), або зміщенням частоти в приймачі. Втрата ортогональності призводить до взаємного перекриття спектрів піднесучих і зниження якості передачі.

Міжсимвольна перешкода (MCI) у системах OFDM. Виникає, коли тривалість затримки сигналу в каналі перевищує межі циклічного префікса, унаслідок чого один символ частково накладається на наступний. Це спричиняє

спотворення часової структури сигналу та збільшення кількості помилок декодування.

У результаті цього сигнал окремого символу OFDM розтягується в часі, що призводить до його накладання на наступний символ. Такий ефект називається міжсимвольною інтерференцією (MCI). [10]

У таблиці 2.1 наведено перелік потенційних видів перешкод, що можуть виникати під час функціонування каналів зв’язку безпілотних літальних апаратів.

Таблиця 2.1

Перелік потенційних видів перешкод

Тип перешкоди	Опис та характерні ознаки	Наслідки
Електромагнітні впливи	Формуються під дією електромагнітних полів від різноманітних джерел (радіопередавачів, промислових установок, електромереж тощо).	Погіршення прийому сигналу, поява шумів, втрата частини пакетів даних, зниження швидкості передачі.
Інтерференція з іншими БПЛА або пристроями	Виникає через накладання сигналів від систем, що працюють на тій самій або близькій частоті, випадково чи навмисно.	Перебої у керуванні, нестабільність зв’язку, можливі втрати телеметрії.
Спрямоване радіоелектронне втручання (підслуховування)	Передбачає спробу перехопити передавання БПЛА та відстежити його за допомогою спеціалізованої антени.	Ризик отримання конфіденційної інформації сторонніми особами, можливе втручання в процес керування.
Підміна або модифікація сигналу (спуфінг)	Намагання навмисно змінити або імітувати сигнал, який повинен отримувати БПЛА.	Хибні навігаційні дані, неправильне керування, зміна маршруту, зниження точності навігації.

2.3 Характеристика ЕМ завад

Вплив радіозавад може викликати широкий спектр негативних ефектів — від перевантаження приймального тракту до глибокого спотворення, маскування або навіть повної імітації корисного сигналу. У таких умовах радіосистема працює в режимі зниженої достовірності прийому, що проявляється у збільшенні

кількості помилок, втраті синхронізації, появі затримок та, у критичних випадках, повному руйнуванні каналу зв’язку. У складних умовах електромагнітного впливу може спостерігатися нерівномірне погіршення якості зв’язку: короткочасні провали, періодичні збої або стійка деградація параметрів прийому.

Ефективність дії навмисних радіозавад визначається низкою параметрів, серед яких ключову роль відіграють:

- співвідношення сигнал/шум (SNR) на вході приймача, що безпосередньо визначає здатність системи коректно декодувати інформацію. При досягненні критичного порогу SNR навіть незначне збільшення потужності завади призводить до різкого зростання імовірності помилок у каналі;

- взаємне співвідношення смуги частот корисного сигналу і спектральних характеристик завадного випромінювання. Якщо спектр завади повністю або частково перекриває робочу смугу сигналу, ймовірність порушення прийому суттєво зростає, особливо у випадках використання вузькосмугових радіоканалів;

- конструктивні та функціональні особливості радіосистеми: застосований тип модуляції, робочий діапазон частот, рівень передаваної потужності, чутливість приймального тракту, спосіб формування пакета даних, наявність корекційних кодів, методів розширення спектра та алгоритмів компенсації завад. Радіосистеми з адаптивними механізмами зміни частоти, швидкості передачі або схеми модуляції демонструють вищу стійкість до завад;

- параметри самих радіозавад: рівень їх потужності, характер спектральної щільності, ширина смуги випромінювання, тип впливу (імпульсний, квазіперіодичний, широкосмуговий шумовий, періодичний маскувальний тощо), а також просторове положення джерела завади щодо приймача. Чим ближче завада розташована до антени приймача, тим сильнішим буде її вплив через менші втрати на поширення.

Класифікація навмисних завад доволі широка, може ділитись по багатьом параметрам. (Рис. 2.2) [11]

Рис 2.2 – Класифікація завад

За своїми параметрами радіоперешкоди можуть класифікуватися за кількома ознаками:

- джерелом походження. Виділяють перешкоди природного походження, пов’язані з природними фізичними процесами, та штучні перешкоди, що виникають унаслідок роботи технічних засобів, які випромінюють електромагнітну енергію;

- типом випромінюваної енергії. До перешкод належать електромагнітні, оптичні та акустичні різновиди залежно від діапазону та фізичної природи випромінювання;

- співвідношенням спектрів. Якщо спектр перешкоди значно ширший за спектр корисного сигналу, така перешкода вважається загороджувальною. Якщо ж спектр перешкоди співмірний зі спектром корисного сигналу, а її частота може змінюватися в межах робочого діапазону засобів радіозв’язку, то така перешкода називається прицільною;

- структурою випромінювання. Розрізняють імпульсні перешкоди — послідовності радіоімпульсів, які можуть бути модульованими або немодульованими, — та безперервні перешкоди, що здатні мати частотну, фазову або амплітудну модуляцію;

- характером впливу на засіб радіозв'язку (ЗРЗ). Маскуючі перешкоди ускладнюють виявлення та визначення параметрів корисного сигналу. Імітуючі перешкоди створюють на вході приймача помилкові сигнали, які можуть сприйматися як справжні;

- потужністю. Слабкі перешкоди мають рівень, що не перевищує рівня корисного сигналу, та спричиняють втрату не більше 25 % інформації. Середні перешкоди мають рівень, близький до рівня корисного сигналу, і здатні викликати втрату щонайменше 50 % інформації. Сильні перешкоди суттєво перевищують рівень корисного сигналу і можуть спричинити його повну втрату; у деяких випадках вони здатні виходити за межі динамічного діапазону приймача.

У радіолокаційних системах перешкоди поділяються на активні та пасивні, що застосовуються з метою створення маскування або дезінформації. Активні перешкоди формуються за допомогою спеціальних радіотехнічних засобів — станцій чи передавачів перешкод, що генерують сигнал із певними заданими характеристиками. Пасивні перешкоди утворюються шляхом розсіювання або відбиття електромагнітного випромінювання штучними об'єктами, такими як дипольні або кутові відбивачі, лінзи Люнеберга, аерозольні утворення тощо. Результуючий сигнал при цьому є сумою багатьох відбитих компонентів із випадковими параметрами амплітуди, частоти та фази.

Маскувальні перешкоди створюються хаотичними шумовими сигналами, які ускладнюють виявлення цільового випромінювання. Дезінформаційні перешкоди застосовують сигнали, що подібні до реальних, але містять неправдиві дані. Активні маскувальні перешкоди найчастіше являють собою радіочастотні коливання, модульовані шумами, або шумові сигнали, які за своїми властивостями нагадують внутрішні шуми радіолокаційного приймача.

За шириною спектра перешкоди поділяються на прицільні та загороджувальні. Спектр прицільних перешкод близький до смуги пропускання приймача і дозволяє впливати на окремі радіолокаційні засоби, налаштовані на конкретні частоти. Для їх ефективного застосування потрібно знати точні параметри радіолокатора, який планується подавити. Загороджувальні перешкоди мають ширшу смугу та охоплюють увесь діапазон роботи засобу радіозв'язку.

Серед різновидів активних перешкод найбільш поширеною є загороджувальна шумова перешкода, яка являє собою білий гаусівський шум із певною спектральною щільністю потужності в обмеженій смузі частот. Смуга такої перешкоди перекриває робочу смугу засобу радіозв'язку, що призводить до суттєвого погіршення прийому. Найбільш ефективно ці перешкоди діють тоді, коли рівень сигналу радіозасобу, який подавляється, є нижчим або порівнянним із рівнем перешкоди.

На рисунку 2.3 [11] наведено випадок, коли спектр корисного сигналу перекритий перешкодою, однак рівень потужності самого сигналу значно перевищує рівень створюваної перешкоди.

Рис 2.3 - Ефективний вплив загороджувальної ЕМ перешкоди

Загороджувальні ЕМ перешкоди перекривають визначені ділянки радіочастотного діапазону, створюючи умови, за яких корисний сигнал істотно послаблюється або повністю втрачається в спектрі завадового випромінювання. Активні ЕМ перешкоди можуть мати вигляд зондуючих РЛ сигналів, модульованих за амплітудою, частотою, фазою, часом запізнення або поляризацією. Такі перешкоди здатні одночасно виконувати функції маскування та дезінформації, що значно ускладнює роботу засобів радіоелектронного спостереження та зв'язку. Вибір інформаційних критеріїв для оцінювання впливу ЕМ перешкод залежить від типу завадового сигналу (ЗС) і класу радіоелектронного засобу, на який спрямовано вплив. Для маскуючих ЕМ перешкод найдоцільніше використовувати показник ентропії ЗС, оскільки він відображає рівень невизначеності, що вноситься у процес прийому корисного сигналу.

Маскуючі ЗС повинні забезпечувати умови, за яких ймовірність виявлення корисного сигналу стає нижчою за наперед задану межу. Для цього необхідно мати хоча б мінімальні апріорні відомості про структуру та параметри корисного сигналу. Маскуючі ЗС мають створювати таку конфігурацію перешкод, при якій навіть після обробки сигналу на приймальній стороні зберігається значна апріорна невизначеність. Інакше кажучи, маскуючі ЕМ перешкоди повинні містити елемент випадковості та непередбачуваності, що мінімізує можливість їх ефективного пригнічення або компенсації. Із зростанням ентропії завадового сигналу рівень потенційної завадостійкості системи зменшується, а технічні методи фільтрації стають менш результативними. Вони спрямовані на збільшення ймовірності помилкової тривоги, тобто ускладнення надійного виявлення корисного сигналу шляхом формування додаткового завадового фону у приймальній частині радіосистеми. Інтенсивність такого ускладнення визначається співвідношенням частотних, часових та структурних параметрів завадового та корисного сигналів. Найчастіше як активні маскуючі перешкоди застосовуються безперервні шумові сигнали.

Прицільні радіоперешкоди характеризуються відповідністю їх спектра

спектру корисного сигналу засобу радіозв’язку або радіолокаційного засобу (ЗРЗ), що піддається впливу. Імітуючі ЕМ перешкоди створюють на приймальній стороні хибну інформацію: параметри таких ЗС формуються таким чином, щоб бути максимально наближеними до характеристик реального корисного сигналу. У деяких випадках частина корисного сигналу може використовуватися як основа для генерації імітаційного ЗС, що ретранслюється засобом постановки перешкод. За відсутності перешкод обробка сигналів дозволяє повністю усунути апріорну невизначеність, тобто забезпечити нульовий рівень апостеріорної ентропії. Проте у присутності ЕМ перешкод частина невизначеності залишається, що визначається рівнем ентропії шумового ЗС. Таким чином, обсяг інформації, яку система може отримати, зменшується пропорційно збільшенню ентропії завадового сигналу. Величина ентропії дає можливість оцінювати ефективність ЕМ перешкод без залежності від конкретних методів цифрової обробки, реалізованих у ЗРЗ. Однією з ключових енергетичних характеристик ЗС є коефіцієнт придушення, який визначається як мінімальне значення відношення енергії ЗС до енергії корисного сигналу на вході приймача, за якого досягається встановлений інформаційний збиток. Інформаційний збиток може проявлятися у вигляді маскування, імітації, затримки в передачі інформації та інших видів погіршення роботи. Характер інформаційної шкоди визначається видом ЗС та можливостями подавляючого засобу. За шириною частотного спектра ЕМ перешкоди поділяються на прицільні та загороджувальні. Прицільні перешкоди мають спектр, співмірний із шириною смуги пропускання приймача, налаштовуються на певну робочу частоту і застосовуються для вибіркового впливу на конкретні радіолокатори. Їхня ефективність можлива лише за умови знання точних параметрів ЗРЗ. Загороджувальні ЕМ перешкоди охоплюють значно ширшу частину діапазону та використовуються для ураження або приглушення великої кількості засобів одночасно.

Серед різновидів активних перешкод найбільш універсальною є загороджувальна шумова перешкода, яка являє собою білий гаусівський шум із певною спектральною щільністю потужності в заданій смузі частот. Спектр

такого ЗС повністю перекриває робочу смугу радіозасобу, що піддається впливу, створюючи стійкі умови деградації прийому. Найефективніше ці перешкоди діють тоді, коли рівень потужності корисного сигналу є нижчим або порівняним із рівнем перешкоди. У випадках, коли корисний сигнал має більший рівень потужності, ступінь подавлення зменшується.

2.4 “Jamming”, “Spoofing” як основні типи перешкод для навігації БПЛА

Jamming - це навмисне блокування або створення перешкод у роботі бездротових систем зв’язку. У певних випадках воно реалізується шляхом випромінювання радіосигналів, які знижують співвідношення сигнал/шум у приймальній частині системи, що призводить до порушення телекомунікаційного процесу.

Такий підхід може застосовуватися і в бездротових мережах передавання даних з метою порушення або зупинення обміну інформацією. У ряді держав із авторитарними режимами радіопридушення використовується як інструмент цензури, спрямований на блокування трансляцій закордонних радіостанцій, особливо в прикордонних регіонах.

Варто розрізняти навмисний jamming та звичайні радіоперешкоди, що виникають унаслідок несправностей обладнання або випадкових факторів. Пристрої, які створюють ненавмисні перешкоди, регулюються за іншими нормами. Ненавмисне радіопридушення може виникати, коли оператор передає на частоті, яка вже зайнята іншими користувачами, не перевіривши її наявність у спектрі, або ж не маючи можливості почути активну станцію. Інший приклад ненавмисного придушення — коли технічне обладнання випадково випромінює сигнал, скажімо, кабельна телевізійна мережа генерує випромінювання в діапазоні аварійної авіаційної частоти. [12]

У воєнних та надзвичайних умовах засоби радіопридушення часто застосовуються для локального прикриття операцій або захисту важливих об’єктів. Однак практика показує, що такі системи можуть створювати значні

проблеми насамперед власним підрозділам. Під час війни в Україні неодноразово фіксувалися ситуації, коли засоби РЕБ українських військ завдавали більше шкоди, ніж дії противника: робота джамерів створювала широкий «купол» перешкод, через що застосування БПЛА навіть на значній відстані від лінії зіткнення сприймалося як вплив російського РЕБ, хоча фактично це був сигнал наших же станцій, про які підрозділи на місці не були поінформовані. Єдиним дієвим способом уникнення таких інцидентів є чітка координація груп, що працюють в межах однієї операційної зони.

Джамери активно використовуються й у цивільному секторі, головним чином для захисту критичної інфраструктури — в районах аеропортів, атомних електростанцій, урядових кварталів і дипломатичних установ. Окрему категорію становлять комерційні пристрої постановки перешкод, відомі як Privacy Protection Devices (PPD). За останні роки вони набули широкої популярності, але водночас стали предметом занепокоєння через низку випадків зловживання. Такі пристрої продаються у відкритому доступі, включно з онлайн-майданчиками, за ціною від 30 євро за найпростішу автомобільну модель (живлення від прикурювача) до складних багатодіапазонних систем, здатних подавляти GPS, GSM, Wi-Fi та інші сигнали й оснащених зовнішніми антенами та налаштовуваними режимами роботи. Причини використання PPD часто перебувають на межі правового поля. Серед поширених мотивів — блокування автомобільних протиугінних систем, що передають координати транспортного засобу; уникнення фіксації поїздок страховими або дорожніми службами; відключення засобів контролю у системах управління автопарком; приглушення сигналів автоматичної ідентифікації суден; або приховування реального місцезнаходження кур’єрів від роботодавців. Попри те, що окремі мотиви можуть здаватися користувачам обґрунтованими, вони зазвичай не усвідомлюють масштаб впливу таких пристроїв. Навіть малопотужний PPD здатен порушити або суттєво спотворити роботу GNSS на відстані у кілька кілометрів, створюючи небезпечні умови для навігації та функціонування навколишніх систем.

GNSS Barrage Jamming - такий тип завад передбачає передавання потужного широкосмугового шумового сигналу в усьому робочому діапазоні GNSS. У результаті слабкі супутникові сигнали, зокрема GPS, перекриваються підвищеним рівнем шуму. Це призводить до зростання шумової підлоги, через що корисні навігаційні сигнали стають нерозпізнаваними, а приймачі БПЛА можуть втрачати точність визначення координат або повністю виходити з ладу. На рисунку 2.4 [13] показана блок-схема модуля GNU Radio, використаного для моделювання широкосмугового GNSS-глушіння. Схема включає генератор шуму, LPF-фільтр зі смугою 3.333 МГц, а також передавальний та приймальний модулі PlutoSDR, що забезпечують формування та контроль завадового сигналу в діапазоні GPS L1.

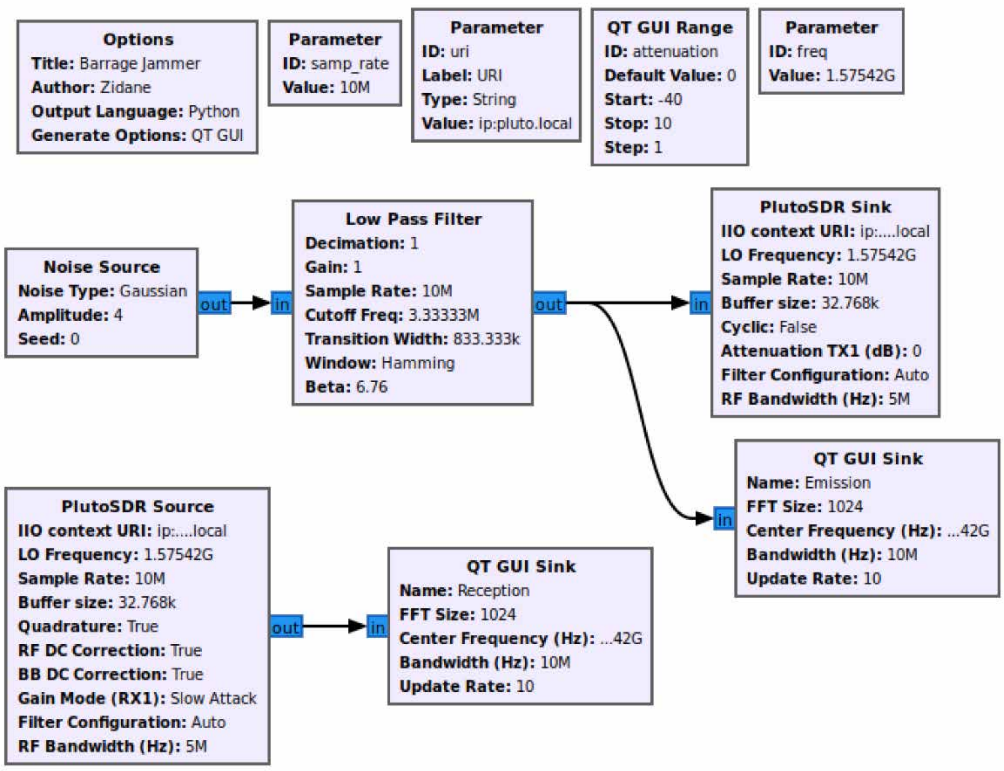

Рис 2.4 - Архітектура скрипту barrage jamming у GNU Radio

Spoofing - це навмисне формування та передавання фальсифікованих сигналів GNSS з метою примусити приймач сформувати неправдиві дані щодо координат, швидкості чи часу. Завдання спуфера полягає в тому, щоб непомітно змусити приймач прийняти підроблений сигнал (або кілька синтезованих сигналів) як справжній та розпочати обчислення хибного місцеположення. Для захищених криптографічних сигналів, таких як GPS P(Y) чи Galileo PRS, пряма підробка майже нереальна, однак навіть такі сигнали уразливі до прийомів типу meaconing. Meaconing передбачає перехоплення справжнього GNSS-сигналу, його запис і подальшу ретрансляцію. Якщо приймач відстежує лише апаратно сформований сигнал, не аналізуючи його структуру, він може визначити координати не власного положення, а координати точки, де розташований ретранслятор, або дещо зміщену їх версію.

Атаки на основі спуфінгу умовно поділяють на такі категорії:

– без перекриття;

– з перекриттям;

– за відносною потужністю сигналу.

Спуфінг без перекриття:

У цьому випадку кодова послідовність і фаза підробленого сигналу не синхронізуються зі справжнім. Піки кореляції автентичного та фальшивого сигналів не накладаються один на одного. Під час холодного старту приймача потужніший спуфінговий сигнал може змусити модуль пошуку й захоплення визначити його як основний. Якщо ж приймач уже відстежує супутники (тобто ініціалізація виконана), то всі несинхронні сигнали зазвичай ігноруються. Тому навіть за суттєвої переваги потужності фальсифікований сигнал не буде прийнятий, якщо затримки та частотні параметри не узгоджені з параметрами реального сигналу.

Спуфінг із перекриттям:

Цей тип атаки є значно складнішим. Джерело підробленого сигналу синхронізує фазу, код та доплерівську складову зі справжнім супутниковим

сигналом. Унаслідок цього піки кореляції починають накладатися та можуть змінювати форму кореляційного максимуму як у бік посилення, так і в бік приглушення. Такий спуфінг можливий у разі використання приймача-генератора, який знає поточний час, положення атакованого приймача, параметри супутників і траєкторію їх руху. Виявити перекривний спуфінг складно, адже спотворення сигналів нагадує типові ефекти багатопроменевого поширення, що ускладнює однозначне визначення факту атаки.

Класифікація за відносною потужністю:

Потужність фальсифікованого сигналу є ключовим фактором, що визначає успішність обману GNSS-приймача. Співвідношення між рівнем спуфінгового сигналу та рівнем автентичних сигналів може значно впливати на здатність приймача розпізнати втручання. Виявлення таких атак потребує знань про характеристики каналу поширення, діаграму спрямованості антени й орієнтацію приймального обладнання. Без цих даних оцінка відносної потужності є нетривіальним завданням.

Таким чином, спуфінгові атаки можуть істотно впливати на коректність визначення навігаційних параметрів і становлять серйозну загрозу для будь-яких систем, які покладаються на GNSS сигнали. Знизу на рисунку 2.5 наведені ці форми впливу для кращого розуміння

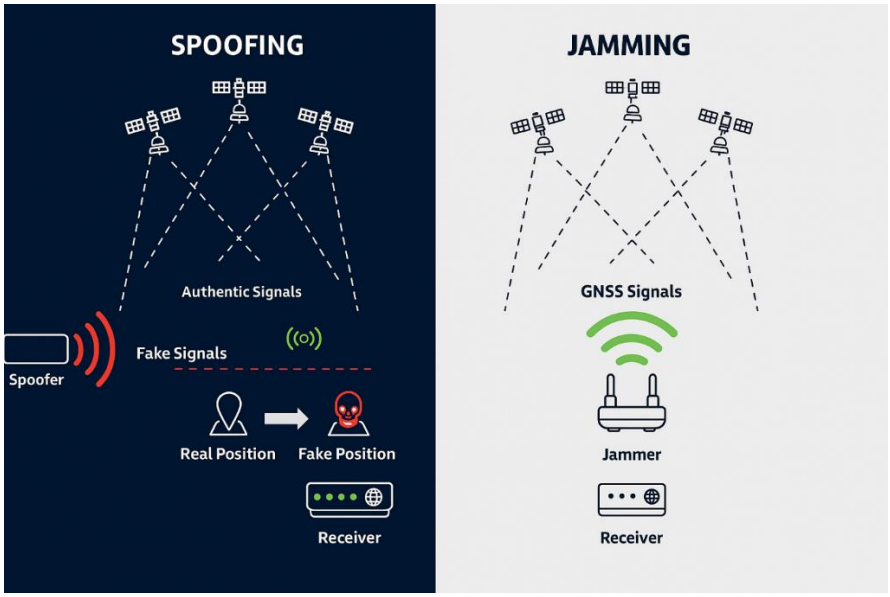

Рис. 2.5 - Порівняння механізмів spoofing та jamming сигналів GNSS

2.5 Перешкоди каналам зв'язку БПЛА в контексті радіоелектронної боротьби

Радіоелектронна боротьба охоплює застосування засобів і методів усіх її ключових компонентів. Для формування ефективного радіоелектронного захисту необхідно враховувати різновиди навмисних перешкод, їхні властивості та параметри, що можуть впливати на канали зв'язку БПЛА. Пасивні заходи радіоелектронного забезпечення передбачають радіорозвідку, яка включає перехоплення сигналів, визначення напрямку їхнього надходження та подальший аналіз. Активне радіоелектронне подавлення і заходи радіоелектронного захисту потребують постійного удосконалення технічних засобів для запобігання порушенню або блокуванню передачі сигналів.

Станції радіоелектронної боротьби, що інтегрують у собі можливості радіорозвідки й радіоподавлення, застосовуються як комплексний інструмент протидії безпілотним літальним апаратам. Такі системи не просто фіксують наявність сигналів, а й аналізують їхню структуру, визначають місце розташування джерела та за необхідності формують спрямоване завадне випромінювання. З міркувань ефективності подібні станції розташовують у зоні

виконання завдань БПЛА або на мінімально можливій відстані від цієї зони, що дозволяє зменшити втрати сигналу та забезпечити більшу точність виявлення. [14]

Разом з тим просторово-енергетичні характеристики каналу зв’язку БПЛА і каналу радіоподавлення є різними за своїм призначенням і структурою. Канал зв’язку БПЛА формує відносно стабільний напрямок передачі: як правило, інформаційний потік надходить від повітряної платформи до наземної станції керування, а у відповідь передаються команди управління. У цьому випадку потужність сигналу оптимізується для забезпечення необхідної дальності та завадостійкості.

Канал радіоподавлення, навпаки, може мати іншу конфігурацію. Спрямоване випромінювання завад може подаватися як від наземної системи у напрямку БПЛА, так і від самого БПЛА — якщо він обладнаний засобами активного завадного впливу. Напрямок руху сигналу залежить від того, хто є ініціатором операції з порушення або блокування радіообміну. Крім того, характеристики сигналів у каналі подавлення значно відрізняються від звичайного каналу: вони зазвичай мають більшу ширину спектра, підвищену потужність і спеціальну структуру, спрямовану на дестабілізацію роботи приймача противника. Ці фактори зумовлюють відмінності в покритті, енергетичному балансі, ефективності та дальності дії між каналами зв’язку та каналами радіоподавлення.

Крім того, частотні смуги, у яких працюють ці канали, також можуть суттєво відрізнятися. Канали зв’язку БПЛА переважно використовують радіочастотний діапазон, який залишається вразливим до впливу сторонніх джерел, технічних пристроїв та електромагнітних перешкод природного чи техногенного походження. Натомість канали радіоподавлення можуть застосовувати інфрачервоний спектр або інші типи випромінювання, що менш схильні до впливу зовнішніх завад, що у свою чергу підвищує їхню ефективність.

Таким чином, частотні діапазони, у яких працюють канали зв’язку БПЛА та канали радіоподавлення, можуть істотно відрізнятися, що безпосередньо

впливає на їхню стійкість до зовнішніх факторів та на загальну ефективність функціонування. Канали зв’язку БПЛА зазвичай використовують стандартні радіочастоти, що належать до найбільш завантажених спектральних ділянок. У цих діапазонах одночасно працює велика кількість цивільних і військових систем, що створює підвищену ймовірність виникнення взаємних перешкод. Додатковими джерелами деградації сигналу можуть бути електромагнітні випромінювання промислового обладнання, природні радіошуми, атмосферні явища та відбиття хвиль від різних об’єктів, які призводять до мультипасового поширення. У сукупності ці чинники здатні погіршувати якість приймання, знижувати співвідношення сигнал/шум та обмежувати радіус стабільного зв’язку.

У протилежність цьому канали радіоподавлення можуть працювати не лише в традиційних радіочастотних діапазонах, а й використовувати інфрачервоний спектр або інші типи електромагнітного випромінювання, які менш схильні до дії сторонніх електромагнітних завад. Такий підхід дозволяє підвищити ефективність створюваних перешкод, оскільки випромінення в альтернативних спектральних областях має інші характеристики затухання, меншу засміченість та вищу спрямованість. Це забезпечує можливість формувати більш керовані та результативні канали впливу на системи зв’язку БПЛА.

З огляду на відмінності у використовуваних частотах, умовах поширення сигналів та чутливості до сторонніх впливів, канали зв’язку БПЛА та канали радіоподавлення мають різні вимоги до проєктування й експлуатації. Для першого типу каналів ключовими є завадостійкість, надійність приймання та оптимізація енергетичного балансу, тоді як для другого — максимальна ефективність створення перешкод і точність спрямування впливу. Це визначає необхідність застосування відмінних технічних рішень, методів налаштування та підходів до оцінювання ефективності роботи кожного з каналів.

На рисунку 2.6 представлено блок-схему засобів радіоелектронної протидії, спрямованої проти безпілотних літальних апаратів. Схема відображає

канал обміну даними між наземною станцією керування та БПЛА, канал створення перешкод, а також структуру сигналу, який надходить на вхід приймача разом із можливими спотвореннями та завадовими компонентами.

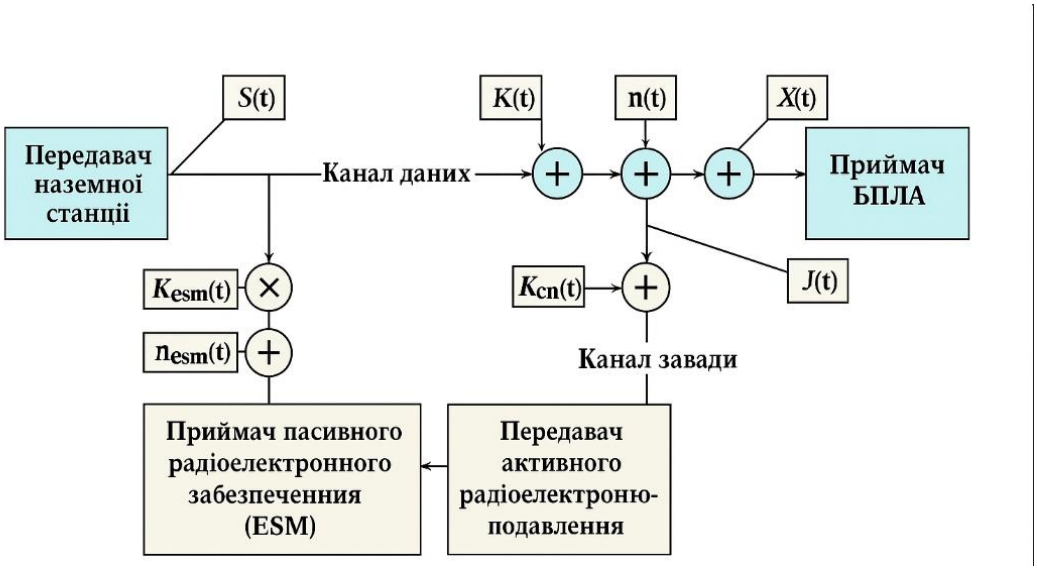

Рис 2.6 - Структурна схема каналів зв'язку та радіоелектронного впливу на БПЛА.

РОЗДІЛ 3

МЕТОДИ ВИРІШЕННЯ ВПЛИВУ ЕМ ПЕРЕШКОД НА КАНАЛИ ЗВ'ЯЗКУ БПЛА

3.1 Виявлення та протидія впливу ЕМ перешкод

Наявні дослідження у сфері кібербезпеки БПЛА переважно зосереджені на приглушенні сигналів супутникової навігації та спуфінгу, тоді як атаки на систему керування та канали обміну даними розглядаються недостатньо. Канал передачі даних, що забезпечує виконання місії та загальну працездатність апарата, є найбільш уразливим елементом. У разі кібервпливу порушення роботи каналу може залишатися непоміченим для оператора: він лише спостерігає відхилення траєкторії без явних ознак зовнішнього втручання.

Стабільність роботи БПЛА з точки зору керування безпосередньо визначається надійністю системи зв'язку. Її відмова призводить до втрати контролю над платформою і потенційної втрати самого апарата. Під життєздатністю каналу зв'язку розуміють здатність підтримувати необхідні параметри функціонування за наявності дестабілізуючих факторів, включно з ненавмисними та навмисними перешкодами. Методи протидії ненавмисним перешкодам є сформованими; серед них — адаптивні схеми модуляції й кодування. У таких випадках життєздатність каналу часто оцінюють через імовірність помилки бітів чи блоків.

Проте для навмисних перешкод такий підхід малоефективний, оскільки характеристика спеціально створених впливів відрізняється від випадкових завад. У цих умовах доцільніше визначати життєздатність каналу як ймовірність збереження працездатності системи керування за умови цілеспрямованого завадного впливу. [15]

Станції радіоелектронної боротьби, що поєднують можливості радіорозвідки та активного радіоподавлення і працюють у широкому частотному діапазоні, застосовуються як основні засоби протидії БПЛА. Поряд із ними

використовують портативні малопотужні антидронові пристрої («рушниці»), які мають обмежений функціонал і працюють у значно вужчих частотних межах.

Такі станції зазвичай розміщують у зоні виконання завдань БПЛА або на мінімальній відстані від неї, що зумовлює істотні відмінності між параметрами каналу зв'язку безпілотника та каналом радіоподавлення. Ці відмінності проявляються як у просторових характеристиках, так і в енергетичних умовах поширення сигналів.

Вплив навмисних перешкод на канал зв'язку БПЛА розглядається як складова радіоелектронної боротьби. У контексті функціонування каналів зв'язку безпілотних апаратів виділяють три основні елементи радіоелектронного впливу:

- пасивне радіоелектронне забезпечення (Electronic Support Measures, ESM);

- активне радіоелектронне подавлення (Electronic Countermeasures, ECM);

- протидія радіоподавленню, або радіоелектронний захист (Electronic Counter-Countermeasures, ECCM).

Пасивна складова для БПЛА переважно охоплює радіорозвідку, яка включає перехоплення сигналів, визначення напрямку їхнього надходження та подальший аналіз. Активні засоби радіоподавлення та системи радіоелектронного захисту перебувають у постійному технологічному розвитку, що створює динамічне протистояння між цими двома напрямами. Для радіоелектронної боротьби характерна одночасна взаємодія всіх трьох компонентів: засобів виявлення, засобів створення перешкод і механізмів захисту від них. Важливою вимогою до програмного забезпечення систем радіоелектронного захисту є його адаптивність та можливість модифікації, тобто відкрита архітектура. Ефективність захисних заходів визначається ступенем розуміння типів навмисних перешкод, їхніх властивостей та умов застосування, які можуть впливати на канал зв'язку БПЛА. Типовий сценарій радіоелектронного протистояння включає конкуренцію між засобами радіорозвідки, засобами подавлення та системами захисту.

Для протидії БПЛА застосовують станції радіоелектронної боротьби, що поєднують функції виявлення та створення радіоперешкод і працюють у широкому діапазоні частот. Додатково використовуються малогабаритні малопотужні антидронові пристрої з обмеженим набором функцій і вузьким частотним спектром. Такі станції, згідно з таблицею 3.1, зазвичай розміщують у безпосередній близькості до району виконання завдання БПЛА. Це зумовлює суттєві відмінності просторових і енергетичних характеристик між каналом зв'язку безпілотника та каналом радіоподавлення, включно з відмінністю у дальності дії та напрямках поширення випромінювання. [16]

Таблиця 3.1

Засоби радіорозвідки, радіостанції зв'язку та елементи радіопридушення

Типи приймачів радіомоніторингу	**Типи радіостанцій**	**Типи антен**	**Засоби радіоекранування**
Приймачі з можливістю сканування спектра	Передавачі створення радіоперешкод	Антени для визначення напрямку сигналу	Екранування на основі куткових відбивачів
Сканувальні приймачі	Передавачі завад із дистанційним доступом	Спрямовані антени для подавлення	Екранувальні конструкції з металізованої тканини
Дистанційні приймачі радіомоніторингу	Передавачі завад, призначені для подавлення БПЛА	Антени з керованою діаграмою спрямованості	Площинні екрани розміром $n \cdot \lambda max \times m \cdot \lambda max$

Проведений огляд відкритих джерел, що стосуються радіоліній керування іноземними БПЛА та їхніх каналів передавання даних, а також інформаційних матеріалів виробників бортового й наземного обладнання, дає підстави стверджувати, що на сьогодні найчастіше використовуються такі робочі діапазони частот (таблиця 3.2) [11]:

1700–1850 МГц (L-діапазон)

2200–2500 МГц (S-діапазон)

4400–4950 МГц (нижній C-діапазон)

5250–5850 МГц (верхній С-діапазон).

Таблиця 3.2

Діапазони та смуги частот БПЛА

Діапазон	**Смуга**	**Призначення**
WiFi 5.8 ГГц	5.7–5.9 ГГц	Передавання відео
WiFi 2.4 ГГц	2400–2480 МГц	Управління
GPS L1	1575.42 МГц	Навігація
GPS L2	1227.60 МГц	Навігація
433 МГц	—	Пульт управління
800/900 МГц, 850–965 МГц	—	Пульт управління

Використовувані канали зв’язку можуть застосовувати як аналогові схеми модуляції (GMSK, NTSC, PAL) у фіксованому частотному режимі або зі стрибкоподібною зміною частоти, так і цифрові методи, включно з OFDM, у яких передбачено компенсацію доплерівського зсуву. Аналогові методи модуляції сьогодні вважаються застарілими та не використовуються в сучасних БпАК.

Пропускна здатність каналу передачі даних з борту БпЛА зазвичай знаходиться в діапазоні 3,5–274 Мбіт/с із тенденцією до збільшення. Ширина смуги пропускання каналів зв’язку становить переважно 10–20 МГц, інколи до 40 МГц. Енергетичні параметри випромінювання наземних і бортових радіоелектронних систем, залежно від класу БпЛА, забезпечують дальність стабільного зв’язку до 100 км і більше за умови прямої видимості.

Радіоелектронні засоби виконують приймання, оброблення та вимірювання параметрів різних типів сигналів, а також передавання інформації між БпЛА, наземною станцією управління й іншими елементами комплексу.

Поява спотворень корисного сигналу або приймання сторонніх випромінювань погіршує роботу РЕЗ і знижує якість виконання покладених функцій. [17]

Просторово рознесені або багатоточкові перешкоди належать до найбільш результативних методів впливу на радіоелектронні засоби, оскільки такі перешкоди важко нейтралізувати звичайними суміщеними джерелами завад. Цей підхід особливо ефективний проти моноімпульсних радіопеленгаторів і багатопозиційних радіолокаційних систем.

Принцип роботи.

Перешкоди створюються одночасно з кількох просторово віддалених точок, що змінює орієнтацію фазового фронту електромагнітної хвилі, яка надходить на приймальну апаратуру. Це призводить до появи хибних пеленгів або помилкових координат, що суттєво відрізняються від реального положення цілей.

Класи просторово рознесених перешкод:

- Маскувальні шумові перешкоди. Потужні шумові випромінювання з декількох точок простору створюють зону, у якій стає неможливим виявлення та супроводження невипромінюючих об’єктів.
- Хибні цілі. Ретранслятори або передавачі, розташовані в різних точках, генерують сигнали, що імітують справжні цілі, але з іншими координатами.
- Перенацілювальні перешкоди. Створенням штучних цілей радіотехнічна система змушується переключатися на хибні об’єкти, втрачаючи контроль над реальними.

Носії просторово рознесених перешкод можуть бути різного типу: пілотовані літаки-постановники, безпілотні апарати, повільно спускаючі носії (парашути, аеростати, автожири), буксировані радіолокаційні пастки, а також ракети чи відстрілювані пристрої, оснащені передавачами перешкод.

У більшості випадків станції радіоелектронної боротьби працюють спільно або інтегруються з обладнанням радіоелектронної розвідки. Для ефективного застосування такі станції повинні генерувати перешкоди саме на

тих частотах, які використовує противник, і спрямовувати випромінювання у відповідний сектор простору. Найвищу ефективність демонструють комплекси РЕБ, що завчасно володіють інформацією про робочі частоти противника — це дозволяє негайно формувати перешкоди без витрати часу на визначення спектральних характеристик цілей. Загальні параметри антенних систем станцій радіоелектронної боротьби наведені в таблиці 3.3 [11]

Таблиця 3.3

Загальна характеристика антен станцій РЕБ

Завдання	**Діаграма**	**Поляризація**	**Діапазон**
Радіомаскування активне	Секторна*	Вертикальна, горизонтальна	VHF, UHF, 3G, Wi-Fi
Радіорозвідка (пеленгація)	Двопелюсткова	Вертикальна	VHF, UHF, 3G, Wi-Fi
Подавання радіостанцій зв’язку	Секторна, однопелюсткова	Вертикальна	VHF, UHF, 3G, Wi-Fi
Подавання каналів управління рухомих командних пунктів	Кругова, секторна*	Вертикальна, кругова	VHF, UHF, 3G, Wi-Fi
Подавання каналів управління і передавання інформації БПЛА	Секторна, однопелюсткова, кокесна	Вертикальна, горизонтальна	VHF, UHF, 3G, Wi-Fi, GPS L1, L2, L3, L4, L5

Одним із найбільш суттєвих ризиків для каналів зв’язку є навмисні перешкоди. Технічні засоби протидії таким впливам мають ключове значення для збереження стабільності та працездатності систем зв’язку БПЛА.

3.2 Використання захищених технологій зв'язку

- Технологія LoRa

Знову доводиться повернутися до вже згадуваної технології LoRa, оскільки саме вона є одним із небагатьох практичних рішень, які одночасно забезпечують стійкість каналу керування та знижують чутливість до навмисних перешкод. Причина полягає у принципах її роботи — LoRa застосовує методи модуляції, що спочатку були розроблені для підвищення завадостійкості в умовах складного радіоефіру. LoRa (Long Range) — це технологія бездротової передачі даних, що забезпечує великий радіус дії при мінімальному

енергоспоживанні. Використання LoRa дозволяє істотно підвищити стійкість каналів керування БПЛА до сторонніх сигналів і навмисних перешкод завдяки застосуванню технології розширеного спектра (Spread Spectrum). Такий підхід забезпечує підвищену здатність каналу зберігати працездатність навіть за наявності активного завадного впливу.

- Frequency Hopping Spread Spectrum (FHSS)

Технологія FHSS (Frequency Hopping Spread Spectrum) передбачає швидке та циклічне перемикання робочої частоти передавача відповідно до визначеного псевдовипадкового алгоритму. Завдяки цьому стороннє перехоплення або спроби заглушення сигналу суттєво ускладнюються. Ймовірність успішного впливу на канал зв'язку з БПЛА помітно зменшується, оскільки сторонній стороні фактично неможливо передбачити частоту, на якій відбуватиметься передавання сигналу в конкретний момент часу.

- Direct Sequence Spread Spectrum (DSSS)

Технологія DSSS передбачає розширення корисного сигналу на ширшу частотну смугу, що суттєво зменшує його чутливість до вузькосмугових завад. Такий принцип забезпечує підвищену стійкість до перешкод і дає змогу ефективно протидіяти як навмисним, так і випадковим впливам на канал зв'язку.

Перешкоди можуть бути спеціалізованими за функцією або гібридними, які поєднують превентивні та реактивні механізми і використовують інтелектуальні алгоритми для економії енергії під час впливу на мережу.

У схемі Hermes перешкоджувач керуючого каналу втрачає ефективність після застосування послідовності частотних стрибків у каналі керування. Технологія MULEPRO забезпечує багатоканальний захист від перешкод, що використовують частотні стрибки. У той час як крос-шарові методи протидіють деградації потоку даних, система FIJI блокує механізми прихованого перешкодження.

Hermes є прикладом вузла, що поєднує гібридний DSSS та FHSS, забезпечуючи підвищену стійкість до складних та адаптивних завад. [18]

Розширення спектра методом прямої послідовності (DSSS) та методом

псевдовипадкової перебудови робочої частоти (FHSS) застосовують для захисту каналів зв’язку від короткочасних та динамічних перешкод. DSSS передає сигнал у ширшій смузі частот, що зменшує вплив вузькосмугових завад, тоді як FHSS забезпечує постійне уникнення перешкод завдяки швидкій зміні робочої частоти.

На основі цих двох підходів розроблено гібридну схему DSSS–FHSS, відому як вузол Hermes, призначену для підвищення завадостійкості в сенсорних мережах. У складі цієї схеми вузол Hermes виконує до 1 000 000 частотних стрибків за секунду, що дає змогу уникати короткочасних радіоперешкод. Механізм DSSS, у свою чергу, робить переданий сигнал подібним до широкосмугового шуму для стороннього приймача, ускладнюючи спроби визначення робочого частотного діапазону. У системі Hermes використовується 55 частотних каналів для FHSS та смуга шириною 275 МГц для DSSS. Для коректного відновлення корисного сигналу необхідні як послідовність частот FHSS, так і псевдошумовий (PN) код DSSS. Генерація обох компонентів здійснюється на основі спеціального секретного слова, що слугує початковим значенням алгоритму та зазвичай жорстко закріплюється за конкретною мережею. Це дозволяє однозначно ідентифікувати новий вузол під час його підключення. Коректна робота Hermes вимагає точного узгодження між вузлами, тому механізм синхронізації, що реалізується через спеціальний канал витоку, є критично важливим елементом функціонування системи. [18]

Запобігання атакам на канал керування

Канал керування у багатоканальній бездротовій мережі відповідає за координацію використання частотних ресурсів, коли для підвищення пропускної здатності застосовується кілька робочих каналів. Щоб зменшити ризик перешкодження, використовують множину кластерів, де кожний кластер має власний канал керування з унікальною послідовністю частотних стрибків.

На рівні мережевої інфраструктури завада може впливати на канал керування, використовуючи дані, отримані від компрометованого вузла, включаючи протокольну інформацію та криптографічні параметри. Ймовірність того, що перешкоджувач зможе передбачити наступний канал керування на

основі попередніх спостережень, оцінюється через показник втекальної ентропії.

Компрометовані вузли визначаються шляхом обчислення Хеммінгової відстані між послідовністю стрибків, яку використовує завада, та реальною послідовністю частотних перестроювань мережі. Після виявлення таких вузлів система виконує відновлення каналу керування шляхом оновлення частотної послідовності FHSS. Час, необхідний для формування нового захищеного керуючого каналу, характеризується затримкою відновлення. Рівень доступності мережевого з'єднання під час атаки визначається коефіцієнтом відхилення. [19]

3.3 Методи розширення спектру для протидії ЕМ перешкодам

Одним із ефективних способів підвищення якості передавання даних у каналах зв'язку, що характеризуються значними лінійними спотвореннями або завмираннями, є застосування технологій розширення спектра. Використання такого підходу призводить до збільшення бази сигналу, що покращує його стійкість до перешкод.

Базою сигналу називають добуток ефективної тривалості сигналу та ефективної ширини його спектра. У найпростішому випадку ширину спектра можна оцінювати за розміром головного пелюстка спектральної характеристики. При цьому тривалість сигналу та його спектральна ширина пов'язані співвідношенням невизначеності, згідно з яким база сигналу не може бути меншою за одиницю.

Технології розширеного спектра первинно були розроблені для військових та спеціальних застосувань, де вимагалася підвищена завадостійкість і захищеність каналів зв'язку. Основний принцип цього методу полягає у розподіленні корисного сигналу в широкій смузі частот, що суттєво ускладнює його подавлення, перехоплення або навмисне спотворення. Першою реалізованою схемою розширеного спектра був метод перебудови робочої частоти. Подальшим розвитком стала схема прямого послідовного розширення, яка є більш сучасною та широко застосовується сьогодні. Обидва підходи

інтегровані в різноманітні стандарти та технології бездротового зв’язку й використовуються у сучасних телекомунікаційних системах.

У сучасних системах застосовуються три основні методи розширення спектра:

- Псевдовипадкова перебудова робочої частоти (FHSS)
- Пряме послідовне розширення спектра (DSSS)
- Лінійно-частотна модуляція (CSS)

FHSS (Frequency Hopping Spread Spectrum) — це технологія передавання сигналу, що реалізує швидке псевдовипадкове перемикання робочої частоти. Суть методу полягає у періодичній та стрибкоподібній зміні несучої частоти згідно з визначеним алгоритмом, який відомий як передавачу, так і приймачу. Стандарт IEEE 802.11 визначає 79 можливих частотних послідовностей, а тривалість однієї передачі становить 20 мс. [20]

Якщо частота перемикання підканалів є нижчою за швидкість передавання даних, такий режим називають повільним розширенням спектра. У протилежній ситуації, коли частота стрибків перевищує швидкість передавання, застосовується режим швидкого розширення спектра.

Швидке розширення спектра забезпечує значно вищу стійкість до перешкод. Це пояснюється тим, що вузькосмугові завади, які пригнічують сигнал у конкретному підканалі, не спричиняють втрати інформації — значення кожного біта повторюється у кількох різних частотних підканалах. Додатковою перевагою є відсутність міжсимвольної інтерференції, оскільки система встигає перейти на іншу частоту ще до приходу затриманих компонентів сигналу по одному з багатопроменевих шляхів.

Повільне розширення спектра такими перевагами не володіє, однак його реалізація є суттєво простішою, а апаратні та енергетичні витрати — меншими.

Методи FHSS застосовуються у низці бездротових технологій, включно з IEEE 802.11 та Bluetooth.

У випадку FHSS використання частотного ресурсу відрізняється від традиційних методів кодування: замість економного розподілення вузької смуги

частот відбувається спроба зайняти весь доступний діапазон. На перший погляд це може видаватися неефективним, оскільки в конкретний момент часу використовується лише одна частота. Але це твердження некоректне в загальному випадку — коди розширеного спектра дозволяють виконувати мультиплексування багатьох каналів у широкій смузі.

Методи FHSS забезпечують одночасне функціонування кількох каналів завдяки використанню різних псевдовипадкових частотних послідовностей, підібраних таким чином, щоб у кожен момент часу кожен канал працював на власній частоті [22].

На рисунку 3.1 для наглядного прикладу зображено принцип роботи чотириканальної системи FHSS, де сигнал послідовно переходить між частотними підканалами відповідно до заданої псевдовипадкової послідовності.

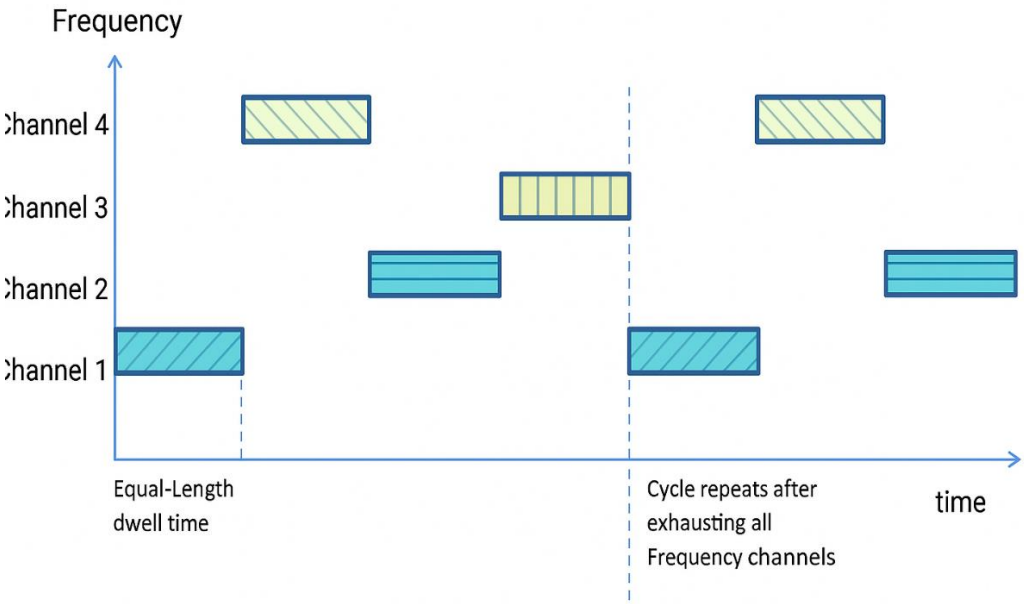

Рис. 3.1 - Чотириканальна система FHSS

Також, на рисунку 3.2 наведено структурну схему формування FHSS-сигналу. Система використовує генератор псевдовипадкової послідовності для

керування стрибками несучої частоти, що видно з характерного спектру сигналу на спектроаналізаторі. [21]

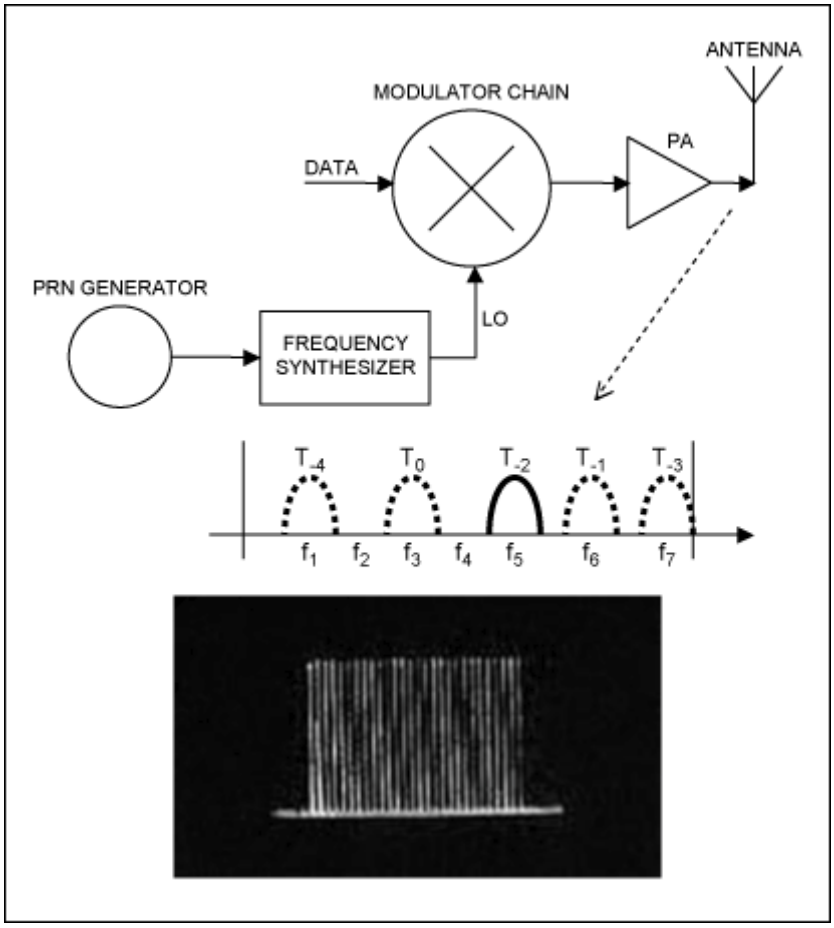

Рис. 3.2 - Схема формування FHSS-сигналу та спектральний вигляд частотних стрибків

Лінійно-частотна модуляція (CSS)

Це різновид частотної модуляції, у якому несуча змінює свою частоту за лінійним законом протягом певного інтервалу часу. Такий принцип широко використовується у радіолокаційних системах та в окремих типах радіомодемів.

Технологія CSS лежить в основі фізичного рівня радіоінтерфейсу LoRa. У цьому методі генератор формує синусоїдальний сигнал, частота якого плавно зростає або зменшується з часом, утворюючи так званий chirp-сигнал. Далі цей «чирп» переноситься на відповідну несучу частоту, утворюючи модульований сигнал.

Лінійне розширення спектра шляхом чирпування дозволяє LoRa

поширювати енергію переданого сигналу на значно ширшу смугу частот. Це забезпечує підвищену стійкість до завад та шумів, покращує співвідношення сигнал/шум на приймальній стороні та підвищує надійність декодування сигналу навіть за низьких рівнів потужності.

У телекомунікаціях методи розширеного або розподіленого спектра застосовуються для цілеспрямованого розтягування вузькосмугового сигналу в широкій частотній області. Такі підходи використовуються для:

– підвищення захищеності зв’язку,

– зменшення впливу природних і штучних електромагнітних перешкод,

– обмеження спектральної густини потужності (актуально для супутникових систем),

– зниження ймовірності виявлення передавача,

– забезпечення можливості багатоканальної роботи в одному діапазоні.

CSS, як одна з форм розподіленого спектра, поєднує енергоефективність, високу завадостійкість та можливість функціонування на великі дистанції при мінімальних вимогах до апаратної частини.

На рисунку 3.3 [23] зображено що графік показує часову еволюцію миттєвої частоти у FS-CSS модуляції. Діаграма FS-CSS включена до роботи для ілюстрації принципу лінійно-частотної модуляції типу CSS, яка використовується в LoRa-подібних системах як метод розширення спектра для підвищення завадостійкості. Графік демонструє механізм кодування інформації шляхом зсуву початкової частоти чирп-сигналу, що є ключовим для пояснення стійкості CSS до електромагнітних перешкод та доцільності застосування таких технологій у каналах зв’язку БПЛА.

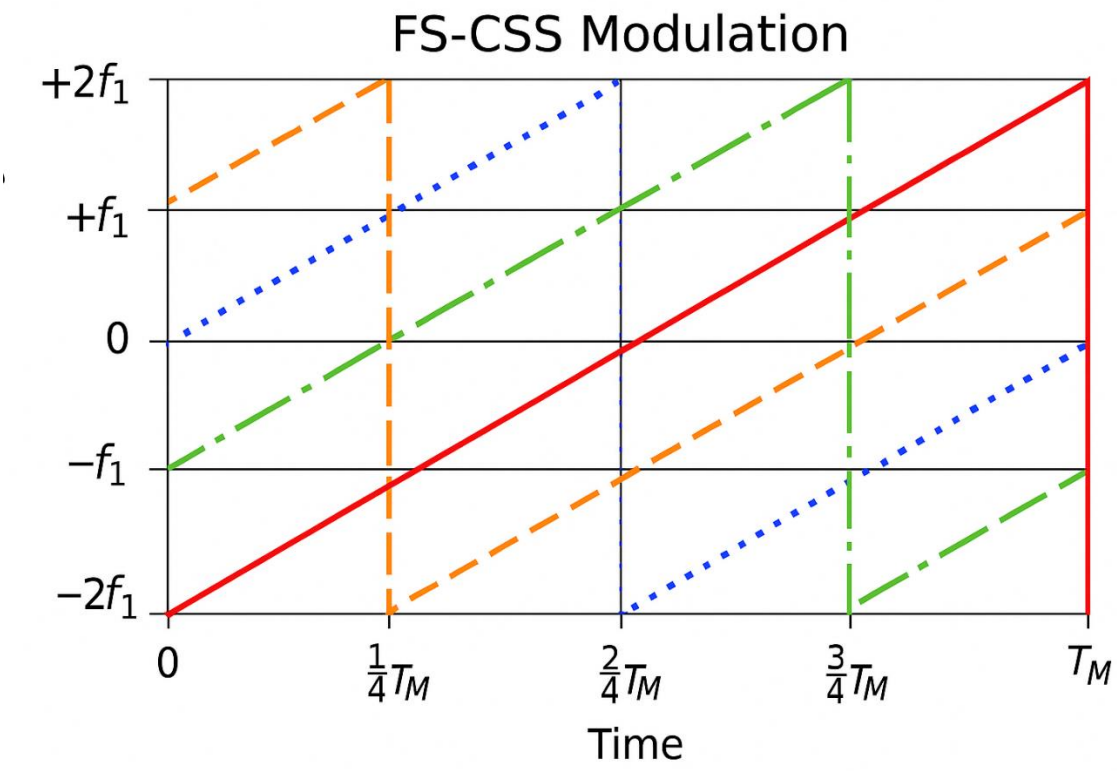

Рис 3.3 - Приклад формування чирп-сигналів у FS-CSS модуляції

Пряме послідовне розширення спектра (DSSS)

Пряме послідовне розширення спектра (DSSS) є методом формування широкосмугового сигналу, у якому вихідний бітовий потік перетворюється на псевдовипадкову послідовність, що використовується для модуляції несучої. Технологія ґрунтується на швидкому накладанні високошвидкісного псевдовипадкового коду на переданий сигнал, що приводить до збільшення його спектральної ширини.

У стандарті IEEE 802.11 цей принцип реалізується за допомогою послідовностей, які визначають правила формування розширеного сигналу. Кожен інформаційний біт замінюється на фіксовану послідовність із 11 чіпів. Усі 11 елементів цієї послідовності передаються паралельно по підканалах. При прийманні ця послідовність декодується тим самим алгоритмом, що й при передаванні. Метод допускає використання різних кодових послідовностей для різних пар передавач–приймач, і кількість можливих варіантів таких алгоритмів може бути значною.

Кожен біт інформації (логічний «0» або «1») перетворюється на набір чіпів. Якщо інформаційні біти подаються як прямокутні імпульси, то окремий чіп також є прямокутним імпульсом, але його тривалість істотно менша за тривалість вихідного біта.

Чіпові послідовності, які накладаються на інформаційні біти, називають шумоподібними кодами або PN-послідовностями. Така назва підкреслює, що після їх використання сформований сигнал набуває шумоподібного вигляду, що істотно ускладнює його відокремлення від природного шуму радіоканалу. Послідовності, які застосовуються для розширення спектра, повинні відповідати визначеним вимогам щодо автокореляційних властивостей. У математичному розумінні автокореляція характеризує ступінь подібності функції із самою собою для різних часових зсувів.

Якщо вибрати чіпову послідовність, автокореляційна функція якої має виражений максимум лише в одному точному моменті часу, то інформаційний сигнал буде можливо виділити навіть на рівні шумового фону. На приймальній стороні корисний сигнал відновлюється шляхом множення отриманої послідовності на ту саму PN-послідовність, яка використовувалася під час передавання, тобто фактично виконується обчислення автокореляційної функції.

Після цього відновлений сигнал знову стає вузькосмуговим, що дає змогу фільтрувати його у вузькій смузі частот. Будь-яка перешкода, що потрапляє в широку смугу DSSS-сигналу, після множення на чіпову послідовність перетворюється на широкосмугову компоненту і відсікається фільтрами. У вузьку смугу корисного сигналу проходить лише невелика частина перешкоди, причому з істотно меншою потужністю, ніж на вході приймача.

У практиці часто використовують послідовність Баркера (Barker code) довжиною 11 біт:

10110111000.

Ця послідовність забезпечує швидку та надійну синхронізацію приймача з передавачем, оскільки має оптимальні автокореляційні властивості. Приймач визначає появу послідовності-маркеру, послідовно порівнюючи прийняті біти зі зразком Баркера.

Перевага DSSS:

Одним із ключових результатів застосування прямого послідовного розширення спектра є підвищений захист переданої інформації від несанкціонованого перехоплення, оскільки сторонній DSSS-приймач, що використовує іншу PN-послідовність, не здатен відновити передані дані.

На рисунку 3.4 [21] знизу зображений функціональна блок-схема DSSS-передавача та фотографія спектру DSSS-сигналу зі спектроаналізатора. Вона показує, що після розширення спектра головна смуга стає ширшою, ніж у немодульованого (неспредованого) сигналу.

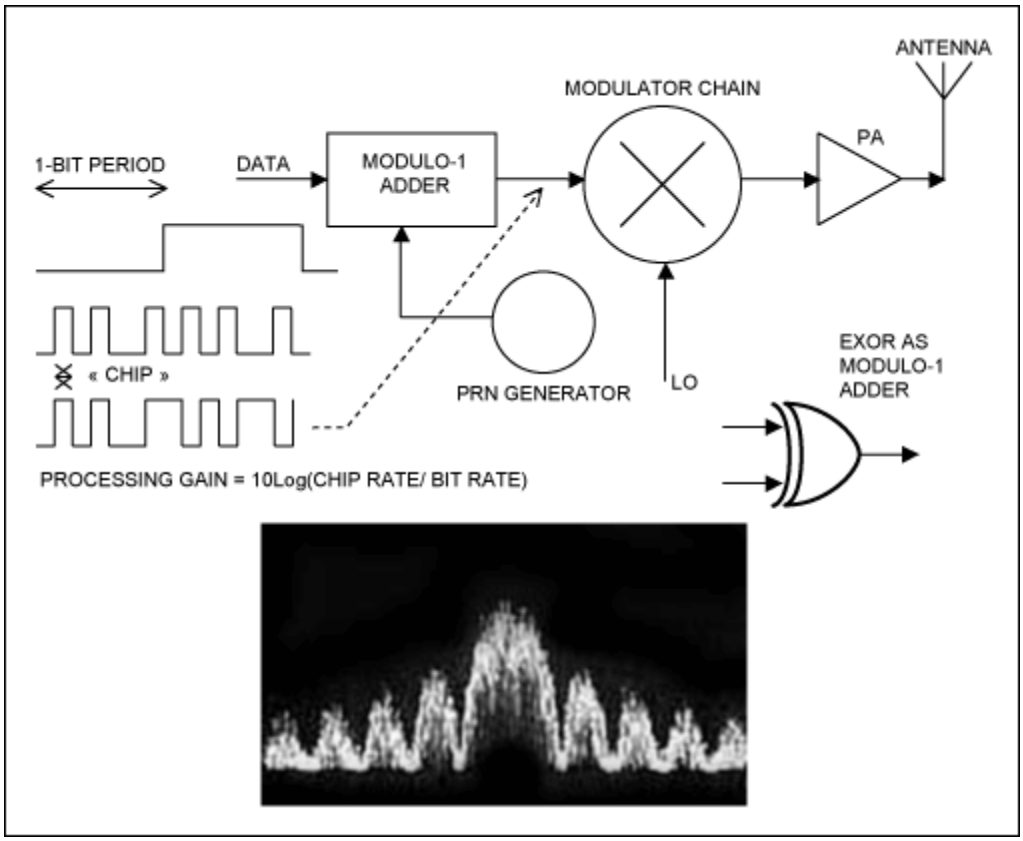

Рис. 3.4 - Структурна схема формування DSSS-сигналу та приклад його спектру на спектроаналізаторі

3.4 Використання ЛЧМ сигналів

Вибір конкретного типу модуляції визначається вимогами до системи та її функціональним призначенням. Частотномодульовані (ЧМ) сигнали застосовують у широкому спектрі задач — від гідро- та радіолокації до іоносферних досліджень, геолокації, радіонавігації, каналів зв'язку наземного та космічного базування, вимірювальних систем і медичних технологій.

Використання складних сигналів із лінійною частотною модуляцією (ЛЧМ) забезпечує високу роздільну здатність за дальністю та швидкістю, а також підвищує інформативність радіотехнічних засобів. Широке застосування ЛЧМ-сигналів зумовлене їхніми ключовими перевагами: можливістю реалізувати значну девіацію частоти (до 1 ГГц і більше), високою швидкістю частотного перестроювання, відносною простотою зміни обвідної та швидкості модуляції для покращення характеристик стисненого сигналу, а також зручністю вимірювання і корекції спотворень.

Використання широкосмугових та надширокосмугових ЛЧМ-сигналів дозволяє одночасно визначати дальність і швидкість навіть за наявності завад, зокрема тоді, коли зондувальний сигнал формується як комбінація кількох ЛЧМ-імпульсів із різними початковими фазами, частотами, тривалостями та швидкостями модуляції. На основі ЛЧМ-сигналів формують неперервні ЧМ-сигнали трикутної, пилкоподібної, зигзагоподібної форми, а також сигнали з V- або М-подібною модуляцією. Значний інтерес становлять ЛЧМ-сигнали з внутрішньоімпульсною фазовою маніпуляцією (ЛЧМ-ФМ), які забезпечують вищу точність і кращу здатність до розрізнення цілей ніж класичні ЛЧМ-імпульси.

Окремий напрямок розвитку — іоносферний моніторинг за допомогою багатофункціональних іонозондів, що використовують ЛЧМ-сигнали з широкими смугами ($B > 100$) у діапазоні коротких хвиль. Якість інформації в таких системах визначається відношенням сигнал/шум на виході приймача, яке пропорційне добутку SNR на вході на базу сигналу B. Використання сигналів з

великими базами дозволяє зменшити потужність випромінювання і відповідно — знизити масо-габаритні характеристики апаратури. У країнах НАТО ЛЧМ-іонозонди є основою сучасних систем іоносферного зондування та частотного диспетчерування.

ЛЧМ-сигнали активно застосовують і в галузі захищених систем зв’язку. Нерегулярні сигнальні конструкції на основі ЛЧМ дозволяють підвищити завадостійкість та прихованість радіоліній. У системах передачі командних сигналів ЛЧМ використовують для підвищення надійності при роботі з сигналами відносної фазової телеграфії (ОФТ), де кожному символу двійкового коду надається власна ЛЧМ-структура, що забезпечує широкосмуговість каналу.

Актуальним завданням під час розроблення радіотехнічної апаратури на основі ЛЧМ є розширення спектра імпульсів без зменшення їхньої тривалості, що реалізують за допомогою внутрішньоімпульсної модуляції та маніпуляції; збільшення девіації частоти; удосконалення методів формування та прийому сигналів в умовах дії пасивних і активних завад; підвищення енергетичної ефективності та зменшення масо-габаритних показників.

Аналогові методи формування широкосмугових ЛЧМ-сигналів мають суттєві недоліки: недостатню стабільність частоти, спотворення форми сигналу, обмежену швидкість частотного керування, складність отримання дуже коротких імпульсів (< 0,1 мкс), значне енергоспоживання та вимоги до живлення. Формування ЛЧМ-імпульсів з великими девіаціями частоти та базами потребує високої точності, що складно забезпечити у традиційних аналогових схемах.

Сучасні цифрові методи — прямий цифровий синтез (DDS), пряма цифрова модуляція (DDM), застосування швидкодіючих АЦП — відкривають можливість формувати практично будь-які типи модульованих сигналів без обмежень, характерних для аналогових систем. Це дозволяє підвищити ефективність використання спектра, інформативність радіолокаційних засобів і завадостійкість без значних конструктивних змін.

ЧМ-сигнали зберігають високу стійкість до завад, точність вимірювань та

здатність працювати «під шумами». У застосуваннях із великими смугами та високими базами ЛЧМ має переваги над іншими ФМ-сигналами:

– простіша корекція спотворень у тракті;

– можливість перетворення широкосмугового ЛЧМ у вузькосмуговий сигнал з подальшою цифровою обробкою;

– використання сучасних надшвидких генераторів СВЧ (включно з генераторами Ганна), що забезпечують смуги в кілька гігагерц зі швидкістю перебудови 20–50 ГГц/мкс.

Отже, зростає інтерес до ЛЧМ-ФМ-сигналів, які розширюють можливості сучасних систем, покращують розрізнення за дальністю та швидкістю і забезпечують можливість застосовувати вагову обробку для зниження бічних пелюсток. Спектр ЛЧМ-ФМ формується як сума зміщених спектрів ЛЧМ-імпульсів, а зі збільшенням довжини кодової послідовності він набуває рис спектра шумоподібного сигналу — при цьому смуга займає ширший частотний діапазон.

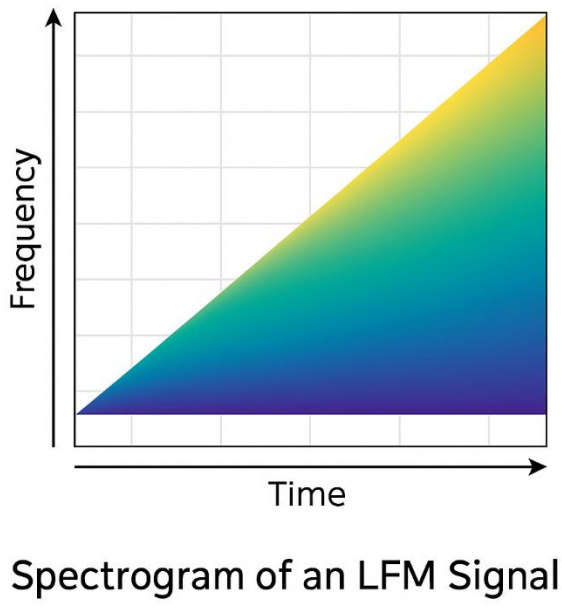

Рис. 3.5 - Спектрограма лінійно-частотно модульованого (ЛЧМ) сигналу

Графік показує типовий вигляд ЛЧМ сигналу у часо-частотній площині: частота сигналу лінійно зростає впродовж часу. Такий «чирп» (chirp) є основою ЛЧМ-

модуляції, яка широко застосовується в радіолокації, зв'язку та завадостійких каналах керування. Він наочно демонструє фундаментальну властивість ЛЧМ сигналів – лінійне розширення спектра у часі, що безпосередньо пов’язано з їх високою завадостійкістю, здатністю працювати «під шумами» та використанням у системах з великими базами сигналів. У контексті роботи про протидію ЕМ перешкодам така ілюстрація обґрунтовує, чому ЛЧМ-сигнали є ефективними в радіолініях керування й каналах зв’язку БПЛА.

РОЗДІЛ 4
ТЕХНІЧНА ЧАСТИНА

Одним із найважливіших завдань під час оцінювання стійкості безпілотних літальних апаратів є визначення реакції їхніх електронних вузлів на вплив електромагнітного випромінювання різної інтенсивності. У сучасних умовах експлуатації БПЛА, особливо під час виконання польотів у районах активного застосування засобів радіоелектронної боротьби, рівень електромагнітних полів може коливатися в широкому діапазоні частот і потужностей. Такі впливи здатні викликати наведення паразитних напруг на провідникових елементах плати, порушення логічних рівнів на входах мікроконтролерів або навіть відмову окремих модулів керування.

Проведення моделювання дозволяє без необхідності фізичних випробувань оцінити, як зміна інтенсивності та частоти електромагнітного поля впливає на параметри електронних компонентів. Це дає змогу прогнозувати умови, за яких можуть виникати збої, і визначати ефективність елементарних заходів захисту — таких як RC-фільтрація, екранування або зміна топології друкованої плати.

Основна мета цього моделювання полягає у кількісній оцінці рівня наведеної напруги на входах мікроконтролера під впливом зовнішнього електромагнітного випромінювання. Отримані результати дозволяють:

- виявити критичні частотні діапазони, у яких електронна система є найбільш вразливою;

- визначити залежність рівня наведеної напруги від інтенсивності електромагнітного поля;

- оцінити ефективність простого вхідного RC-фільтра у зменшенні амплітуди наведень;

- сформувати практичні рекомендації щодо підвищення завадостійкості схем керування БПЛА.

Я це зробив, щоб отримати кількісну оцінку того, як електромагнітне випромінювання різної інтенсивності впливає на електронні компоненти системи керування БПЛА. У реальних умовах експлуатації безпілотних літальних апаратів, особливо в середовищі з підвищеною радіочастотною активністю або навмисним застосуванням засобів радіоелектронного придушення, на провідникових елементах плати можуть виникати наведені напруги, здатні порушувати нормальну роботу мікроконтролера та інших критичних модулів.

Щоб оцінити реакцію системи керування на зовнішнє електромагнітне поле, була побудована спрощена модель, яка включає:

Вхід системи керування моделюється як простий RC-фільтр:

- серійний резистор R_s,

- шунтуючий конденсатор C_f.

Схема для обчислення фільтра:

$$|H_{RC}(j\omega)| = \frac{X_C}{\sqrt{R_s^2 + X_C^2}}, \quad X_C = \frac{1}{\omega C_f}.$$

Фільтр імітує базовий захист від високочастотних завад (типовий для польотних контролерів, GPS-модулів та радіомодемів БПЛА).

Порогове значення:

Для оцінки збою приймається, що на входах логіки порушення може виникати при рівнях: $V_{\text{th}} = 0.2\ \text{В}.$

Це спрощене порогове значення, що відображає реальний факт: цифрові входи чутливі до високочастотних наведень навіть на субвольтних рівнях.

У коді я задав такі параметри:

- частоти: 100 кГц–1 ГГц (характерний діапазон завад БПЛА)

- рівні поля: 1–100 В/м

- довжина провідника: 5 см

- площа петлі: 1 см²

- RC-фільтр: $R_s = 100\ \Omega, C_f = 1$ нФ

Для створення графіків я використовував середовище Google Colab:

Код буде зображений у Додатку А:

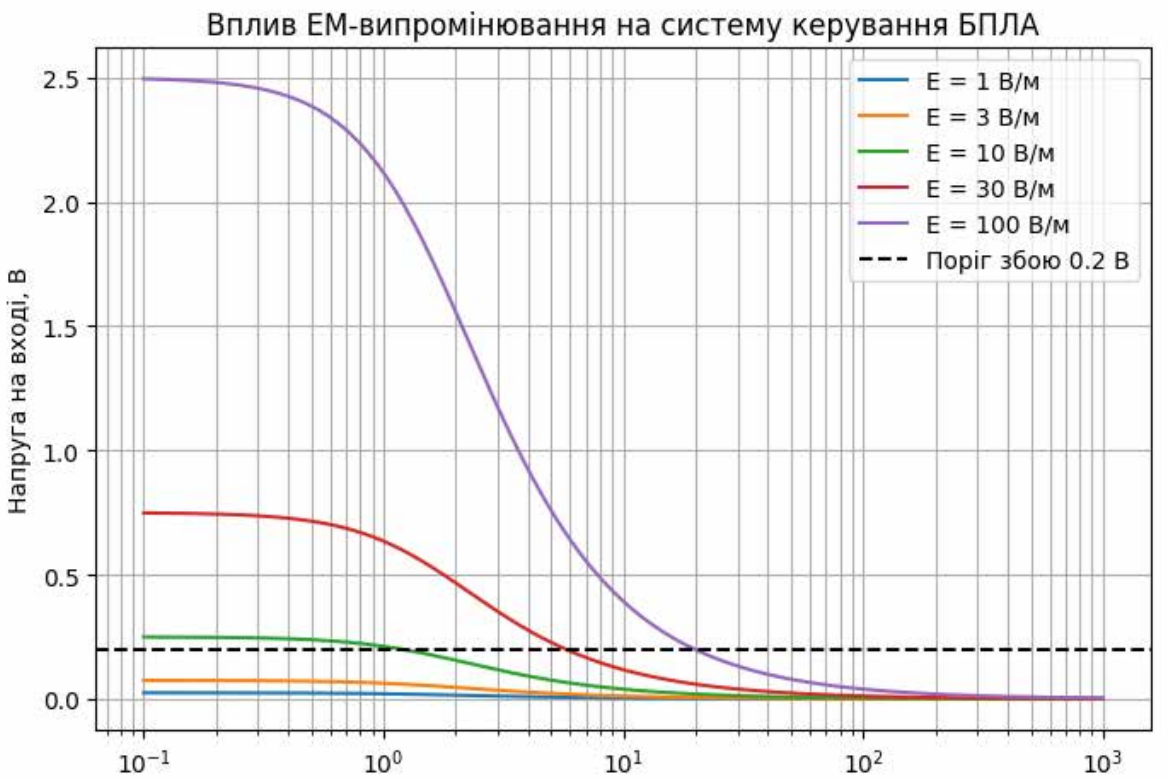

Рис. 4.1 – Залежність напруги від частоти і рівня зовнішнього поля

На графіку видно, як наведена напруга залежить від частоти і рівня зовнішнього поля.

На низьких частотах переважає електричний канал наведення.

На високих частотах (100–1000 МГц) магнітний канал через залежність від потужності різко збільшує амплітуду наведеної напруги. При рівнях поля 30–100 В/м напруга на вході наближається або перевищує 0.2 В → це може спричинити хибні спрацьовування мікроконтролера.

Це повністю відповідає практичним ситуаціям з РЕБ, коли високочастотні імпульси можуть порушувати роботу автопілота БПЛА.

У другому графіку я зобразив зони, де вхідна напруга перевищує поріг збою. Цей графік дозволяє зрозуміти, в яких поєднаннях частоти та E-поля БПЛА найбільш вразливий та оцінити ефективність навіть базового RC-фільтра;

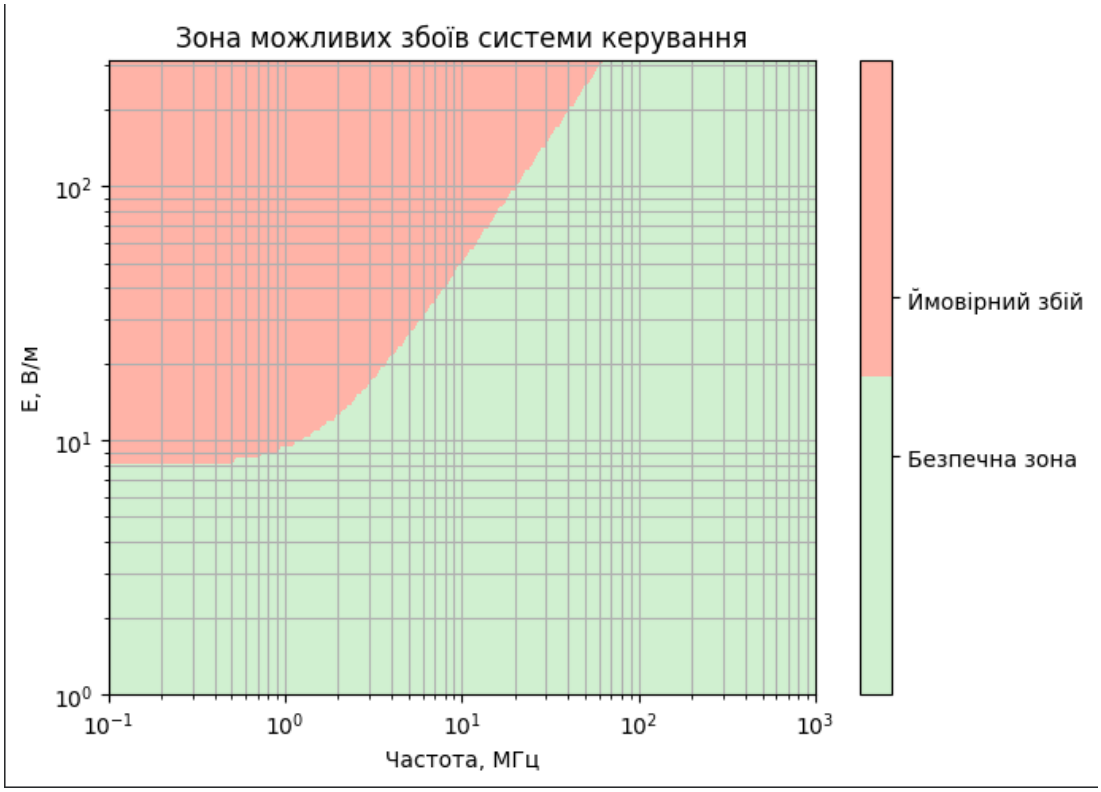

Рис. 4.2 - Карта ризику

- Зелена зона — безпечна область, де ЕМ-вплив не спричиняє критичних наведень.

- Рожева зона — область, де рівень наведеної напруги достатній для можливих збоїв у системі керування.

У межах виконаного моделювання було встановлено, що рівень електромагнітного впливу здатний суттєво змінювати умови роботи електронних компонентів системи керування БПЛА. Аналіз залежності наведеної напруги від частоти зовнішнього поля та інтенсивності випромінювання показав, що у високочастотному діапазоні спостерігається різке зростання амплітуди наведень, зумовлене домінуванням магнітної складової поля. За визначених геометричних параметрів плати та прийнятого порогового

рівня було зафіксовано області, у яких наведена напруга досягає значень, потенційно здатних вплинути на роботу входів мікроконтролера та порушити цілісність керуючих сигналів.

Дослідження також продемонструвало, що елементарні фільтрувальні засоби, зокрема простий RC-ланцюг, забезпечують помітне зменшення рівня високочастотних наведень, проте не усувають ризик повністю в умовах дії інтенсивного електромагнітного поля. Побудована карта ризику підтвердила наявність чітко окреслених зон, у яких поєднання частоти та напруженості поля створює підвищену ймовірність некоректної роботи системи керування.

Таким чином, отримані результати свідчать про необхідність урахування електромагнітних впливів під час проектування апаратної частини БПЛА, зокрема оптимізації топології друкованих плат, мінімізації розмірів провідникових петель, вибору ефективніших фільтрувальних елементів та можливого застосування додаткових засобів екранування. Проведене моделювання формує аналітичну основу для подальшого підвищення завадостійкості систем керування безпілотних літальних апаратів і підтверджує важливість комплексного підходу до їх електромагнітної сумісності.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

Виконана магістерська робота присвячена комплексному дослідженню стійкості безпілотних літальних апаратів до впливу електромагнітних перешкод. Поставлена у завданні мета — дослідити функціонування БПЛА в умовах дії завад — була реалізована шляхом поєднання теоретичного аналізу, огляду сучасних засобів радіоелектронної боротьби та практичного моделювання електромагнітних впливів на елементи системи керування апарата. Згідно з визначеним у тексті об’єктом дослідження, робота зосереджувалася на БПЛА як радіоелектронній системі, що функціонує у складному електромагнітному середовищі

У роботі показано, що електромагнітні завади, які можуть виникати як у природних умовах, так і внаслідок цілеспрямованого застосування засобів РЕБ, здатні впливати на працездатність ключових підсистем БПЛА — радіоканалу керування, навігаційних модулів, сенсорних систем та обчислювальної частини автопілота. Виконане моделювання підтвердило, що окремі елементи друкованої плати системи керування можуть працювати як пасивні приймальні структури, на яких індукуються паразитні напруги з амплітудами, здатними порушувати коректність роботи цифрових входів. Зокрема, побудовані моделі та графіки дозволили кількісно оцінити залежність наведеної напруги від частоти випромінювання та напруженості поля, що є фундаментальним аспектом під час проєктування апаратури БПЛА.

Особливе значення мають результати моделювання високочастотної дії електромагнітного поля: було встановлено, що із зростанням частоти різко збільшується внесок магнітної складової, що призводить до формування зон ризику, у яких рівень наведеної напруги перевищує порогові значення для входів мікроконтролера. Це співвідноситься з тими висновками, які вже частково відображені в документі — про існування частотно-польових областей, де ймовірність некоректної роботи системи керування суттєво зростає.

Результати дослідження підтвердили, що навіть елементарні засоби захисту, такі як серійні резистори та шунтуючі ємності, можуть значною мірою зменшувати вплив високочастотних наведень, але не усувають його повністю за умов дії інтенсивних полів. Це свідчить про необхідність використання комбінованого підходу до забезпечення електромагнітної стійкості, який включає оптимізацію топології друкованої плати, мінімізацію провідникових петель, застосування екранувальних матеріалів, удосконалення фільтраційних схем і використання спеціалізованих захисних компонентів.

Таким чином, отримані у роботі результати формують аналітичну основу для подальшого вдосконалення конструкції БПЛА з погляду електромагнітної сумісності. Дослідження доводить важливість урахування електромагнітного середовища на ранніх етапах проєктування системи керування та підтверджує, що правильний вибір схемотехнічних і конструктивних рішень здатний суттєво підвищити надійність функціонування апарата в умовах інтенсивних електромагнітних впливів. Це узгоджується з висновками, відображеними у документі, щодо значення комплексного врахування електромагнітних факторів під час проєктування апаратної частини БПЛА.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kumar S., Shukla S. Concepts and Applications of Microwave Engineering. – New Delhi : PHI Learning Pvt. Ltd., 2014. – 3 p. – ISBN 978-8120349353.

2. Design, Simulation and New Applications of Unmanned Aerial Vehicles. – 2023.

3. Vinogradov E., Kumar A. V. S. S. B., Minucci F., Pollin S., Natalizio E. Remote ID for separation provision and multi-agent navigation // Proceedings of the 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC). – 2023. – P. 1–10. – DOI: 10.1109/DASC58513.2023.10311133.

4. Kaidenko M., Kravchuk S. Principles of Constructing Communication and Control Systems Protected from the Effects of Jamming Attacks for Small-Sized Unmanned Aerial Vehicles // In: Ilchenko M., Uryvsky L., Globa L. (eds) Progress in Advanced Information and Communication Technology and Systems. MCiT 2021. – Cham : Springer, 2023. – (Lecture Notes in Networks and Systems ; vol. 548). – DOI: 10.1007/978-3-031-16368-5_20.

5. Electromagnetic Interference and Shielding. – Weinheim : Wiley-VCH GmbH, 2021.

6. Mili S., Deniau V., Sodoyer D., Heddebaut M., Ambellouis S. Jamming Detection Methods to Protect Railway Radio Communication // International Journal of Engineering and Innovative Technology (IJEIT). – 2015. – Vol. 4, № 7. – P. 71–77.

7. Cadence PCB Solutions. RF Interference: Types and Effects [Електронний ресурс]. – Режим доступу: https://www.cadence.com

8. Bilandzija J. The key elements of communication jamming. How can intentional signal disorders be prevented? [Електронний ресурс]. – Режим доступу: https://www.grin.com/document/416070

9. Haider Z., Saleem M., Jamal T. Wireless Communication Interference and Mitigation Techniques. – arXiv:1810.13164, 2018. – Режим доступу: https://arxiv.org/pdf/1810.13164

10. Interference basics and interference types. RF Wireless World [Електронний ресурс]. – Режим доступу: https://www.rfwirelessworld.com/Articles/Interference-basics-and-Interference-types.html

11. Способи підвищення надійності та стійкості каналів телеметрії в умовах радіоперешкод та РЕБ. [Електронний ресурс]. – Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/04fd672c-b6ea-45f7-a323-edc916bf63da/content

12. Berg J. S. Broadcasting on the Short Waves, 1945 to Today. – Jefferson, NC : McFarland, 2008. – P. 46. – ISBN 978-0-7864-5198-2.

13. Zidane Y. Jamming and Spoofing Techniques for Drone Neutralization // Drones. – 2024. – Vol. 8, № 12. – Article 743. – DOI: 10.3390/drones8120743.

14. Groza-S counter-UAV electronic warfare station. [Електронний ресурс]. – Режим доступу: https://www.bvpservice.by/en/catalog/radio-aintelligence-and-electronic-warfare-equipment/groza-s-counter-uav-electronic-warfare

15. Кайденко М. М., Роскошний Д. В., Гетьман О. В. Оцінка живучості каналу зв'язку БПЛА в умовах впливу навмисних та ненавмисних завад // Перспективи телекомунікацій : матеріали XVI Міжнародної науково-технічної конференції ПТ-2022. – Київ : КПІ ім. І. Сікорського, 2022. – С. 124–126.

16. Гетьман О. В., Кайденко М. М. Характеристики навмисних завад, що діють на канал зв'язку безпілотного літального апарату // Перспективи телекомунікацій : матеріали XVI Міжнародної науково-технічної конференції ПТ-2022. – Київ : КПІ ім. І. Сікорського, 2022. – С. 143–145.

17. Іщенко Д. А., Кирилюк В. А. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем // Проблеми створення, випробування та експлуатації складних інформаційних систем. – 2017. – Вип. 14. – С. 116–129. – Режим доступу: http://nbuv.gov.ua/UJRN/Psvz_2017_14_15

18. Mpitziopoulos A., Gavalas D., Pantziou G., Konstantopoulos C. Countermeasures against radio jamming attacks in wireless sensor networks // IEEE Communications Surveys & Tutorials. – 2011.

19. Jamming and Anti-jamming Techniques in Wireless Networks: A Survey. [Електронний ресурс]. – Режим доступу: https://scholarworks.montana.edu/server/api/core/bitstreams/b1d9de32-0aa5-4aa9-b6e1-9dde2aee188c/content

20. Методи розширення спектру. [Електронний ресурс]. – Режим доступу: https://prezi.com/ndxzu9giwq-a/dsss/

21. Analog Devices. Direct-Sequence Spread Spectrum (DSSS) Techniques. – Norwood, MA : Analog Devices, 2003. – 28 p.

22. Технологія розширення спектру. [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/5949802/page:29/

23. Shoaib M. WirelessPi: A Signal Processing Crash Course. – Online tutorial. – Режим доступу: https://wirelesspi.com

Додаток А.

```
import numpy as np

import matplotlib.pyplot as plt



# --------------------------

# 1. Фізичні параметри

# --------------------------

mu0  = 4 * np.pi * 1e-7

eta0 = 377.0



f_Hz  = np.logspace(5, 9, 400)

omega = 2 * np.pi * f_Hz



E_levels = np.array([1, 3, 10, 30, 100])



l_trace = 0.05

A_loop  = 0.01 * 0.01

N_loop  = 1
```

```
Rs  = 100.0

Cf  = 1e-9


V_th = 0.2



# ---------------------------

# 2. Моделі наведень

# ---------------------------

def voc_electric(E, l):

    return E * (l / 2)


def voc_magnetic(E, A, N, omega):

    H = E / eta0

    return omega * mu0 * N * A * H


def rc_transfer_mag(omega, Rs, Cf):

    Xc = 1 / (omega * Cf)

    return Xc / np.sqrt(Rs**2 + Xc**2)
```

```
H_rc = rc_transfer_mag(omega, Rs, Cf)



# ---------------------------

# 3. Графік наведеної напруги

# ---------------------------

plt.figure(figsize=(7, 5))

for E in E_levels:

    Voc_E = voc_electric(E, l_trace) * np.ones_like(f_Hz)

    Voc_H = voc_magnetic(E, A_loop, N_loop, omega)



    Vin_E = Voc_E * H_rc

    Vin_H = Voc_H * H_rc

    Vin_max = np.maximum(Vin_E, Vin_H)



    plt.semilogx(f_Hz/1e6, Vin_max, label=f"E = {E} В/м")



plt.axhline(V_th, linestyle='--', color='k', label='Поріг збою 0.2 В')
```

```
plt.xlabel('Частота, МГц')

plt.ylabel('Напруга на вході, В')

plt.title('Вплив ЕМ-випромінювання на систему керування БПЛА')

plt.grid(True, which="both")

plt.legend()

plt.tight_layout()

plt.show()



# ---------------------------

# 4. Карта ризику

# ---------------------------

E_grid = np.logspace(0, 2.5, 120)

f_grid = np.logspace(5, 9, 240)

Omega  = 2*np.pi*f_grid


H_rc_grid = rc_transfer_mag(Omega, Rs, Cf)
```

```
Vin_map = np.zeros((len(E_grid), len(f_grid)))


for i, E in enumerate(E_grid):
    VocE = voc_electric(E, l_trace) * np.ones_like(f_grid)
    VocH = voc_magnetic(E, A_loop, N_loop, Omega)

    Vin_map[i] = np.maximum(VocE * H_rc_grid, VocH * H_rc_grid)


fail_mask = (Vin_map >= V_th).astype(float)


plt.figure(figsize=(7, 5))
c = plt.contourf(f_grid / 1e6, E_grid, fail_mask,
                 levels=[-0.5, 0.5, 1.5],
                 colors=["#d0f0d0", "#ffb3a7"])


plt.xscale('log')
plt.yscale('log')


plt.xlabel('Частота, МГц')
```

```
plt.ylabel('E, В/м')

plt.title('Зона можливих збоїв системи керування')

plt.grid(True, which="both")


cbar = plt.colorbar(c, ticks=[0.25, 0.75])

cbar.ax.set_yticklabels(['Безпечна зона', 'Ймовірний збій'])


plt.tight_layout()

plt.show()
```