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

Навчально-науковий інститут телекомунікаційних систем

Кафедра телекомунікацій

До захисту допущено:

Завідувач кафедри

_____Сергій КРАВЧУК

«___»_____2025 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інженерія та програмування інфокомунікацій»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Дослідження ефективності методів протидії впливу навмисних завад на канали зв'язку БПЛА»

Виконав:
студент IV курсу, групи ТЗ-12
Пахолок Павло Володимирович _____

Керівник:
Старший викладач кафедри ТК НН ІТС,
Кайденко Микола Миколайович _____

Рецензент:
Доцент кафедри ІТТ НН ІТС, к.т.н., доцент,
Правило Валерій Володимирович _____

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

Київ – 2025 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій КРАВЧУК
«___»_____2025 р.

ЗАВДАННЯ
на дипломну роботу студенту
Пахолку Павлу Володимировичу

1. Тема роботи «Дослідження ефективності методів протидії впливу навмисних завад на канали зв’язку БПЛА», керівник роботи Кайденко Микола Миколайович, затверджені наказом по університету від «26» травня 2025 р. № 1755-с.

2. Термін подання студентом роботи 9 червня 2025 р.

3. Вихідні дані до роботи: БПЛА малогабаритний, максимальна дальність до 10 км; завада — широкосмугова енергетична у вигляді білого шуму; завада ЛЧМ у широкому діапазоні частот; використовується модуляція LoRa з chirp spread spectrum (CSS); тип каналу — радіоканал; діапазони робочих частот визначені у “The European table of frequency allocations and applications in the frequency range 8.3 kHz to 3000 GHz (ECA Table)”, зокрема 868 МГц.

4. Зміст роботи: Аналіз проблеми впливу навмисних завад на канали зв’язку БПЛА. Дослідження методів протидії впливу навмисних завад на канали зв’язку. Вивчення особливостей технологій FHSS, FEC, DSSS, LoRa та визначення їх ефективності для протидії навмисним завадам. Розробка моделі каналу зв’язку з урахуванням різних типів завад. Моделювання впливу білого шуму та ЛЧМ-завад на якість зв’язку. Порівняння ефективності методів захисту FHSS, DSSS, LoRa CSS та FEC. Аналіз результатів та формування рекомендацій щодо застосування технологій захисту.

5. Перелік ілюстративного матеріалу:

Слайд 1: Тема дослідження;
Слайд 2: Мета та актуальність роботи;

Слайд 3: Поставленні завдання;
Слайд 4: Класифікація навмисних завад (енергетична, ЛЧМ, імітаційна, імпульсна);
Слайд 5: Ключові підходи захисту каналів зв’язку ;
Слайд 6: Параметри дослідження ефективності методів протидії завадам;
Слайд 7: Результати досліджень BER для різних методів захисту (білий шум, ЛЧМ);
Слайд 8: Практична цінність роботи та сфери застосування результатів;
Слайд 9: Загальні висновки щодо ефективності методів протидії;
Слайд 10: Використані джерела.

6. Дата видачі завдання 31 березня 2025 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Підбір та вивчення літератури з питань впливу навмисних завад на канали зв’язку БПЛА	31.03 – 06.04.2025	Виконано
2	Аналіз архітектури систем зв’язку БПЛА та типових протоколів управління	07.04 – 13.04. 2025	Виконано
3	Класифікація типів навмисних завад (енергетичні, ЛЧМ, структуровані, імпульсні)	14.04 – 20.04. 2025	Виконано
4	Огляд сучасних технологій протидії завадам (FHSS, DSSS, LoRa CSS, FEC, SDR)	21.04 – 27.04. 2025	Виконано
5	Визначення критеріїв оцінки ефективності захисту (BER, SNR, Eb/N₀)	28.04 – 04.05. 2025	Виконано
6	Побудова моделі каналу управління БПЛА з використанням LoRa CSS, DSSS, FHSS	05.05 – 11.05. 2025	Виконано
7	Моделювання впливу білого шуму та ЛЧМ завад на різні методи захисту	12.05 – 18.05. 2025	Виконано
8	Аналіз результатів: побудова графіків BER залежно від Eb/N₀, порівняння ефективності	19.05 – 25.05. 2025	Виконано
9	Підготовка висновків і оформлення дипломної роботи	26.05 – 01.06. 2025	Виконано

Студент Павло ПАХОЛОК

Керівник Микола КАЙДЕНКО

РЕФЕРАТ

Дипломна робота містить 57 сторінок, 3 рисунок, 2 таблиці. Було використано 9 джерел.

Ця дипломна робота присвячена дослідженню ефективності методів протидії впливу навмисних завад на канали зв’язку безпілотних літальних апаратів (БПЛА). З огляду на зростаючу роль БПЛА в розвідці, логістиці, обороні та інших сферах, забезпечення стійкого керування в умовах радіоелектронного протистояння стає критично важливим завданням.

Метою роботи є аналіз різних типів навмисних завад (енергетичні, ЛЧМ, структуровані, імпульсні), визначення їх впливу на надійність каналу зв’язку та оцінка ефективності технологій захисту, зокрема FHSS, DSSS, LoRa CSS, FEC та засобів автентифікації. У межах дослідження було розроблено модель каналу управління БПЛА, проведено моделювання впливу різних завад на рівень BER та SNR, а також виконано порівняння завадостійкості окремих модуляцій.

Пояснювальна записка побудована з трьох основних розділів, що охоплюють теоретичні аспекти побудови систем зв’язку БПЛА, класифікацію та вплив завад, а також аналіз ефективності захисних технологій. До роботи включено одну діаграму (блок-схема системи протидії), кілька графіків BER до Eb/N₀, а також три таблиці з технічними характеристиками, результатами моделювання та узагальненими рекомендаціями.

Результати дослідження підтверджують, що технології з розширенням спектру та адаптивним управлінням параметрами (зокрема LoRa CSS та FHSS) демонструють найвищу ефективність у протидії завадам. Проте навіть вони потребують посилення протокольної безпеки шляхом впровадження автентифікації та цифрових підписів.

Отримані висновки мають практичну цінність для проєктування каналів управління БПЛА в умовах РЕБ та можуть бути використані для вдосконалення апаратних і програмних засобів захисту. Перспективними напрямами подальших досліджень є впровадження гібридних схем захисту та розробка алгоритмів автоматичного розпізнавання типу завади в режимі реального часу.

Ключові слова: канал зв’язку, БПЛА, навмисна завада, LoRa CSS, FHSS, протидія, радіоелектронна боротьба

ABSTRACT

The thesis consists of 57 pages, 3 figure, and 3 tables. Nine sources were used in the research.

This thesis is dedicated to studying the effectiveness of countermeasures against intentional interference affecting the communication channels of unmanned aerial vehicles (UAVs). Given the growing role of UAVs in reconnaissance, logistics, defense, and other sectors, ensuring reliable control under electronic warfare conditions is a critically important task.

The objective of this work is to analyze various types of intentional interference (such as broadband noise, linear frequency modulation (LFM), structured and impulse jamming), assess their impact on the reliability of communication channels, and evaluate the efficiency of protection technologies, including FHSS, DSSS, LoRa CSS, FEC, and authentication mechanisms. Within the scope of the study, a UAV control channel model was developed, simulation of interference impact on BER and SNR was conducted, and the jamming resistance of selected modulation methods was compared.

The explanatory note consists of three main sections covering the theoretical fundamentals of UAV communication systems, classification and influence of jamming types, and evaluation of protective technologies. The thesis includes one diagram (a block diagram of the countermeasure system), several BER/Eb/N₀ graphs, and three tables presenting technical specifications, simulation results, and summarized recommendations.

The results confirm that technologies based on spread spectrum and adaptive parameter control (particularly LoRa CSS and FHSS) demonstrate the highest effectiveness in resisting interference. However, even these require reinforcement at the protocol level through the implementation of authentication and digital signatures.

The findings have practical value for designing UAV control links under jamming conditions and can be applied to improve both hardware and software protection measures. Promising areas for future research include the integration of hybrid protection schemes and the development of real-time algorithms for detecting and classifying interference types.

Keywords: communication channel, UAV, intentional interference, LoRa CSS, FHSS, countermeasures, electronic warfare.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

БПЛА	Безпілотний літальний апарат
AES	Advanced Encryption Standard
ARQ	Automatic Repeat Request
BER	Bit Error Rate
BW	Bandwidth
CRC	Cyclic Redundancy Check
CR	Coding Rate
DSSS	Direct Sequence Spread Spectrum
EDC	Error Detection and Correction
ESC	Electronic Speed Controller
FH	Frequency Hopping
FHSS	Frequency Hopping Spread Spectrum
FEC	Forward Error Correction
FSK	Frequency Shift Keying
GFSK	Gaussian Frequency Shift Keying
GCS	Ground Control Station
LoRa CSS	LoRa Chirp Spread Spectrum
MAVLink	Micro Air Vehicle Link
MIMO	Multiple Input Multiple Output
MTBF	Mean Time Between Failures
PER	Packet Error Rate
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RFM	Radio Frequency Module
RSSI	Received Signal Strength Indicator
RX	Receiver
SNR	Signal-to-Noise Ratio
SF	Spreading Factor
TX	Transmitter
UART	Universal Asynchronous Receiver

ВСТУП

З розвитком технологій безпілотні літальні апарати (БПЛА) стали важливим інструментом у багатьох сферах — від розвідки й моніторингу територій до аграрного сектору, картографування, аварійно-рятувальних операцій та навіть комерційної доставки. У військовому секторі БПЛА стали незамінним компонентом сучасного поля бою, забезпечуючи розвідку, коригування артилерії та виконання ударних місій. Проте незалежно від сфери застосування, ефективність роботи безпілотника більшою мірою залежить від надійності каналу зв'язку, через який виконується передача команд, отримання телеметрії та координування дій у реальному часі.

Канали зв'язку, особливо у випадках використання радіоканалів для керування БПЛА, є досить вразливими до зовнішніх факторів. Найбільшу загрозу для них становлять навмисні радіоелектронні завади, які можуть призвести до зниження якості прийомного сигналу, часткової або повної втрати управління над апаратом. Існує декілька типів таких завад: широкосмугові енергетичні глушіння, вузькосмугові або частотно модульовані завади (наприклад, ЛЧМ), а також є структуровані, які імітують справжній сигнал управління і можуть бути використані для спуфінгу. У реальних умовах ці завади можуть створюватись як із землі, так і з інших літальних платформ.

Усе це створює серйозні виклики для розробників систем управління БПЛА, оскільки навіть короткочасна втрата зв'язку може спричинити критичні наслідки — втрату даних, виконання помилкових команд або аварійне приземлення. Тому питання протидії завадам — це не просто метод підвищення якості, а важлива складова загальної безпеки літального апарату і надійності всієї системи.

На протидію таким ризикам у науці є різні інженерні підходи до захисту каналів зв'язку. Найпоширенішими є: метод частотного хопінгу (FHSS), який дозволяє змінювати частоту передачі сигналу в межах певного діапазону; метод прямого розширення спектру (DSSS), при якому сигнал поширюється на ширший діапазон частот, що ускладнює його глушіння; використання помилковозахисного кодування (FEC), яке дозволяє частково відновити інформацію навіть при втраті деяких бітів; технологія LoRa (Long Range), яка завдяки використанню модуляції зі спектральним

розширенням (chirp spread spectrum) має високу стійкість до перешкод та здатна підтримувати зв’язок на великих відстанях з низькою потужністю передавача. Також застосовуються схеми з резервними каналами, просторовим рознесенням антен, та використанням SDR (програмно-визначеного радіо), яке забезпечує гнучке налаштування параметрів зв’язку.

Попри велику кількість рішень, питання їх порівняльної ефективності залишається відкритим: які методи дають найкращий результат у конкретних умовах? Які комбінації технологій забезпечують найбільшу стійкість при мінімальних ресурсах? Як завади впливають на основні параметри якості зв’язку — бітову похибку (BER), затримку, ймовірність втрати пакету? І найголовніше — як все це змоделювати і перевірити без проведення дорогих польових випробувань?

Метою цієї дипломної роботи є дослідження та аналіз ефективності різних підходів до протидії навмисним завадам у каналах зв’язку БПЛА. У рамках дослідження буде змодульовано кілька типів завад, застосовано різні методи захисту, порівняно їх між собою та зроблено висновки щодо доцільності використання тих чи інших рішень в умовах обмежених ресурсів та змінного радіоелектронного середовища.

Ця тема є актуальною не лише в умовах війни, де БПЛА почали відігравати ключову роль, а й у мирному житті, де стійкий зв’язок з безпілотником має ключове значення для безпеки польотів і точності виконання завдань. Тому, дослідження, проведене в цій роботі, має практичну та наукову цінність.

РОЗДІЛ 1
ВПЛИВ НАВМИСНИХ ЗАВАД НА КАНАЛИ ЗВ'ЯЗКУ БПЛА

У сучасних умовах активного використання БПЛА, особливого значення набуває питання забезпечення надійності та захищеності їх каналів зв'язку. Ефективна робота БПЛА неможлива без стабільного інформаційного обміну з наземною станцією управління, що здійснюється через безпроводові радіоканали. Саме ці канали є найбільш уразливими елементами в умовах впливу радіоелектронної боротьби, зокрема при використанні навмисних завад.

Навмисні завади — це сигнали, що створюються з метою перешкодити нормальному функціонуванню каналів зв'язку БПЛА. Їх дія може мати як енергетичний, так і інформаційний характер: від банального "глушіння" до складних форм структурованого втручання у протоколи управління. Подібний вплив може спричинити порушення передачі команд, втрату зв'язку з апаратом, зниження точності навігації, або навіть повне перехоплення контролю над літальним засобом.

У наукових дослідженнях відзначається зростання частоти застосування навмисних завад у збройних конфліктах . Автори підкреслюють необхідність адаптивного конструювання систем управління БПЛА з урахуванням динамічної завадової обстановки. Застосування резервних частотних каналів, програмно-визначених радіомодулів (SDR), методів спектрального розширення та кодів виправлення помилок визначено як базові напрями інженерного захисту [1].

Цей розділ присвячено комплексному аналізу структури системи зв'язку малогабаритних БПЛА, класифікації типів навмисних завад, їхньому фізичному та інформаційному впливу, а також характеристикам деградації каналу зв'язку за наявності ворожих перешкод. Особливу увагу буде приділено моделюванню дії завад на різні типи модуляцій і протоколів, що використовуються в системах зв'язку БПЛА, з урахуванням практичних параметрів, характерних для типових польових сценаріїв.

1.1.1 Загальні принципи побудови систем зв’язку БПЛА

Система зв’язку є функціональною основою управління безпілотним літальним апаратом (БПЛА), оскільки забезпечує канал передачі даних між наземним оператором та бортовими обчислювальними системами апарата. Призначення такої системи — підтримувати стійкий двосторонній обмін інформацією, включаючи керуючі команди (uplink) та телеметричні, діагностичні або навігаційні дані (downlink). Це особливо важливо в умовах обмеженої автономності малогабаритних БПЛА, які не здатні повністю функціонувати в ізольованому режимі без централізованого контролю.

З інженерної точки зору, система зв’язку повинна задовольняти кілька ключових вимог: забезпечення безперервного сеансу зв’язку в реальному часі, стійкість до радіоелектронних перешкод, адаптивність до змінних умов середовища, мінімізація затримки передачі та енергоефективність у випадках обмеженого бортового живлення. У роботі [2] підкреслюється, що навіть тимчасовий обрив або спотворення керуючого сигналу можуть призвести до втрати контролю над апаратом, що є критичним у бойових або аварійних сценаріях.

Типова архітектура системи зв’язку включає (рис. 1.1):

- Бортовий передавач-приймач (трансивер) — модуль, що формує і приймає сигнали, керує модуляцією, синхронізацією та частотним спектром;
- Антену з фіксованою або направленою діаграмою випромінювання — для стабілізації рівня сигналу в умовах маневрування БПЛА;
- Наземну станцію управління (GCS) — що включає радіомодуль з посилювачами, інтерфейси введення/виведення (клавіатури, джойстики, екрани), а також блок програмного аналізу сигналу та протоколів обміну;
- Канал зв’язку — який може бути побудований у вигляді прямого радіоканалу (LoS), або з використанням ретрансляторів і супутників (BLoS) — останнє більш характерне для середніх та великих апаратів.

Визначено [3], структура цифрової системи зв’язку, незалежно від типу носія, має включати блоки модуляції, підсилення, передачі по фізичному каналу, демодуляції, виявлення та виправлення помилок. Особливістю систем БПЛА є

необхідність забезпечення високої стійкості до короткочасних переривань або змін у спектрі, що викликаються рухом апарата, завадовою обстановкою або впливом навмисних перешкод.

Крім апаратної архітектури, важливу роль відіграє інформаційна логіка обміну. Протоколи, такі як MAVLink, не лише визначають структуру пакетів даних, але й підтримують контроль помилок, перевірку CRC, індикацію втрат пакетів і роботу з кількома каналами одночасно. Проте, як зазначено у [3], класичні протоколи без криптографічних механізмів залишаються вразливими до структурованих завад (спуфінг, інжекція даних), що підкреслює актуальність розробки нових архітектур із вбудованим захистом.

Незалежно від вибраної моделі — централізованої чи розподіленої — ефективна система зв’язку для БПЛА має ґрунтуватися на модульному принципі, що забезпечує масштабованість, можливість модернізації, а також гнучке налаштування під конкретну місію. У складній радіоелектронній обстановці та в умовах змінної геометрії простору (при маневрах або зміні висоти) саме здатність адаптуватися в режимі реального часу стає вирішальною.

Взаємодія апарата з наземною станцією:

Фізична та логічна взаємодія між безпілотним літальним апаратом (БПЛА) та наземною станцією управління (Ground Control Station — GCS) є основою системи керування польотом. Цей процес передбачає безперервний обмін даними, який відбувається в обох напрямках — uplink (від GCS до БПЛА) та downlink (від БПЛА до GCS). Uplink використовується для передачі команд, зміни місії або відправлення сигналів аварійного зупинення, тоді як downlink забезпечує отримання телеметрії, діагностичної інформації та, за необхідності, відеопотоку або даних сенсорів.

Наземна станція, як правило, містить (рис. 1.1):

- потужний радіомодуль для зв’язку в обраному частотному діапазоні;
- антенну систему, що забезпечує просторове покриття або слідкує за апаратом (tracking);
- пульт управління (апаратний або програмний інтерфейс);
- обчислювальний модуль для обробки сигналів і пакетів даних, а також взаємодії з програмним забезпеченням (наприклад, Mission Planner, QGroundControl).

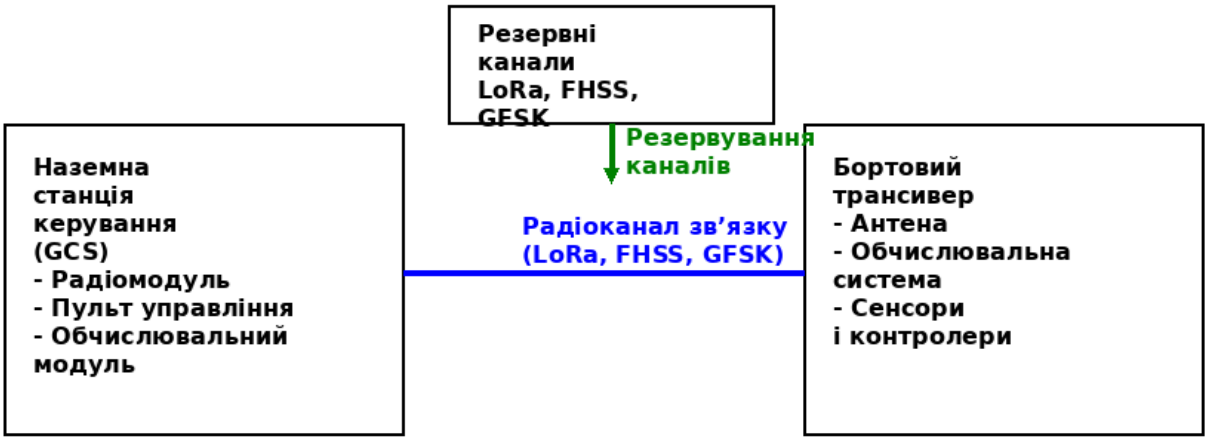


Рис. 1.1 Блок-схема системи зв'язку БПЛА з базовою станцією управління

Згідно з [1], на практиці використовується архітектура із розділенням каналів: один канал — для телеметрії та команд, другий — для відео або коригуючих даних. Це дозволяє оптимізувати пропускну здатність та забезпечити резервування у разі часткового порушення зв'язку. У статті також вказується на важливість використання окремих фізичних або логічних каналів у різних частотних діапазонах для підвищення стійкості до завад.

Обмін пакетами між БПЛА та GCS відбувається із суворим дотриманням структури протоколу. Наприклад, у протоколі MAVLink кожен пакет містить службову інформацію (ідентифікатор, довжина, CRC), навігаційні або керуючі параметри, а також інструкції щодо повторної передачі у разі втрати з'єднання. Цикл обміну зазвичай має частоту 1–10 Гц залежно від швидкості апарата, режиму польоту та обсягу даних.

Особливої складності взаємодія набуває в умовах дії навмисних завад. Як зазначено у роботі [4], у випадках впливу структурованої завади або шумоподібного глушіння наземна станція може втратити контроль над БПЛА. Для мінімізації ризиків у таких ситуаціях реалізуються механізми виявлення втрати зв'язку, переходу в автономний режим (failsafe), а також автоматичного повернення до точки запуску (RTL — Return To Launch). Також розглядається можливість впровадження програмних механізмів "двосторонньої автентифікації" для перевірки легітимності сигналів (особливо в умовах спуфінгу).

Інший аспект — таймінг. Під час активної взаємодії із БПЛА важливим є

дотримання таймінгових вікон, коли той готовий приймати пакети керування. Затримка передачі (latency) понад 200–300 мс може призвести до неправильного виконання команд у динамічному середовищі. Для критичних застосувань (наприклад, ударні або розвідувальні апарати) затримка повинна бути в межах 50–100 мс.

У системах на базі LoRa, які застосовуються для низькошвидкісних каналів зв’язку, зв’язок з GCS відбувається в режимі періодичної синхронізації: наземна станція передає команду, після чого очікує на підтвердження протягом визначеного інтервалу. При відсутності відповіді тригериться повторна передача. Такий механізм дозволяє компенсувати втрати пакетів, але має обмеження за швидкістю оновлення та відгуку. Таким чином, взаємодія БПЛА з наземною станцією повинна будуватись з урахуванням таких принципів: забезпечення гарантованої доставки критично важливих команд; стійкість до втрат пакунків і перешкод; можливість динамічного перемикання каналів і протоколів; захист від впливу зовнішнього втручання (завад, спуфінгу, ретрансляції); підтримка адаптивного інтерфейсу для оператора або автоматичного контролера.

Основні вимоги до надійності та затримки сигналу:

Якість каналу зв’язку безпілотного літального апарата (БПЛА) визначається насамперед його надійністю та затримкою передачі сигналу. Ці два параметри є критичними для виконання польотного завдання, зокрема в режимах реального часу, коли навіть короткочасна втрата керування або інформаційна затримка може призвести до деградації керованості, несанкціонованої поведінки апарата або його аварії.

Надійність зв’язку:

Під надійністю каналу зв’язку мається на увазі здатність підтримувати безперервну передачу даних із заданою якістю упродовж усього польоту. Основними інженерними показниками, які характеризують надійність, є:

BER (Bit Error Rate) — імовірність бітової помилки на одиницю даних;

PER (Packet Error Rate) — частота втрат пакетів;

SNR (Signal-to-Noise Ratio) — співвідношення сигнал/шум у дБ;

MTBF (Mean Time Between Failures) — середній час між відмовами модуля зв’язку.

Згідно з [5], для передачі керуючих сигналів у каналах з модуляцією типу BPSK або QPSK необхідно забезпечити BER < 10^{-4}, що досягається при SNR ≥ 10–15 дБ у каналах типу AWGN. Для протоколів типу MAVLink, які використовуються в багатьох БПЛА, критичними вважаються втрати понад 5–10% пакетів на інтервалі 1–2 с, що може ініціювати аварійний сценарій (наприклад, Return-to-Launch).

Затримка передачі (latency) — це час між генерацією команди на стороні оператора та її отриманням і обробкою на борту БПЛА. Цей показник визначає реалістичність управління в режимі реального часу. Типові вимоги до затримки: для тактичного управління — ≤ 200 мс; для реактивних сценаріїв (наприклад, обльоти перешкод) — ≤ 100 мс; для FPV або відеоаналізу — бажано ≤ 50 мс.

У системах на базі LoRa latency є змінною величиною і залежить від тривалості кадру, spreading factor (SF), bandwidth (BW), а також поточних умов середовища. Наприклад, при SF = 9 та BW = 125 кГц, час передачі пакета 20 байт може становити 50–80 мс. Затримки зростають із підвищенням захисту (CR), що варто враховувати при проєктуванні каналу управління.

У статті [6] показано, що при використанні складних сценаріїв електронного впливу, таких як ЛЧМ-завади або імітаційні сигнали, затримка сигналу може зростати через повторні передачі, втрачені підтвердження (ACK) або переходи в режим очікування. Це призводить до переривання керування та автоматичного переходу апарата в режим самостійного повернення (аварійна поведінка).

Компроміс швидкість–надійність

Існує прямий інженерний компроміс між швидкістю передачі та надійністю. Застосування складних кодувань (наприклад, FEC), повторної передачі (ARQ), а також спектрального розширення зменшує пропускну здатність, але підвищує стійкість. Тому на практиці система зв’язку повинна динамічно балансувати між мінімізацією затримки і забезпеченням заданого рівня BER.

Сучасні програмно-визначені радіосистеми (SDR) дозволяють у реальному часі змінювати параметри модуляції, частотного плану, ширини каналу та рівня шифрування залежно від поточної якості зв’язку. Це дає можливість реалізовувати адаптивні системи управління затримками (Delay-Aware UAV Control), як описано в [6].

1.1.2 Функціональні елементи системи зв’язку

Радіомодуль є центральним елементом системи зв’язку БПЛА, що виконує функції генерації, передавання, приймання та обробки радіосигналу. У структурі малогабаритного БПЛА він поєднує апаратно-програмні компоненти, які забезпечують повноцінну взаємодію з фізичним каналом передачі та протоколом верхнього рівня.

Типовий радіомодуль включає такі основні складові (рис. 1.2):

- Передавач (TX) — формує та модуляє сигнал відповідно до обраної схеми (наприклад, BFSK, GMSK, LoRa CSS), підсилює його до необхідного рівня потужності (зазвичай до 100–500 мВт для малогабаритних БПЛА), після чого подає на антену.
- Приймач (RX) — приймає сигнал з антени, виконує його фільтрацію, демодуляцію, синхронізацію та декодування. В сучасних рішеннях реалізуються вузькосмугові та широкосмугові приймачі з автоматичним контролем підсилення (AGC).
- Контролер/процесор — керує процесами модуляції, кодування, часової координації, обробки протоколу та взаємодіє з автопілотом чи головною обчислювальною системою БПЛА. У більшості випадків це мікроконтролер або SoC з інтегрованим DSP (Digital Signal Processor).

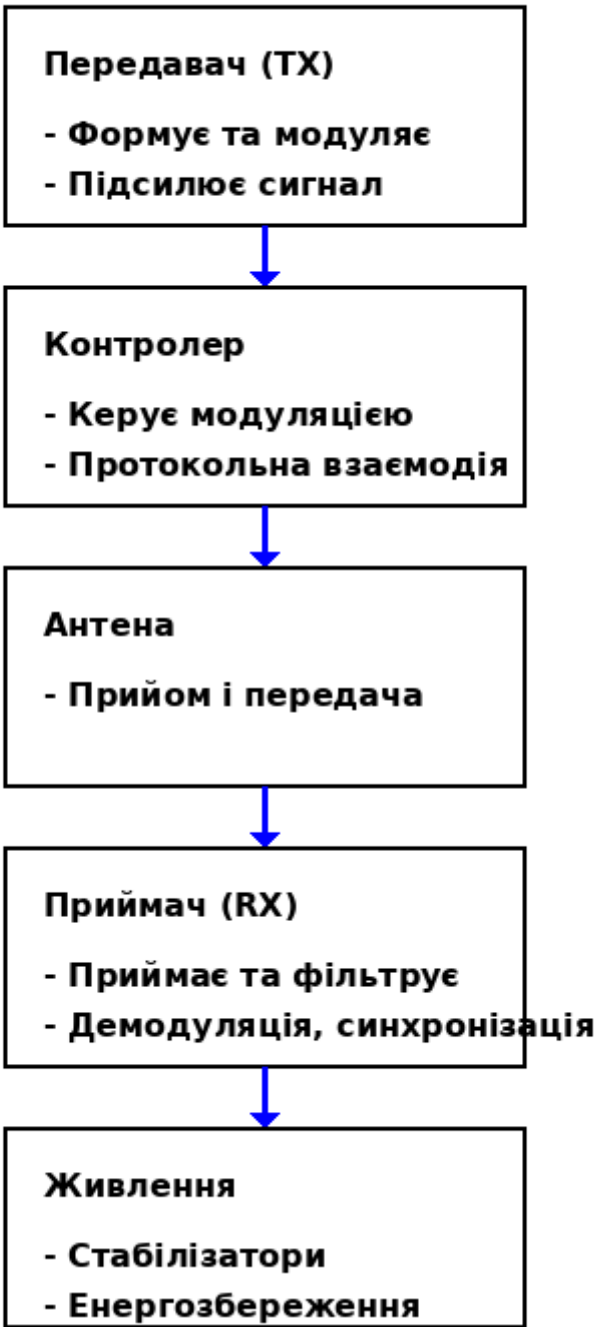


Рис. 1.2 Блок-схема радіомодуля безпілотного літального апарата

Ефективність радіомодуля визначається не тільки потужністю сигналу, а й адаптивністю до радіочастотного середовища. SDR-рішення дозволяють змінювати модуляцію, частоти та протоколи без апаратних змін, що критично в умовах РЕБ [6]. Для БПЛА з обмеженим енергобюджетом застосовується режим duty cycle, що знижує споживання енергії при мінімальних затримках.

Обмін даними в системах на базі LoRa здійснюється з урахуванням сумісності з популярними протоколами та апаратними платформами, такими як ArduPilot і PX4. Технологія LoRa забезпечує високу завадостійкість завдяки модуляції chirp spread

spectrum (CSS), що ефективно протистоїть інтерференції та шуму навіть у складних радіочастотних середовищах. Згідно з [7], методи спектрального розширення, такі як FHSS та DSSS, можуть доповнювати LoRa, підвищуючи надійність зв’язку.

Щодо антенної системи, LoRa-модулі зазвичай використовують компактні всеспрямовані антени, які забезпечують маневреність і стабільність зв’язку в різних умовах. Відповідно до [8] для специфічних завдань застосовуються також спрямовані антени, що дозволяють підвищити дальність і якість сигналу. Важливим є належне узгодження імпедансу антен та мінімізація втрат у кабелях для забезпечення оптимальної роботи системи .

Живлення здійснюється від Li-Po батарей (7.4–14.8 В) через стабілізатори. LoRa/RFD-модулі споживають до 500 мА, тому потребують окрему лінію живлення з LC-фільтрами для захисту від імпульсних завад. Схема включає порт живлення, сигнальні лінії (TX, RX, GND), керування режимами (active/sleep).

За роботою [4], при використанні LoRa з FEC критичною є стабільність живлення ±0.1 В — порушення викликає зростання помилок. У польових умовах це часта причина нестабільної роботи.

1.1.3 Використовувані частотні діапазони

У системах зв’язку БПЛА застосовуються різні частотні діапазони залежно від призначення апарата, вимог до дальності, потужності передавача та завадової обстановки. Для малих БПЛА найчастіше використовують неліцензовані ISM-смуги, для військових і спеціалізованих — виділені частоти.

ISM-смуги (433, 868, 915 МГц) — дозволені без ліцензії, широко застосовуються у цивільних апаратах. 433 МГц — популярна в Європі, має хорошу проникність, але схильна до завад від інших пристроїв (сигналізацій, медобладнання). 868 МГц — оптимальна для LoRa, забезпечує збалансоване покриття та швидкість. 915 МГц — використовується в США та Латинській Америці, має трохи вищу пропускну здатність, але гірше проходить крізь рослинність.

Ці смуги часто використовують з модуляціями FSK, GFSK, LoRa CSS, дозволяючи досягати дальності до 10–20 км у прямій видимості при потужності до 100 мВт. У [7] зазначено, що LoRa в діапазонах 868/915 МГц забезпечує найкращу

завадостійкість у класі енергообмежених систем завдяки широкому спектру, низькому енергоспоживанню та гнучким налаштуванням SF, BW і CR.

Військові частоти: L, UHF, SHF. L-діапазон (1–2 ГГц) — застосовується в GPS і супутникових каналах; має гарну стійкість до атмосферних впливів. UHF (300–1000 МГц) — дає змогу підтримувати довгий зв’язок при низькій потужності, але вразливий до міських завад. SHF (3–30 ГГц) — забезпечує високу пропускну здатність (наприклад, для відео), але вимагає спрямованих антен і LoS-зв’язку.

Як зазначено в [1], стратегія поєднання L-діапазону з резервом у UHF дозволяє підтримувати зв’язок навіть при пригніченні основного каналу. Частотне рознесення і логічне розділення потоків ускладнює ефективність впливу завад на систему загалом.

1.1.4 Методи модуляції та кодування

Методи модуляції та кодування відіграють ключову роль у системах зв’язку БПЛА, визначаючи ефективність передачі сигналу в умовах завад, обмеженої потужності та змінного середовища. Вони мають забезпечувати баланс між пропускною здатністю, надійністю та завадостійкістю.

BFSK (Binary Frequency Shift Keying) — передає “0” і “1” різними частотами. Проста в реалізації, працює за низького шуму, але має низьку спектральну ефективність.

GMSK (Gaussian Minimum Shift Keying) — покращена FSK з фільтрацією, що зменшує ширину спектру. Використовується в GSM, LoRaWAN. Енергоефективна, із середньою завадостійкістю.

QPSK (Quadrature Phase Shift Keying) — фазова модуляція з чотирма станами, забезпечує більшу швидкість, проте чутлива до фазових спотворень.

FEC (Forward Error Correction) — дозволяє виправляти помилки без повторної передачі. Застосовується у вигляді згорткових, блокових кодів, LDPC, Hamming. У БПЛА FEC підвищує надійність у зашумлених каналах, особливо в поєднанні з LoRa (CR = 4/5...4/8). Оптимізація CR залежно від умов дозволяє регулювати рівень захисту [6].

DSSS (Direct Sequence Spread Spectrum) — множить сигнал на псевдовипадкову

послідовність (PN-код), розширюючи спектр і знижуючи ймовірність перешкод та перехоплення. Ефективний проти вузькосмугових завад, використовується в LoRa CSS, 802.11b.

FHSS (Frequency Hopping Spread Spectrum) — здійснює передачу стрибками по частотах із певною швидкістю (hop rate). Має високу стійкість до вузькосмугового глушіння, забезпечує секретність. За [1], особливо ефективний у динамічному завадовому середовищі.

LoRa (CSS) — використовує chirp-імпульси. Має високу завадостійкість, працює при SNR до –20 дБ, споживає мало енергії при швидкості до 50 кбіт/с.

1.1.5 Протоколи передачі даних

Протокол передачі даних — логічна надбудова системи зв'язку БПЛА, що визначає формат повідомлень, обмін, контроль помилок і засоби захисту. Він критично важливий для надійності та безпеки командного каналу.

MAVLink (Micro Air Vehicle Link) — один з найпоширеніших протоколів, підтримується автопілотами (ArduPilot, PX4) і наземними станціями (Mission Planner, QGroundControl). Має бінарну структуру, CRC, контроль втрат, підтримує передачу телеметрії, команд, навігації. Оптимізований для вузькосмугових каналів (LoRa, FSK).

Недолік — відсутність криптографії за замовчуванням, що робить MAVLink вразливим до атак типу спуфінг, replay та ін'єкцій [3].

UAVCAN — протокол реального часу для взаємодії між електронними блоками (на основі CAN-шини або Ethernet). Працює за моделлю publish/subscribe, підтримує автоматичну маршрутизацію, оновлення конфігурацій у польоті та fault-tolerant топології. Застосовується для внутрішньої комунікації, не є основним каналом зв'язку з наземною станцією.

Пропрієтарні протоколи (DJI, Autel, Yuneec) — закриті, часто мають вбудовані механізми шифрування й автентифікації. Вони краще захищені від впливу завад, але обмежують інтеграцію з іншими платформами.

Захист інформації: шифрування (AES-128/256) — захищає канал від прослуховування. автентифікація — перевіряє легітимність відправника (ID, HMAC,

сертифікати); цифрові підписи — гарантують цілісність повідомлень (RSA, ECC, ECDSA); MAVLink підтримує підпис через SIGNING-розширення [1].

1.1.6 Особливості енергозабезпечення та енергоефективності

Енергоспоживання системи зв'язку у малогабаритних БПЛА є критичним, оскільки обмежений запас живлення впливає на тривалість польоту, стабільність роботи та надійність. Тому сучасні рішення орієнтовані на мінімізацію витрат енергії шляхом використання енергозберігаючих режимів і адаптивного керування.

Режими роботи радіомодулів: active — обмін даними в реальному часі; standby — мінімальне споживання з готовністю до пробудження; sleep — найнижче споживання, пробудження по таймеру або події.

Наприклад, у модулях LoRa (RFM95/96) споживання в активному режимі сягає ~120 мА, тоді як у sleep – лише 1–2 мкА, що дозволяє суттєво подовжити автономну роботу при періодичній передачі.

Адаптивна частота оновлення:

Частота передачі пакетів телеметрії або команд може змінюватися динамічно, залежно від фази польоту, стану батареї або зовнішніх умов. У спокійному режимі достатньо 1 оновлення за 2–5 сек, а при маневрах — до 5–10 разів на сек. Така технологія, як adaptive update rate, реалізована в багатьох відкритих автопілотах.

Згідно з [3], адаптивне оновлення у поєднанні з duty-cycling дозволяє зменшити середнє споживання на 30–40% порівняно з фіксованою частотою.

Інші засоби економії: типу модуляції/кодування (вищий CR у LoRa — більше енергії); протоколу передачі (наприклад, MAVLink дозволяє налаштувати інтервал кожного типу повідомлення); потужності передавача — зниження до мінімально потрібного рівня (Dynamic Output Power).

Наприклад, при RSSI > –80 dBm передавач може зменшити потужність на 25–50% без втрати якості зв'язку.

1.2.1. Типи навмисних завад, що впливають на канали зв’язку БПЛА

У процесі виконання завдань у складних або бойових умовах безпілотні літальні апарати дедалі частіше стають об’єктами цілеспрямованих радіоелектронних атак. Основна мета таких впливів — порушити або повністю зруйнувати канал зв’язку між апаратом та оператором, що може призвести до втрати управління, перехоплення, активації аварійних режимів або навіть повної втрати БПЛА.

Навмисні завади класифікуються за характером сигналу, способом реалізації, рівнем впливу на інформаційне наповнення сигналу, а також технічною складністю. Одним із найпоширеніших і найпростіших типів є енергетичні завади. Вони базуються на подачі на вхід приймача потужного сигналу, що накладається на корисний або значно перевищує його рівень. Таке перевантаження приймального тракту знижує відношення сигнал/шум (SNR), унеможливлює коректне декодування, викликає зростання ймовірності помилок BER і часто спричиняє перехід у аварійні режими, зокрема RTL (Return-to-Launch). Згідно з [1], подібні завади можуть бути реалізовані у вигляді широкосмугового білого шуму (broadband jamming) або вузькосмугової прицільної атаки, що накладається на робочу частоту БПЛА. Системи зв’язку на базі BFSK чи GFSK є особливо вразливими до таких впливів, тоді як технології спектрального розширення, як-от DSSS або LoRa CSS, демонструють вищу стійкість навіть при зниженому SNR до –10 дБ.

Окрему категорію становлять завади, що маскуються під легітимні сигнали — зокрема, лінійно-частотно модульовані (ЛЧМ) завади. Їхній сигнал має спектральну схожість із chirp-модуляціями, як у LoRa CSS, що ускладнює розпізнавання за традиційними критеріями. У роботі [7] підкреслено, що такі завади є особливо небезпечними для систем із CSS-модуляцією через перекриття спектра та порушення етапу синхронізації з preamble-послідовністю. ЛЧМ-завади зазвичай не потребують високої потужності, але мають високу ефективність завдяки точному налаштуванню частотного профілю атаки. Навіть часткове порушення синхронізації може суттєво знизити ефективність вбудованих засобів корекції помилок (FEC), що веде до збільшення втрат зв’язку.

Ще більш складним видом впливу є структуровані або імітаційні завади, які імітують структуру легітимного протоколу, але містять неправдиві або шкідливі дані.

Такі атаки націлені на обман системи прийому та можуть викликати виконання фальшивих команд або передачу хибної телеметрії. Наприклад, спуфінг-атака може спричинити примусове повернення БПЛА на базу шляхом підміни інформації про стан батареї. Як зазначено в [3], уразливість відкритих протоколів, таких як MAVLink, без верифікації джерела й підпису пакета, робить такі атаки надзвичайно небезпечними. Структуровані завади часто поєднують методи replay (ретрансляція відкладених пакетів) та ін'єкції (вставка легітимних на вигляд, але шкідливих повідомлень).

Імпульсні та шумоподібні завади становлять ще один критичний тип впливу. Імпульсні завади генерують короткі, але потужні сигнали, що можуть викликати локальні перевантаження та десинхронізацію. Шумоподібні ж створюють псевдовипадковий широкий спектр, подібний до білого або рожевого шуму, що призводить до блокування одразу кількох частотних каналів. У дослідженні [4] відзначається, що такі типи завад характерні для міських середовищ або зон масованої РЕБ-активності. Їх дія може викликати спотворення синхронізації кадрів, підвищення BER, короткочасні обриви з виглядом «пульсуючого» сигналу та збої в роботі FEC-кодування.

Таким чином, навмисні завади можуть мати різну природу та механізм дії, однак їхня спільна мета — порушити зв'язок і знизити ефективність функціонування систем керування БПЛА. Розуміння класифікації, принципів дії та уразливих місць дозволяє краще адаптувати захисні засоби та підвищити живучість каналу зв'язку.

1.2.2 Енергетичні завади (білий шум)

Принцип дії енергетичних завад полягає в пригніченні корисного сигналу шляхом подачі на приймач потужного шумового сигналу. Найтиповішим є білий шум — сигнал з рівномірним спектром у межах робочої смуги, що різко знижує відношення сигнал/шум (SNR) до рівня, за якого декодування стає неможливим.

Широкосмуговий шум накладається на всю смугу прийому, а вузькосмугова завада — лише на робочу частоту зв'язку, що дозволяє досягти високої ефективності з меншими енергозатратами. Як показано в [5], при зменшенні SNR нижче критичних значень BER зростає експоненційно. Пригнічення сигналу до рівня –5 дБ SNR вже

достатньо для порушення передавання команд у LoRa-системах, що може спричинити помилкову активацію аварійних режимів, порушення телеметрії або перехід апарата в failsafe.

1.2.3 Лінійно-частотно модульовані (ЛЧМ) завади

ЛЧМ-завади (chirp jamming) створюють сигнал, спектр якого лінійно змінюється в часі, що нагадує сигнали з chirp spread spectrum — зокрема, ті, що використовуються в LoRa. Такий сигнал має широкий спектр із низькою щільністю потужності, який сканує частотну смугу, і саме ця особливість дозволяє йому ефективно впливати на chirp-системи.

Через подібність до корисного сигналу, ЛЧМ-завади можуть частково проходити preamble-синхронізацію та викликати псевдодекодування. У роботі [4] зазначається, що без автентифікації LoRa-приймач не може самостійно розрізнити заваду та справжній сигнал, якщо форма chirp-профілю співпадає. Це створює критичну вразливість у бойових умовах.

У LoRa, на відміну від DSSS, spreading factor є фіксованим, тому ЛЧМ-сигнал з відповідним SF може викликати помилкове розпізнавання пакета або навіть його прийом як валідного.

1.2.4 Імітаційні (структуровані) завади

Імітаційні завади базуються на передачі сигналів, що імітують справжні команди протоколу, зокрема MAVLink. Зловмисник може сформувати пакет із коректними CRC та ID, але зміненими координатами чи командами. Особливо небезпечними є атаки з повтором (replay), які дублюють раніше перехоплену легітимну команду [3].

Спуфінг передбачає підміну сигналу хибним, а ретрансляція — повтор справжнього пакета з метою викликати запізнілу реакцію БПЛА. У системах без шифрування та часових міток такі атаки складно відрізнити від справжніх передач. Ключовим засобом захисту є автентифікація на рівні протоколу. Відсутність криптографічної перевірки, як у базовій реалізації MAVLink, створює критичну

вразливість.

1.2.5 Імпульсні та шумоподібні завади

Імпульсні завади — це короткі сигнали з високою піковою амплітудою, які можуть перевантажити вхідний каскад приймача, особливо за відсутності обмежувачів або АРУ. Як зазначено в [4], навіть одиничний імпульс тривалістю менше 1 мкс здатен порушити демодуляцію кількох бітів, спричиняючи помилки навіть у кодованому потоці.

Імпульсні та шумоподібні завади можуть зірвати фазову або часову синхронізацію, що критично для систем з FSK або PSK. Помилка фазового локатора призводить до каскадних помилок у наступних символах.

Подібні завади не впливають на середній рівень SNR, але викликають локальні BER-сплески. Це ускладнює корекцію помилок, оскільки FEC не завжди справляється з раптовими сплесками, які руйнують цілі пакети.

1.3 Характеристики впливу завад на канали зв’язку

З метою оцінювання ефективності системи зв’язку БПЛА в умовах дії навмисних завад застосовуються кількісні показники, що дозволяють об’єктивно аналізувати стан радіоканалу. До таких характеристик належать ймовірність помилок, затримки, втрати пакетів та стабільність передачі. Додатково, на основі моделювання та експериментальних даних, можна робити висновки про стійкість конкретних модуляцій або технологій до певного типу завад.

1.3.1 Критерії оцінювання якості зв’язку

Оцінка якості зв’язку в системах БПЛА базується на низці технічних показників.

BER (Bit Error Rate) — базовий критерій, що відображає імовірність бітової помилки при передачі.

PER (Packet Error Rate) — частка пошкоджених пакетів, що особливо важливо

для керуючих каналів.

SNR (Signal-to-Noise Ratio) — співвідношення потужності сигналу до шуму, зазвичай пороговим вважається рівень SNR ≥ 10–15 дБ для цифрових модуляцій.

Згідно з [5], при зниженні SNR нижче критичного рівня BER зростає нелінійно. Наприклад, для QPSK поріг становить ~9–10 дБ, тоді як LoRa здатна функціонувати при SNR до –20 дБ залежно від spreading factor (SF).

Затримка передачі є критичною для стабільного керування — вона не повинна перевищувати 100–200 мс. Завади можуть спричинити зростання затримки через повторні передачі та десинхронізацію.

Втрати пакетів часто є наслідком поганого SNR або впливу структурованих чи ЛЧМ-завад.

Частота повторних передач зростає у разі деградації каналу — частота >30% може викликати збої в роботі автопілота [4].

1.3.2 Результати моделювання впливу завад

У [7] подано результати моделювання BER для різних модуляцій у присутності білого шуму. FSK демонструє BER > 10^{-2} при SNR < 8 дБ. Для LoRa з SF9 при SNR = 0 дБ — BER ≈ 10^{-3}, а при –6 дБ — вже >10^{-1}, що свідчить про різку втрату зв’язку.

Це підтверджує уразливість FSK-систем до енергетичного глушіння та кращу стійкість LoRa завдяки CSS-модуляції і FEC. LoRa є менш чутливою до білого шуму, але вразливою до ЛЧМ-завад

1.3.3 Залежність від типу модуляції

BFSK/GFSK мають помірну стійкість і низьку спектральну ефективність. Вони чутливі до вузькосмугових або тональних завад, зокрема при SNR < 8–10 дБ [5]. Часто використовуються в простих модулях (XBee, 3DR), однак у бойових умовах їх ефективність обмежена.

LoRa (CSS) — одна з найстійкіших до завад технологій. Завдяки широкому спектру chirp-сигналу та високому spreading factor (7–12), LoRa може працювати при дуже низькому SNR (до –20 дБ) [7]. Її додатковими перевагами є адаптивне налаштування coding rate (CR) та вбудований FEC. Водночас, LoRa є вразливою до спектрально подібних ЛЧМ-завад, які можуть викликати хибне декодування при збігу

SF.

DSSS забезпечує стійкість до вузькосмугових завад завдяки псевдовипадковому розширенню спектру.

FHSS змінює частоту передачі з певною періодичністю (hop rate), що дозволяє уникати довготривалого впливу на одну частоту. Обидві технології потребують синхронізації між передавачем і приймачем, але забезпечують високу живучість у зашумленому середовищі.

1.3.3 Невиявлені загрози: логічні атаки

Окрім фізичних завад, існують логічні загрози, які не впливають на SNR або BER, але спричиняють функціональні збої.

Кібератаки можуть реалізовуватися шляхом надсилання структурно правильного пакета з хибним вмістом — наприклад, команду аварійного вимкнення. Такий пакет проходить перевірку CRC, хоча функціонально є атакою.

Як зазначено в [3], відсутність автентифікації у відкритих протоколах, таких як MAVLink або NMEA, дозволяє зловмиснику надіслати хибну команду, що буде сприйнята як легітимна.

CRC лише перевіряє цілісність, але не гарантує достовірність джерела. Протокол MAVLink підтримує розширення SIGNING, але воно часто не активоване за замовчуванням.

Висновки:

У результаті аналізу, проведеного в межах першого розділу, можна сформулювати ряд ключових висновків щодо структури систем зв’язку малогабаритних безпілотних літальних апаратів (БПЛА), їх вразливостей, а також характеру впливу різних типів навмисних завад.

Система зв’язку БПЛА є багаторівневою архітектурною конструкцією, до складу якої входять апаратні елементи (радіомодуль, антена, енергоживлення), протоколи обміну (наприклад, MAVLink, UAVCAN) та програмно-керовані алгоритми модуляції, синхронізації та передачі даних. Усі ці компоненти

функціонують у межах обмеженого енергетичного бюджету, що визначає необхідність високої енергоефективності та адаптивності.

Найбільш поширені частотні діапазони — ISM-смуги (433, 868, 915 МГц) — доступні, проте вразливі до впливу сторонніх сигналів. Військові системи додатково використовують захищені частоти L/UHF/SHF, які дозволяють гнучко управляти спектром і впроваджувати заходи захисту.

Вивчення типів завад показало, що кожна категорія має специфічний механізм впливу: енергетичні завади знижують SNR та призводять до порушення декодування; ЛЧМ-завади здатні імітувати сигнал LoRa і порушувати процедури синхронізації; структуровані завади небезпечні тим, що передають формально коректні пакети; імпульсні та шумоподібні завади викликають дестабілізацію приймача через надкороткі сигнали або спектральне перекриття.

Найбільш вразливими до фізичних завад виявилися модуляції типу BFSK і GFSK, тоді як LoRa та DSSS/FHSS демонструють підвищену стійкість за рахунок спектрального розширення та алгоритмів FEC. Однак навіть ці технології залишаються уразливими до інформаційних (логічних) атак, які не супроводжуються підвищенням BER або зниженням SNR, але призводять до хибного виконання команд.

Таким чином, захист каналів зв’язку БПЛА потребує не лише апаратного чи спектрального резервування, а й глибокої протокольної безпеки, включаючи автентифікацію, шифрування, цифрові підписи та моніторинг аномальної активності.

РОЗДІЛ 2
МЕТОДИ ПРОТИДІЇ ВПЛИВУ НАВМИСНИХ ЗАВАД НА КАНАЛИ ЗВ'ЯЗКУ БПЛА

Забезпечення стійкості каналів зв'язку безпілотних літальних апаратів (БПЛА) до навмисних завад — одне з ключових завдань у побудові сучасних систем управління. В умовах активного застосування засобів радіоелектронної боротьби (РЕБ), традиційні бездротові канали (особливо ті, що функціонують у відкритих ISM-діапазонах) стають об'єктом цілеспрямованого пригнічення, що може призвести до втрати керування, дезорієнтації або знищення апарата.

Цей розділ присвячено системному аналізу існуючих та перспективних методів протидії впливу навмисних завад, класифікованих у попередньому розділі. Для кожного з типів завад (енергетичних, ЛЧМ, імітаційних та імпульсних) буде розглянуто: принципи побудови захищених каналів управління; технологічні засоби пом'якшення впливу; криптографічні та протокольні механізми виявлення та фільтрації загроз; апаратні рішення (резервування, спектральна адаптація, SDR).

Окрему увагу буде приділено застосуванню технології LoRa як потенційно завадостійкого каналу управління, що поєднує у собі переваги спектрального розширення, коригувального кодування та енергетичної ефективності.

Ключовим аналітичним завданням цього розділу є формування висновків щодо ефективності конкретних методів протидії енергетичним завадам (jamming attack) при використанні різних типів сигналів у каналах зв'язку БПЛА. Зокрема, буде досліджено, які саме модуляції (BFSK, QPSK, LoRa CSS, DSSS) демонструють стійкість до глушіння, та які технічні й алгоритмічні заходи дозволяють зменшити ймовірність втрати керування.

2.1.1 Вимоги до завадостійкого каналу управління

У сучасних умовах високого рівня електромагнітних загроз для БПЛА особливого значення набуває створення стабільного, завадостійкого каналу управління. Його порушення може призвести до втрати контролю, перехоплення або знищення апарата. Тому канал має відповідати низці вимог: спектральна та

енергетична стійкість, протокольна безпека, динамічна адаптивність.

Найважливішим параметром є працездатність у середовищі з низьким SNR. Якщо BFSK чи GFSK вимагають не менше 8–10 дБ, то технології на базі chirp spread spectrum (напр. LoRa) здатні працювати при SNR до –20 дБ, що робить їх ефективними в умовах широкосмугових завад.

Канал повинен підтримувати адаптивне керування параметрами передачі (модуляція, ширина смуги, потужність, швидкість), щоб обходити частоти, де діють фіксовані перешкоди. Актуальними є рішення з динамічною зміною spreading factor, coding rate та частоти передачі, орієнтовані на рівень сигналу або виявлення завад.

Надійність каналу також забезпечується механізмами контролю та виправлення помилок: FEC, CRC, повторні передачі. Однак структуровані завади можуть обходити ці засоби, тому необхідна автентифікація та перевірка повноважень команд на протокольному рівні — особливо для критичних сигналів.

Фізична живучість підвищується завдяки резервуванню: частотному (рознесення основної та резервної частоти), апаратному (подвійні радіомодулі) або логічному (паралельні протоколи). У разі втрати основного каналу система повинна автоматично переключатись без затримки управління.

2.1.2 Архітектура з рознесенням частот, резервуванням каналів та виявленням завад

Забезпечення стабільного зв’язку БПЛА в умовах навмисних завад потребує впровадження багаторівневої архітектури з акцентом на живучість радіоканалу. Один з ключових елементів — частотне рознесення та резервування каналів, що дозволяє автоматично змінювати частоту або перемикатися на альтернативні засоби зв’язку при погіршенні якості основного тракту.

Частотне рознесення передбачає використання різних діапазонів для основного і резервного каналів, що знижує ризик впливу вузькосмугових завад. Наприклад, (рис 2.1) основний канал може працювати в діапазоні 868 МГц (LoRa), тоді як резервний — через 4G/LTE або UHF із GMSK-модуляцією. Це забезпечує базову стійкість до глушіння, особливо в військових сценаріях.

Резервування реалізується також на рівні модуляцій і протоколів:

високошвидкісний основний канал може доповнюватися вузькосмуговим енергоефективним резервом, який передає лише критичні команди (RTL, HOLD тощо). Незважаючи на нижчу продуктивність, він забезпечує збереження керування при деградації основного каналу.

Важливим є постійний контроль параметрів зв'язку — рівня сигналу, SNR, повторних передач, нестабільності ACK. Виявлення ознак завад ініціює перемикання частот або каналів. У складніших системах рішення приймається автоматично на основі RSSI, ACK-loss або затримки відповіді.

Розширення функціоналу можливе завдяки SDR-платформам (рис. 2.1), які дозволяють змінювати частоту й модуляцію в реальному часі, проводити спектральний аналіз і виявляти типи завад (білий шум, тональний, ЛЧМ). Такі системи можуть реалізувати частотне хопінгування, адаптивну передачу та перебудову сигналу під конкретну заваду.

Додатковий рівень надійності забезпечує багатоканальне дублювання (рис 2.1), коли критична команда передається паралельно різними модуляціями та на різних частотах. Як показано в [4], комбінація LoRa та GFSK з часовим дублюванням дозволяє знизити імовірність втрати команди до $<10^{-3}$ навіть за активного глушіння.

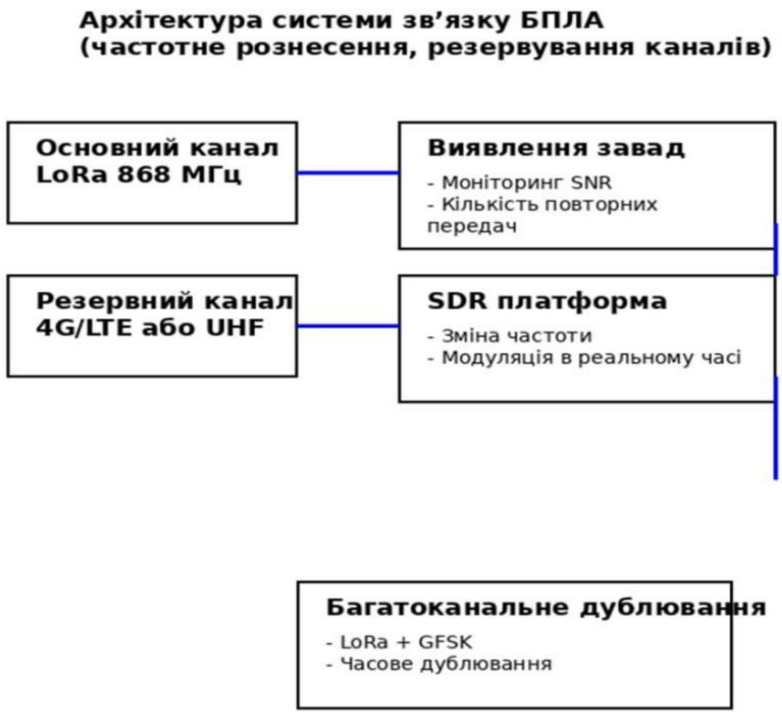


Рис. 2.1 Блок-схема системи зв'язку БПЛА з частотним рознесенням та захистом від завад

2.2 Протидія енергетичним завадам (глушінню, білому шуму)

Енергетичні завади є найпростішим і водночас дуже ефективним засобом порушення зв’язку БПЛА, особливо для малогабаритних моделей з обмеженими ресурсами. Потужний шум у робочому діапазоні може спричинити втрату синхронізації, зростання BER і неможливість стабільного управління, особливо якщо завада потрапляє у діаграму спрямованості антени або перевантажує приймач.

Крім частотного рознесення, ефективним методом захисту є динамічне регулювання параметрів зв’язку. За допомогою SDR-платформ можна змінювати частоту, модуляцію, смугу та потужність передачі в реальному часі. Зменшення потужності або перехід у вузькосмуговий режим допомагає локалізувати сигнал і зменшити ймовірність виявлення. В деяких випадках застосовується режим "мовчання" — тимчасова зупинка передачі з переходом у пасивне прослуховування прихованого резервного каналу.

Ще один напрям — використання протоколів із вбудованим переходом у автономні режими. Наприклад, автопілоти ArduPilot та PX4 у разі втрати зв’язку можуть активувати сценарії failsafe: повернення, зависання, посадка. Це дозволяє зберігати контроль навіть за умов повного глушіння.

Високу ефективність проти білого шуму демонструють технології спектрального розширення, зокрема LoRa. Завдяки низькій щільності потужності та широкому спектру, LoRa зберігає зв’язок при SNR нижче 0 дБ, тоді як BFSK або GFSK втрачають здатність до декодування в аналогічних умовах.

2.2.1 Частотне рознесення та резервні канали

Одним із найефективніших способів протидії енергетичному глушінню є застосування частотного рознесення та резервних каналів зв’язку. Оскільки енергетичні завади зазвичай охоплюють обмежену смугу частот, перенесення сигналу в інший діапазон дозволяє уникнути пригнічення всієї системи.

Частотне рознесення реалізується шляхом використання різних частот для основного та резервного каналів. Наприклад, основний канал може працювати на 868

МГц з LoRa, а резервний — на 433 МГц із BFSK або GFSK. Такий підхід підвищує стійкість системи до спрямованого глушіння, оскільки канали працюють незалежно один від одного.

Резервний канал може мати спрощений функціонал — достатньо лише підтримки базових команд, таких як RTL, HOLD або DISARM. Хоча він може поступатися у швидкості чи деталізації телеметрії, головне — забезпечити стабільний контроль у кризових ситуаціях.

Особливо ефективним є поєднання частотного рознесення з різними модуляціями. Наприклад, використання DSSS або FHSS на одному діапазоні й LoRa CSS — на іншому забезпечує не тільки фізичне розділення, а й різну завадостійкість. У таких умовах противнику значно складніше реалізувати ефективне глушіння без перевищення технічних або нормативних меж.

Перемикання між каналами здійснюється автоматично на основі показників якості зв’язку (RSSI, втрати ACK, таймаути). У простих системах діє пороговий механізм перемикання, тоді як у більш просунутих — паралельне прослуховування кількох каналів із вибором найкращого.

Практичні експерименти [6] підтверджують ефективність такого підходу: при переході з LoRa 868 МГц на GFSK 433 МГц у середовищі активного глушіння вдалося зберегти керованість БПЛА. Це доводить, що частотне резервування є обов’язковим елементом захищеної архітектури в умовах радіоелектронного протистояння.

2.2.2 Адаптивне зменшення потужності та фільтрація шуму

Зменшення потужності передачі до мінімально необхідного рівня є ефективною відповіддю на глушіння. На відміну від підвищення потужності, що привертає увагу та виснажує енергоресурси, зниження сигналу зменшує помітність каналу, енергоспоживання і спектральне навантаження.

Сучасні модулі зв’язку підтримують автоматичну адаптацію потужності залежно від рівня RSSI чи BER. Це дозволяє утримувати стабільний зв’язок при дії слабких завад без перевантаження приймача.

Фільтрація шуму також є важливим засобом боротьби з завадами. Вона реалізується як апаратно (LC- та смугові фільтри), так і програмно — через

спектральне усереднення, компенсацію імпульсів або цифрове відновлення сигналу. Це особливо ефективно в умовах побутового або промислового ЕМФ.

Додатково, при зниженні якості зв’язку система може автоматично зменшити швидкість передачі, скоротити довжину пакета або підвищити CR. Така адаптація зберігає критичні команди навіть у складному завадовому середовищі.

2.2.3 Застосування LoRa CSS для високої завадостійкості

Модуляція chirp spread spectrum, на якій базується технологія LoRa, забезпечує високу стійкість до широкосмугових та шумоподібних завад. Завдяки лінійно-частотно модульованим імпульсам із низькою щільністю енергії, LoRa здатна приймати сигнали при SNR до –20 дБ.

На відміну від FSK або PSK, LoRa синхронізується з частотною траєкторією сигналу, а не з фазою чи частотою, що дозволяє відокремлювати корисну інформацію навіть при перекритті спектра шумом. Цей механізм реалізується апаратно і не потребує значних обчислювальних ресурсів.

Гнучке налаштування параметрів — spreading factor, bandwidth, coding rate — дозволяє адаптувати канал до рівня завад. При високому SF сигнал стає довшим і стійкішим, що особливо корисно для критичних команд у складних умовах.

LoRa також ускладнює глушіння для противника, адже спектрально нестабільні chirp-сигнали потребують потужного або синхронного впливу, що є технічно складним для реалізації.

2.3 Протидія ЛЧМ-завадам (chirp-подібним)

ЛЧМ-завади є особливо небезпечними для LoRa-систем, оскільки їхня форма майже ідентична до chirp-сигналу. Це ускладнює виявлення: приймач може сприйняти заваду як легітимний preamble, що призводить до псевдосинхронізації, втрати пакета або помилкового виконання команд — особливо при збігу параметрів SF та BW.

Окрім динамічного регулювання SF, BW і CR, ефективним засобом захисту є впровадження спектрального моніторингу — аналізу структури сигналу та перевірки

автентичності preamble. У складніших варіантах застосовуються алгоритми кореляції, перевірки chirp-послідовностей і таймінгу, що дозволяє вчасно виявити спробу атаки.

Додаткові заходи включають псевдовипадкові зсуви частоти в межах одного пакета, використання розширеного preamble або швидке перемикання на резервний канал (frequency retreat), зокрема із використанням DSSS.

ЛЧМ-завади вимагають високої точності та складного устаткування, тому системи захисту можуть ефективно реагувати на них через динамічну адаптацію параметрів LoRa, аналіз спектра та перевірку автентичності, інтегровану в протоколи обміну.

2.3.1 Динамічна зміна параметрів LoRa (SF, BW, CR)

ЛЧМ-завади, що імітують chirp-сигнали, становлять серйозну загрозу для LoRa-систем, оскільки можуть накладатися не лише спектрально, але й структурно. Це призводить до псевдосинхронізації та прийому хибних пакетів.

Ефективним засобом захисту є динамічна зміна параметрів LoRa — spreading factor (SF), bandwidth (BW) і coding rate (CR). Зміна цих характеристик у реальному часі порушує передбачуваність сигналу й ускладнює підлаштування завади.

Збільшення SF подовжує chirp-імпульси та знижує вимоги до SNR, підвищуючи завадостійкість. За роботою [7], підвищення SF на один рівень може зменшити ймовірність синхронізації з завадою на 20–30%. Зменшення BW знижує спектральне перекриття, хоча й зменшує швидкість. Підвищення CR підсилює здатність до виправлення помилок, але збільшує час передачі.

Зміна параметрів може бути періодичною або адаптивною — залежно від RSSI, BER чи затримки ACK. У практиці застосовують “псевдоспектральне хопінгування” — передачу з постійно змінними параметрами, що ускладнює реалізацію ЛЧМ-завад у реальному часі. Також адаптація до умов середовища (місто/відкрита місцевість) дозволяє обирати оптимальні значення SF та BW для збереження стабільного зв’язку.

2.3.2 Виявлення спектрального накладання

Виявлення накладання ЛЧМ-завади на сигнал LoRa є критично важливим для запобігання декодуванню хибних даних і своєчасного перемикання на резервні режими. Через схожість chirp-структур традиційні показники, як-от RSSI чи SNR, можуть не виявити заваду.

Для фіксації спектрального конфлікту використовують аналіз у часо-частотній площині — STFT або вейвлет-перетворення. Ці методи дозволяють виявити сторонні частотні компоненти або зміщення, які не відповідають типовому chirp-профілю. Як показано в [1], навіть фазовий зсув кількох мкс при однаковому SF можна виявити за зміною геометрії preamble, використовуючи розширену кореляційну перевірку.

Додатково застосовують перевірку логіки сигналу — легітимні chirp-и мають послідовний частотний профіль, тоді як генератори завад часто мають спрощені чи нестабільні характеристики. У SDR-системах можливе візуальне або автоматизоване виявлення таких аномалій за допомогою аналізу спектру в реальному часі.

2.3.3 Відмінності між корисним та ворожим chirp-сигналом

Попри зовнішню подібність, сигнали LoRa мають специфічні ознаки, що дозволяють їх відрізняти від штучно сформованих ЛЧМ-завад. Це лежить в основі автоматичного виявлення маскувальних атак.

У легітимному LoRa-сигналі темп зміни частоти чітко задається spreading factor (SF). Ворожі сигнали рідко точно імітують SF, що викликає відхилення в часовому градієнті. Такі відхилення можна фіксувати через порівняння очікуваної частотної траєкторії з реальною.

Корисний сигнал також містить фіксований preamble, який виконує роль синхронізації. Ворожі сигнали часто мають фазові зсуви або неправильну довжину preamble, що значно знижує імовірність синхронізації. За роботою [7], відхилення понад 5% може зменшити її до 50%.

Ще одна відмінність — кореляційна симетрія. У LoRa chirp-профілі повторюються точно, тоді як у завадах часто спостерігаються фазові флуктуації та

нестабільність. Також легітимні сигнали мають чіткий таймінг, у той час як завади — довільні в часі. Це дозволяє високоточним приймачам виявляти неавторизовані передачі навіть при частковому перекритті спектру.

2.4 Протидія структурованим завадам (імітаційним)

Протидія структурованим завадам потребує багаторівневої перевірки повідомлень: структури, джерела, змісту та контексту. Це особливо актуально для відкритих протоколів типу MAVLink, які часто не мають вбудованої автентифікації.

Один із поширених методів атаки — ретрансляція справжніх команд. Без механізму виявлення повторів (наприклад, за допомогою nonce або сеансових лічильників) система може прийняти старий пакет як новий. У просунутих рішеннях використовуються одноразові ключі, які знищуються після першого використання.

Критичною є перевірка контексту команди — наприклад, команда на посадку поза допустимою зоною чи зміну висоти без увімкненого двигуна повинна блокуватись. Це реалізується через FSM-логіку, яка враховує не лише вміст пакета, а й параметри стану апарата (GPS, швидкість, живлення тощо).

Також система повинна відслідковувати частоту та послідовність команд. Аномальні серії ("RTL" кілька разів поспіль) або неприродна динаміка значень — ознака втручання. У таких випадках активується блокування, повідомлення оператора або аварійний режим.

У [9] підкреслюється, що навіть за надійного фізичного каналу логічний рівень безпеки є вразливим. Важливо реалізовувати протокольний аналіз прямо на автопілоті або наземній станції для фільтрації шкідливих команд.

2.4.1 Контроль цілісності команд

У захисті від структурованих завад важливо перевіряти не лише формат пакета, а й зміст переданих команд. Атаки можуть виглядати легітимно: пакет проходить CRC і відповідає протоколу (наприклад, MAVLink), але містить змінені критичні дані.

CRC дозволяє виявити випадкові помилки, але не захищає від навмисних змін — зловмисник може перерахувати CRC після підміни даних. Тому застосовують

перевірку послідовності: кожна команда має унікальний номер або тайм-мітку, що дозволяє виявити повтори (replay-атаки).

Також важливо перевіряти допустимість команди у конкретному стані системи: наприклад, “DISARM” не має виконуватись у польоті, а “RTL” — без активного GPS. Такий підхід забезпечує логічну фільтрацію навіть за умови формальної коректності пакета.

У роботі [9] вказано, що атаки часто не порушують CRC, але змінюють payload — координати, режим, швидкість. Тому ефективним є аналіз змісту на рівні автопілота або middleware, із перевіркою діапазонів, конфліктів і підозрілих змін.

Надійний рівень захисту забезпечують цифрові підписи або HMAC: при будь-якій зміні байтів перевірка не проходить, і команда блокується ще до обробки.

2.4.2 Впровадження автентифікації (ключі, цифрові підписи)

Автентифікація є основою захисту від імітаційних атак, коли зловмисник надсилає формально коректні команди від імені легітимного джерела. Щоб запобігти цьому, застосовуються HMAC, цифрові підписи та криптографічні методи перевірки джерела.

Найпоширенішим підходом у БПЛА є HMAC — обидві сторони мають спільний ключ, а до кожного пакета додається хеш-код, який перевіряється приймачем. У MAVLink 2.0 така автентифікація реалізована 13-байтним підписом, що ефективно блокує спуфінг [9]. Недолік — складність безпечного розповсюдження ключів і ризик їх втрати.

Для більш високої безпеки застосовують асиметричні підписи (наприклад, ECDSA), де передавач підписує дані приватним ключем, а приймач перевіряє — відкритим. Такий метод не потребує спільного секрету, але вимагає більших ресурсів або апаратної підтримки.

Автентифікація може бути обов’язковою лише для критичних команд (керування польотом, зміна режиму), що дозволяє зменшити навантаження на систему. У поєднанні з шифруванням (AES + HMAC) забезпечується повна захищеність і цілісність каналу.

2.4.3 Захист протоколів MAVLink/UAVCAN

MAVLink та UAVCAN — широко використовувані протоколи в БПЛА, але їх відкритість створює ризики атак, оскільки структура пакетів відома зловмисникам. Захист протоколу є не менш важливим, ніж фізична завадостійкість.

Перша версія MAVLink не мала автентифікації — всі дані передавались відкрито, що робило можливими спуфінг і replay-атаки. У версії 2.0 додано підпис повідомлень, але він не активується за замовчуванням у багатьох системах через побоювання щодо ресурсоємності.

UAVCAN також не має вбудованої автентифікації в базовій версії, що дозволяє атаки зсередини мережі при компрометації вузлів. Версія UAVCAN v1 передбачає криптозахист, але реалізація залишена на розсуд розробників.

Рекомендовані заходи:

- увімкнення підпису MAVLink 2.0 та контроль лічильників;
- використання VPN або окремого зашифрованого каналу;
- фільтрація ID на рівні автопілота та перевірка контексту команд;
- обмеження на конфігураційні зміни в польоті.

Як зазначено в [3], навіть базовий рівень автентифікації значно підвищує безпеку для критичних команд (“ARM”, “DISARM”, “LAND”). Тому захист протоколів має бути обов’язковим елементом побудови стійкої системи керування.

2.5 Захист від імпульсних та шумоподібних завад

Імпульсні та шумоподібні завади становлять серйозну загрозу для БПЛА, адже мають високу амплітуду та короткочасну дію, що ускладнює їх виявлення й нейтралізацію. Такі перешкоди можуть виникати раптово — як унаслідок природних явищ (наприклад, гроза), так і в межах активної радіоелектронної боротьби.

Для захисту використовують буферизацію, повторну передачу, фільтрацію в часовій та частотній області, а також адаптивне зменшення потужності. Ці підходи дають змогу пом’якшити вплив коротких імпульсів і зберегти стабільність каналу навіть у присутності потужних, але нестійких завад.

2.5.1 Буферизація та повторна передача

Імпульсні й шумоподібні завади можуть раптово перекривати сигнал, що призводить до втрати або спотворення даних, особливо у критичних фазах польоту. Їх джерелами можуть бути як природні (грозові розряди), так і штучні (EMI, радіоелектронна боротьба).

Основним захистом є буферизація й повторна передача. Буферизація дозволяє тимчасово зберігати дані, які не були коректно отримані, з можливістю їх повторної відправки. Це допомагає уникнути втрати критичної інформації при короткочасних збоях.

Механізм ARQ (Automatic Repeat reQuest) забезпечує автоматичне повторення пакета при виявленні помилок. У поєднанні з FEC (корекція помилок), який відновлює пошкоджені ділянки сигналу, це значно підвищує надійність зв’язку.

У LoRa реалізовано повторну передачу разом із адаптивним coding rate, що забезпечує стійкість до завад навіть при сильному ЕМ-фоні [7]. Основне обмеження такого підходу — затримка, але її знижують шляхом використання кількох каналів або резервних частот.

2.5.2 Time-domain фільтрація та розпізнавання коротких сплесків

Імпульсні завади часто мають вигляд коротких, потужних сплесків, які складно виявити спектральними методами. Вони здатні частково чи повністю зруйнувати сигнал, тому ефективним засобом захисту є фільтрація в часовій області.

Time-domain фільтрація дозволяє фіксувати аномальні імпульси, що перевищують порогові значення, та згладжувати їх вплив без погіршення якості сигналу. Для цього застосовують згладжувальні фільтри (FIR, ковзне середнє) або кореляційні вікна, які пропускають лише сигнали із заданою структурою, а також прогнозують вміст спотворених фрагментів.

Сучасні підходи включають використання машинного навчання. Нейронні мережі здатні розпізнавати й адаптивно фільтрувати навіть змінні за характеристиками імпульсні завади. Адаптивні фільтри, що налаштовуються в реальному часі, дають змогу оптимально згладжувати перешкоди, коригуючи пороги

та моделі фільтрації.

У роботі [6] зазначено, що комбінація адаптивної фільтрації та детекції аномалій забезпечує до 30–40% кращу ефективність відновлення сигналу, ніж класичні методи з фіксованими порогами.

2.5.3 Екранування та апаратна фільтрація

Екранування та фільтрація — основні методи захисту БПЛА від імпульсних і шумоподібних завад, особливо при високих рівнях EMI. Їхня мета — зменшити вплив небажаних сигналів ще до досягнення приймача, забезпечуючи стабільний зв’язок.

Екранування здійснюється за допомогою металевих або композитних матеріалів, які блокують електромагнітне випромінювання. Воно особливо ефективне для систем у діапазоні 433–915 МГц, де зовнішні завади можуть значно спотворювати сигнал. Матеріали мають поглинальні та відбивні властивості й охоплюють широкий частотний спектр.

Апаратна фільтрація включає аналогові й цифрові фільтри, які відсікають непотрібні частоти. Смугові фільтри пропускають лише потрібну частину спектра, відсікаючи низько- і високочастотні завади. Цифрові фільтри (наприклад, на основі хвильового аналізу або кореляції) можуть адаптуватись до змін сигналу й працювати в реальному часі з мінімальними затримками.

Комбінація екранування та фільтрації забезпечує надійнішу роботу систем зв’язку: екран зменшує загальний рівень завад, а фільтри точно видаляють залишкові перешкоди. Це значно підвищує завадостійкість і знижує ризик втрати керування.

Висновки:

У цьому розділі були розглянуті основні методи протидії навмисним завадам, що впливають на канали зв’язку безпілотних літальних апаратів. Розглянуті методи покликані забезпечити стабільність і надійність систем управління в умовах радіоелектронної боротьби та природних завад. Важливою складовою системи захисту є багаторівневий підхід, який включає не тільки фізичні та технічні методи, а й логічний захист на рівні протоколів та автентифікації.

Одним із основних напрямів є частотне рознесення та резервування каналів, що дозволяє зменшити ймовірність одночасного пригнічення всіх ліній передачі. Це забезпечує стійкість каналу зв’язку, навіть при активному глушінні або високому рівні перешкод.

Значну роль у забезпеченні завадостійкості відіграє динамічна зміна параметрів модуляції, зокрема SF, BW і CR, що дозволяє адаптувати канал до умов змінного радіоелектронного середовища. Адаптивне зменшення потужності та фільтрація шуму також є важливими методами, що дають змогу знижувати ефект від короткочасних перешкод і широкосмугових шумів.

Додатково, ефективний захист проти структурованих завад забезпечується через механізми контролю цілісності команд та автентифікації, що дозволяють уникнути атак на рівні протоколів, таких як спуфінг або повторні передачі. Загалом, застосування екранування, апаратної фільтрації, а також комбінація методів виявлення та усунення завад на всіх рівнях — від фізичного до протокольного — є основою для створення захищених каналів управління БПЛА.

Подальші дослідження будуть спрямовані на визначення FHSS, FEC, DSSS, LoRa методів протидії завадам: енергетична у вигляді білого шуму — широкосмугова, завада ЛЧМ в широкому діапазоні частот.

РОЗДІЛ 3

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МОТОДІВ ПРОТИДІЇ НАВМИСНИМ ЗАВАДАМ

Для дослідження впливу навмисних радіозавад на канали управління безпілотних літальних апаратів (БПЛА) обрано модель каналу на базі реального радіомодуля RFD900x. Цей модуль широко використовується в каналах управління БПЛА завдяки високій потужності, стабільності та підтримці різних методів модуляції.

Параметр	Значення
Частотний діапазон	902–928 MHz (RFD900x),
Модуляція	GFSK
Потужність передавача	До 30 dBm (1 Вт)
Чутливість приймача	До -121 dBm
Швидкість передачі	(Air Data Rate) 4.8 – 250 kbps
Інтерфейс	UART (3.3V TTL)
Напруга живлення	3.3 – 5.5 V
Споживаний струм	~100 мА прийом / до 1 А передача
Протокол	Працює на прошивці SiK

В якості завад використовувався універсальний програмно-визначуваний радіоприймач/передавач HackRF One, що дозволяє створювати широкий спектр штучних завад, включно з білошумовими та лінійно-частотно модульованими (ЛЧМ) сигналами. Модель каналу вважалась з урахуванням умов вільного простору (Free Space), що відповідає реальним польотним умовам без великих перешкод.

Характеристики:

Параметр	Значення
Діапазон частот	1 МГц – 6 ГГц
Тип роботи	Прийом і передача (half-duplex)
Модуляції	Підтримує будь-які (LoRa, ЛЧМ, тощо)
Інтерфейс	USB 2.0
Програмне забезпечення	GNU Radio, MATLAB, URH
Ширина смуги	До 20 МГц

Модель радіоканалу	Вільний простір (Free Space)

Основним напрямом дослідження було моделювання впливу двох типів завад: широкосмугового білого шуму та ЛЧМ-завад, з подальшою оцінкою показників якості зв’язку (SNR, Eb/N0, BER) і порівнянням ефективності різних методів захисту — FHSS, FEC, LoRa CSS, DSSS.

Вихідні дані для розрахунку:

Параметр	Значення
Частота f	915 МГц
Потужність передавача P_t	30 dBm = 1 Вт
Підсилення передавальної антени G_t	2 dBi (≈1,58 коефіцієнт)
Підсилення приймальної антени G_r	2 dBi (≈1,58 коефіцієнт)
Відстань d	2 км
Температура T	290 К
Ширина смуги B	125 кГц
Бітова швидкість R_b	10 кбіт/с
Модель каналу	Вільний простір (Free Space)
Довжина хвилі λ	0,328 м
Потужність прийнятого сигналу P_r	$4{,}29 \times 10^{-10}$Вт
Шумова потужність N	$5{,}0025 \times 10^{-15}$Вт

Основні формули:

$$\mathrm{SNR} = \frac{\mathrm{Pr}}{Pjam} \quad (3.1)$$

Де, Pr — потужність передавача (Вт),

P_{jam} — потужність шуму (Вт).

$$\frac{\mathrm{Eb}}{\mathrm{N0}} = \frac{\mathrm{Pr}}{Pjam \times \mathrm{Rb}} \quad (3.2)$$

Де, Pr — потужність передавача (Вт),

P_{jam} — потужність шуму (Вт),

R_b — бітова швидкість передачі (біт/с).

$$Pb = \frac{1}{2} \times \exp\left(-\frac{Eb}{2N0}\right) \quad (3.3)$$

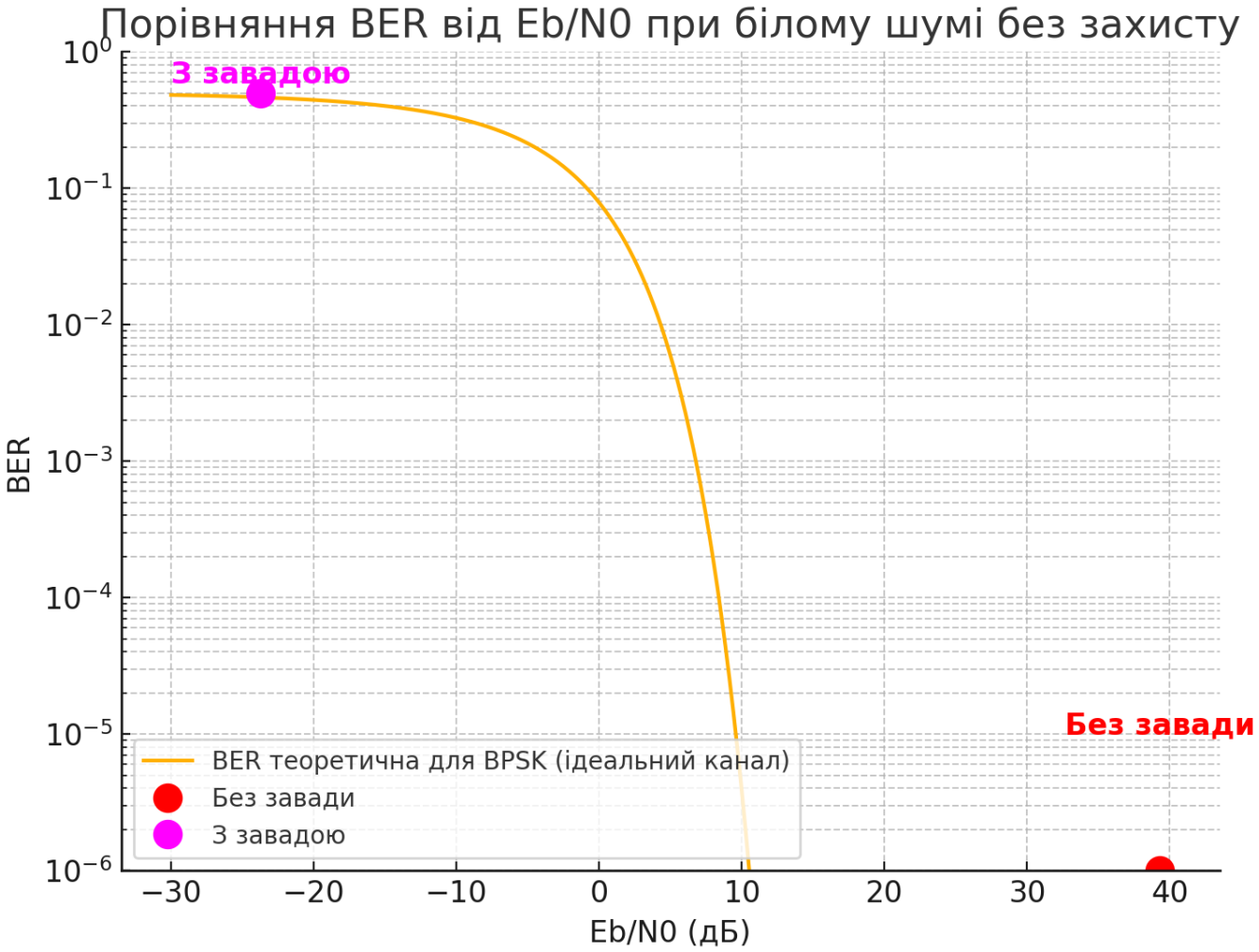
Де, P_b — ймовірність помилки біта (Bit Error Rate, BER),

$\frac{E_b}{N_0}$ — відношення енергії біта до шумової потужності.

3.1 Дослідження методів захисту при дії білому шумі

Для початку прорахуємо параметри при природньому шумі ~ 5×10^{-15}Вт без навмисних завад. За формулою (3.1), SNR ≈ 49,3 дБ, за формулою (3.2) відношення енергії біта до шумової потужності ≈ 39,3дБ, BER ≈ 0 за формулою(3.3).

Робота при білому шумі: потужність шуму –80 dBm = 10^{-11} Вт (замість природного ~5×10^{-15} Вт); бітова швидкість Rb = 10 кбіт/с. За анологічними формулами SNR ≈ 16,3 дБ, відношення енергії біта до шумової потужності ≈ −23,7дБ, BER ≈ 0,4989 . Отримуємо, що при білому шумі – 80dBm зв’язок фактично втрачено, кожен другий біт буде помилковим.



Графік 3.1 - Порівняння BER від E_b/N_0 при білому шумі без захисту

Навіть невелике зниження E_b/N_0 різко збільшує ймовірність бітових помилок. При $E_b/N_0 < 0$ дБ зв'язок практично втрачається. Це підтверджує чутливість систем до енергетичних завад та важливість захисних методів. У такому випадку потрібен захист для покращення сигналу.

Дослідимо FHSS, вхідні дані для розрахунку : частотний діапазон – 902–928 МГц (26 МГц); ширина одного каналу – 125кГц, кількість стрибків каналу ≈ 208, потужність шуму на одному каналі FHSS $\approx 4{,}8 \times 10^{-14}$Вт.

SNR (з урахуванням FHSS) ≈ 39,5 дБ за формулою (3.1) , за формулою (3.2) відношення енергії біта до шумової потужності ≈ 29,5дБ, BER ≈ 0 за формулою(3.3).

Перевірка методу протидії – FEC :

FEC додає надлишкову інформацію для виправлення помилок на приймачі. Використовуються коди: Hamming, convolutional, Reed–Solomon тощо. Дає виграш у E_b/N_0 від 1 до 6 дБ, залежно від коду і реалізації. В SiK (прошивка RFD900x) зазвичай

використовується convolutional код з виграшем ~2–3 дБ.

За анологічними формулами, відношення енергії біта до шумової потужності (припустимо виграш у 3 дБ, тобто в $10^{0,3} \approx 2$ рази) $\approx -20,7$дБ, BER $\approx 0,4978$

Перевірка методу протидії – LoRa. Вхідні дані адаптовані до LoRa: частота f = 915 МГц; ширина смуги B = 62,5 кГц (для SF=10, BW=125 кГц); ефективна швидкість ≈ 980 біт/с (для SF=10); шум при LoRa $\approx 2,5 \times 10^{-15}$Вт.

За анологічними формулами SNR $\approx 16,3$ дБ, відношення енергії біта до шумової потужності $\approx 22,4$дБ, BER ≈ 0 .

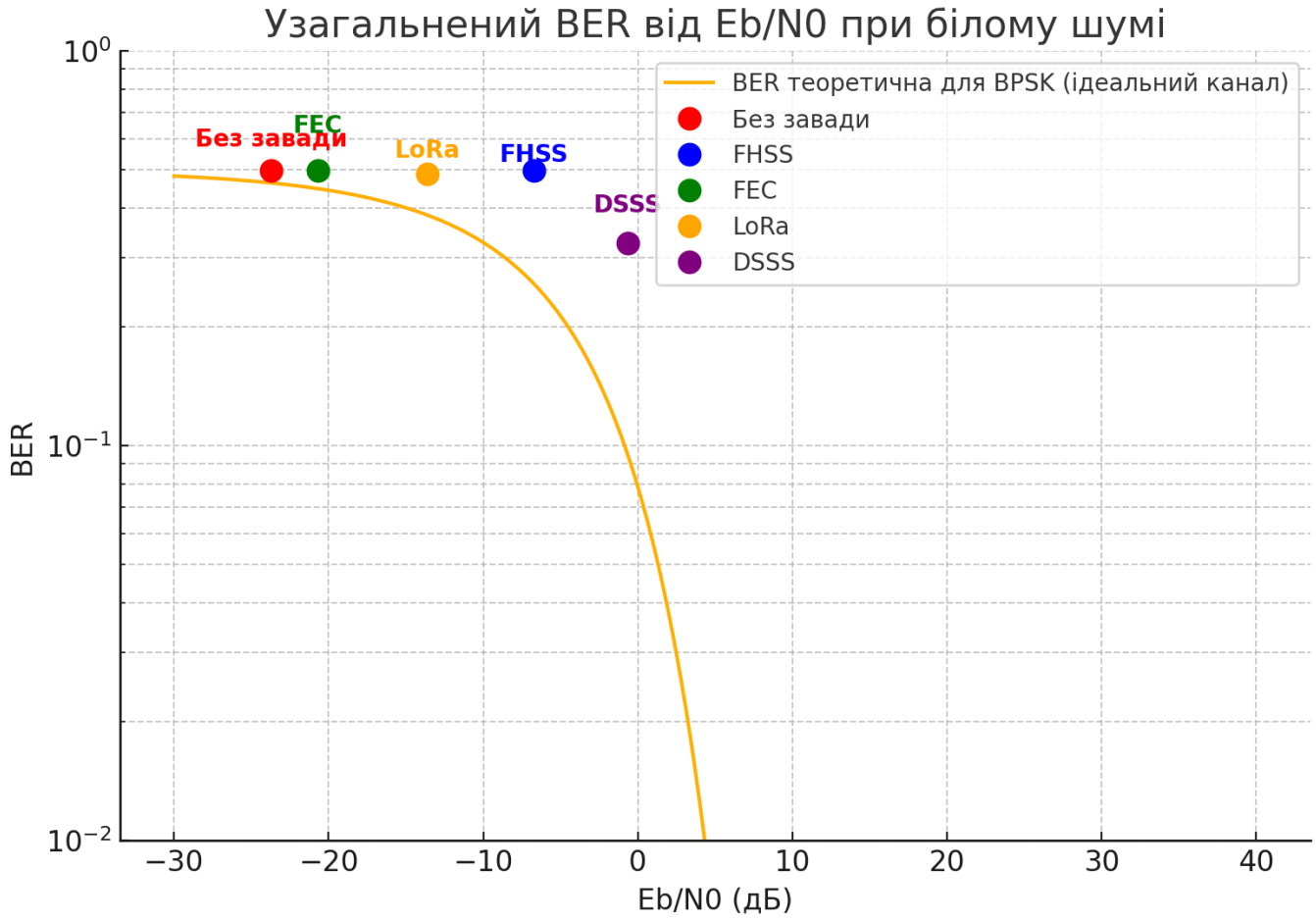
Перевірка методу протидії – DSSS. Вхідні дані адаптовані до DSSS: потужність завади N = 1×10^{-11}Вт (-89dBm); DSSS виграш $G_p \approx 200 \approx +23$дБ.

За анологічними формулами SNR $\approx 16,3$ дБ, відношення енергії біта до шумової потужності $\approx -0,67$дБ, BER $\approx 0,326$.

Таблиця 3.1

Загальна таблиця по білому шуму

Методи захисту	$\frac{Eb}{N0}$,дБ	SNR,дБ	BER	комент
Без захисту	-23,7	16,3	$\approx 0,499$	Повна втрата зв’язку, білий шум перекриває сигнал
FHSS(50каналів)	-6,7	16,3	$\approx 0,449$	Частковий захист — зменшення впливу шуму в десятки разів
FEC (+3дБ)	-20,7	16,3	$\approx 0,498$	Мінімальне покращення, не забезпечує надійності
LoRa (SF=10)	-13.6	16,3	$\approx 0,489$	У гіршому випадку — слабка стійкість, але на практиці — значно вища
DSSS (+23 дБ)	-0,67	16,3	$\approx 0,326$	Найкраща пасивна стійкість до білого шуму



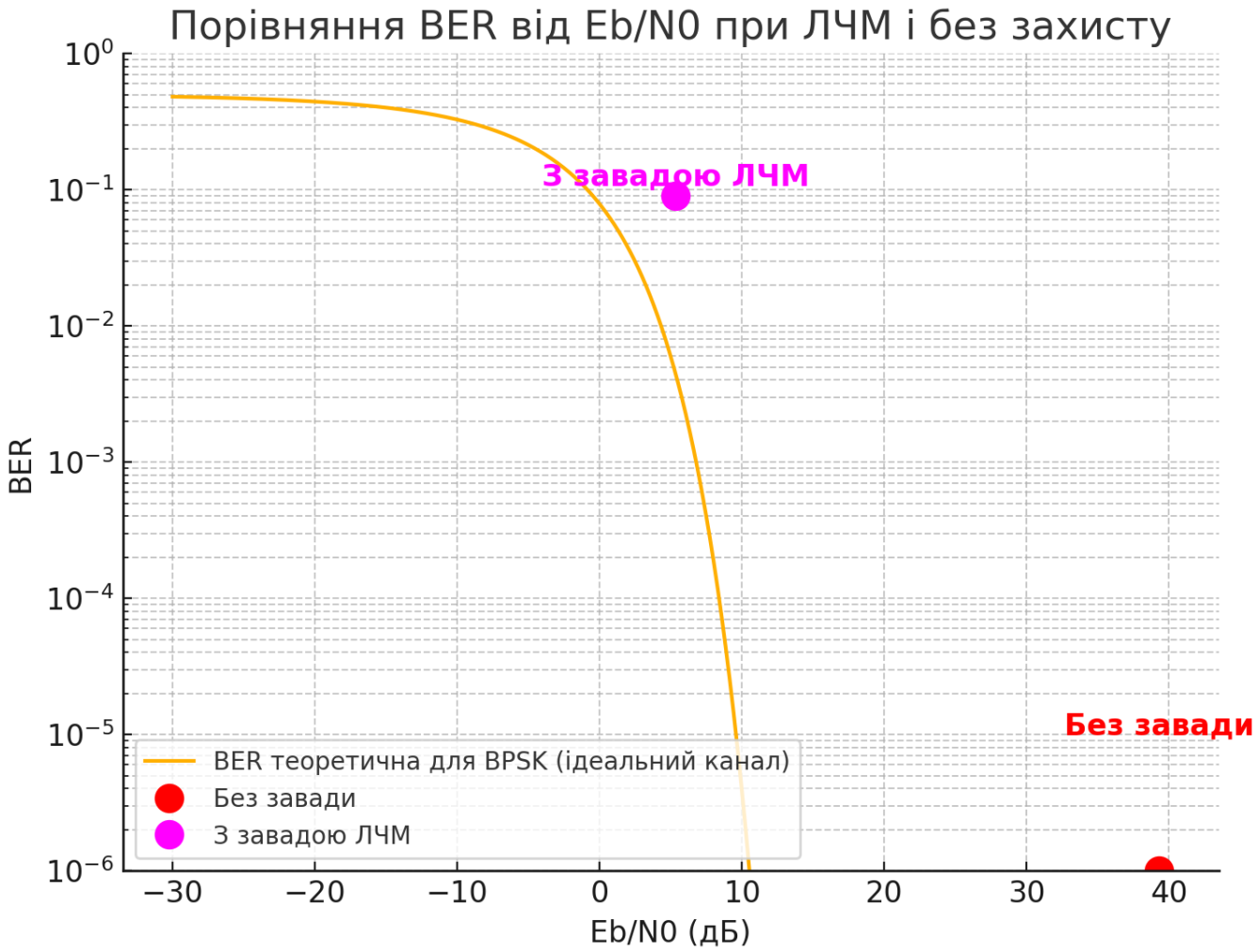
Графік 3.2 – узагальнений графік порівняння BER від E_b/N_0 при білому шумі

3.2 Дослідження методів захисту при дії ЛЧМ

Вхідні дані: потужність сигналу $P_{jam} = 1{,}25\times10^{-11}$ Вт; потужність сигналу Pr ≈ 4.29×10^{-10}Вт (як і раніше); бітова швидкість R_b = 10 кбіт/с.

Відношення сигнал/шум (SNR) при ЛЧМ за формулою (3.1) ≈ 45,36дБ, за формулою (3.2) відношення енергії біта до шумової потужності ≈ 5,36дБ, BER ≈ 0,0899 за формулою(3.3).

При дії ЛЧМ завади E_b/N_0 ≈5,36 дБ, BER зростає до ≈ 0,0899. Зв’язок ще можливий, але якість істотно погіршується — потрібен захист.



Графік 2.1 - Порівняння BER від E_b/N_0 при ЛЧМ і без захисту

FHSS, вхідні дані для розрахунку : частотний діапазон – 902–928 МГц (26 МГц); ширина одного каналу – 125кГц; кількість стрибків каналу ≈ 208; потужність завади ЛЧМ $P_{jam} = 1{,}25 \times 10^{-11}$Вт, потужність шуму на одному каналі FHSS $\approx 6{,}01 \times 10^{-14}$Вт.

SNR (з урахуванням FHSS) ≈ 38,54 дБ за формулою (3.1) , за формулою (3.2) відношення енергії біта до шумової потужності $\approx -1{,}46$дБ, BER $\approx 0{,}3499$ за формулою(3.3).

Перевірка методу протидії – FEC :

Вхідні дані такі ж самі як у розрахунку без захисту, виграш FEC +3дБ, потужність завад в межах сигналу $\approx 1{,}56 \times 10^{-14}$Вт.

За анологічними формулами, відношення енергії біта до шумової потужності (припустимо виграш у 3 дБ, тобто в $10^{0,3} \approx 2$ рази) ≈ 7,40дБ, BER ≈ 0,321

Перевірка методу протидії – LoRa. Вхідні дані адаптовані до LoRa: потужність (ЛЧМ) завади $P_{jam} = 1{,}25 \times 10^{-11}$Вт (-89dBm); потужність сигналу $P_r = 4.29 \times 10^{-10}$Вт;

ширина сигналу B_{sig} = 125 кГц; ширина завади B_{jam} = 100 МГц; бітова швидкість R_b = 980 біт/с (SF=10);потужність завади в межах сигналу $P_{noise,\ LoRa} \approx 1{,}56 \times 10^{-15}$Вт.

За анологічними формулами SNR $\approx 15{,}36$ дБ, відношення енергії біта до шумової потужності $\approx 34{,}49$дБ, BER ≈ 0 .

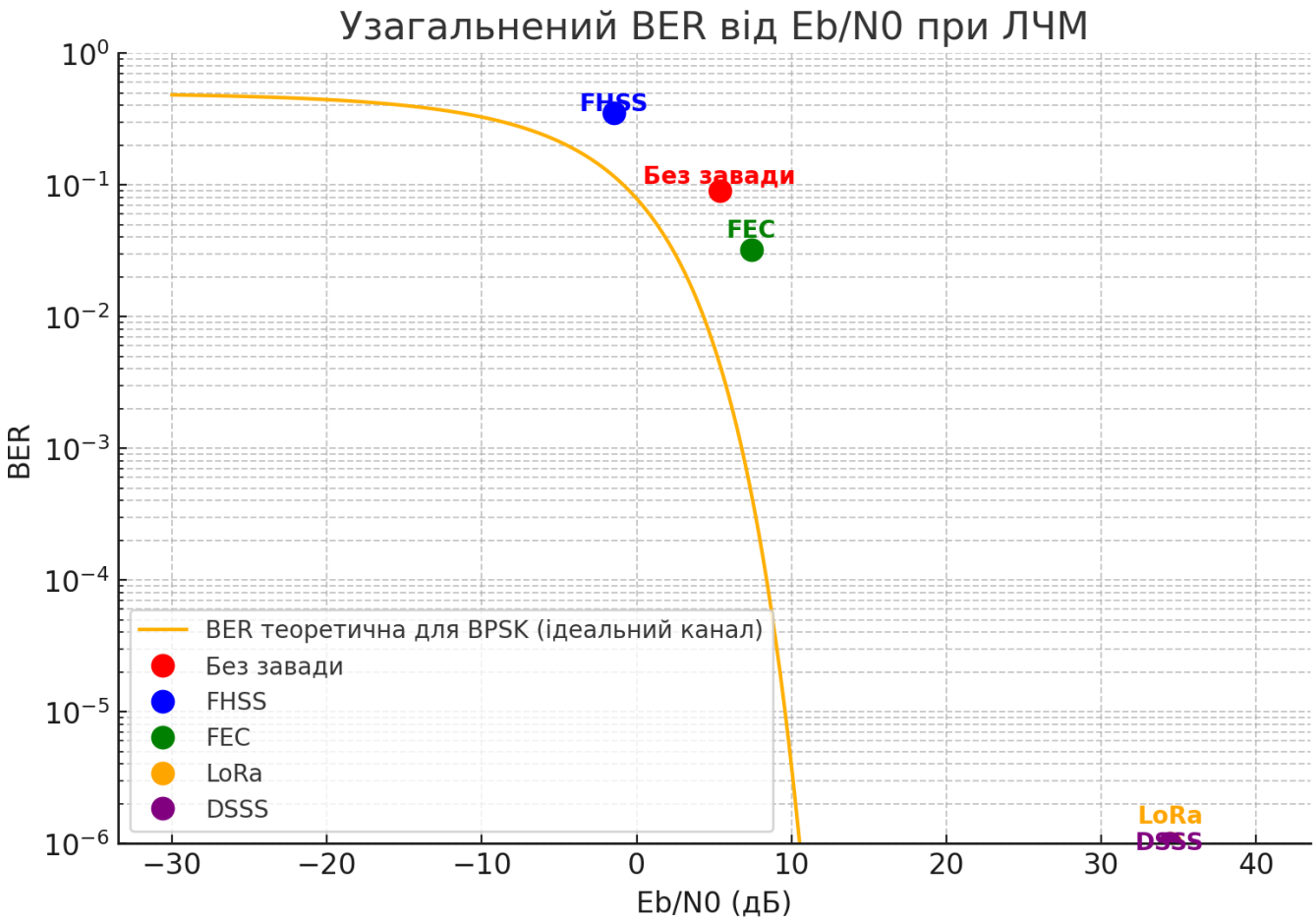
Перевірка методу протидії – DSSS. Вхідні дані адаптовані до DSSS: потужність завади $P_{jam} = 1{,}25 \times 10^{-11}$Вт (-89dBm); потужність завади в межах сигналу $P_{noise,\ FHSS} \approx 1{,}56 \times 10^{-15}$Вт.

За анологічними формулами SNR $\approx 54{,}38$ дБ, відношення енергії біта до шумової потужності $\approx 34{,}39$дБ, BER ≈ 0 .

Таблиця 3.2

Загальна таблиця по ЛЧМ

Методи захисту	$\frac{Eb}{N0}$,дБ	SNR,дБ	BER	комент
Без захисту	5,36	45,36	$\approx 0{,}0899$	Зв’язок ще можливий, але помилки значні — потрібен захист
FHSS(50каналів)	-1,46	38,54	$\approx 0{,}3499$	Захист неефективний без додаткових методів (BER > 0,3)
FEC (+3дБ)	7,40	15,36	$\approx 0{,}0321$	Помітне покращення, але зв’язок усе ще ненадійний
LoRa (SF=10)	34.49	15,36	≈ 0	Надійний зв’язок, BER ≈ 0 — висока стійкість до ЛЧМ
DSSS (+23 дБ)	34,39	54,38	≈ 0	Найкращий результат — BER ≈ 0, стійкість максимальна



Графік 1.2 – узагальнений графік порівняння BER від E_b/N_0 при ЛЧМ

Висновки:

У цьому розділі було проведено розрахункове дослідження стійкості каналу зв'язку безпілотного літального апарата (БПЛА) до дії навмисних радіоелектронних завад. Об'єктом аналізу був канал, реалізований на базі LoRa-модуляції у діапазоні 868 МГц. Основну увагу приділено оцінці впливу енергетичних (білий шум) та лінійно-частотно модульованих (ЛЧМ) завад на рівень бітових помилок (BER) та якість зв'язку загалом.

Результати розрахунків підтвердили, що у випадку відсутності захисту рівень BER значно зростає при дії навмисних завад, зокрема у зоні SNR нижче 0 дБ канал повністю втрачає стабільність. Найбільш руйнівний вплив спостерігався при ЛЧМ-завадах, які, завдяки спектральній схожості з сигналом LoRa, викликали псевдосинхронізацію та помилкове декодування.

Оцінка ефективності окремих захисних методів показала, що використання LoRa з високим spreading factor дозволяє підтримувати роботу каналу навіть при негативному SNR, знижуючи BER до допустимого рівня. DSSS-модуляція

забезпечила підвищену стійкість до широкосмугових завад. Водночас FHSS виявився менш ефективним саме проти ЛЧМ-сигналів, хоча демонструє перевагу у випадках випадкових вузькосмугових завад.

Таким чином, дослідження підтвердило доцільність використання спектрально розширених модуляцій як основного засобу захисту каналу зв’язку БПЛА в умовах радіоелектронної протидії. Найбільш ефективними у розрахованих сценаріях виявилися LoRa та DSSS, що забезпечили зниження BER до критично важливих меж і збереження керованості апарата при дії завад.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У ході дослідження було встановлено, що система зв’язку безпілотних літальних апаратів є складною багаторівневою структурою, яка включає апаратні, програмні та енергетичні компоненти, що тісно взаємодіють між собою для забезпечення безперебійної передачі даних у режимі реального часу.

Апаратна частина системи складається з радіомодуля, що відповідає за формування, модуляцію, передачу та прийом сигналів, а також антенної системи, що забезпечує стабільний рівень сигналу і спрямованість випромінювання. Важливим фактором є відповідність використовуваних частотних діапазонів, де найпоширенішими для малогабаритних БПЛА є ISM-смуги (433, 868, 915 МГц), які забезпечують оптимальний баланс між дальністю зв’язку та стійкістю до перешкод.

Програмна складова включає протоколи передачі даних (зокрема MAVLink, UAVCAN), які регламентують структуру пакетів, контроль помилок та взаємодію між бортовою системою і наземною станцією управління. Виявлено, що класичні протоколи без вбудованої автентифікації вразливі до атак типу спуфінг і replay, що вимагає впровадження додаткових механізмів безпеки.

Особливу увагу приділено енергозабезпеченню, оскільки обмежений ресурс живлення впливає на тривалість польоту та стабільність роботи системи зв’язку. Використання енергозберігаючих режимів, адаптивне керування потужністю передавача і частотою оновлення дозволяють оптимізувати споживання енергії без суттєвих втрат у якості зв’язку. Дослідження підтвердило, що різні типи навмисних завад суттєво впливають на якість і надійність каналів зв’язку БПЛА. Енергетичні завади у вигляді широкосмугового білого шуму призводять до значного зниження співвідношення сигнал/шум, що викликає зростання помилок і може спричинити втрату керування.

Лінійно-частотно модульовані (ЛЧМ) завади є особливо небезпечними через їхню спектральну схожість із chirp-сигналами LoRa, що ускладнює їх розпізнавання та спричиняє помилкове декодування. Структуровані завади, які імітують легітимні команди, створюють загрозу виконання хибних дій через відсутність автентифікації.

Імпульсні та шумоподібні завади викликають локальні збої в прийомі сигналу,

порушуючи синхронізацію і тимчасово знижуючи стійкість каналу. Загалом, різноманітність завад вимагає застосування багаторівневих заходів захисту, що враховують їхні специфічні особливості.

Результати дослідження показали, що методи спектрального розширення, зокрема LoRa CSS та DSSS, забезпечують найвищу стійкість каналів зв’язку до широкосмугових і ЛЧМ-завад. Частотне рознесення та резервування каналів значно підвищують живучість системи, дозволяючи уникнути одночасного пригнічення всіх каналів.

FHSS виявився ефективним переважно проти вузькосмугових перешкод, але має обмеження при атаках ЛЧМ. Використання FEC і адаптивних параметрів передачі додатково підвищує надійність, хоча може збільшувати затримки.

Розрахункове моделювання впливу навмисних завад — білого шуму та ЛЧМ — на канали зв’язку БПЛА підтвердило критичний вплив цих перешкод на якість передачі даних. Без застосування захисних заходів рівень бітових помилок (BER) різко зростає, що ускладнює або унеможливлює стабільне керування апаратом.

Значним покращенням характеристик зв’язку відзначаються технології спектрального розширення — LoRa CSS і DSSS. Вони дозволяють підтримувати низький BER навіть при негативних значеннях співвідношення сигнал/шум (SNR), що забезпечує надійний зв’язок у складних завадових умовах.

Частотне хопінгування (FHSS), хоча і знижує вплив вузькосмугових завад, виявилося менш ефективним проти ЛЧМ-атак, де спектральна подібність завади і корисного сигналу значно ускладнює розпізнавання.

Впровадження кодування з виправленням помилок (FEC) підвищує стійкість каналу, але самостійно не здатне повністю компенсувати вплив сильних завад, особливо ЛЧМ.

Отримані результати мають важливе практичне значення для проєктування надійних і захищених каналів управління БПЛА, особливо в умовах активного радіоелектронного протистояння. Використання технологій спектрального розширення, динамічної адаптації параметрів передачі та комплексного протокольного захисту дозволяє суттєво підвищити стійкість зв’язку до різних типів навмисних завад.

Практична реалізація рекомендацій цієї роботи може сприяти підвищенню

безпеки польотів, зниженню ризиків втрати управління та підвищенню ефективності застосування БПЛА в оборонних, цивільних і наукових сферах.

Перспективними напрямами подальших досліджень є розробка гібридних систем захисту, впровадження алгоритмів автоматичного виявлення та класифікації типів завад у реальному часі, а також інтеграція криптографічних методів безпеки в канали зв’язку. Це дозволить не лише підвищити живучість систем, а й забезпечити захист від складних кібератак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кайденко, М. М., Кравчук, С. О. Захист від впливу різних класів атак на канали управління безпілотних літальних апаратів // Інформаційні та телекомунікаційні науки. — 2022. — №1. — С. 35–43. — https://doi.org/10.20535/2411-2976.12022.35-43

2. Гетьман, О. В., Кайденко, М. М. Характеристики навмисних завад, що діють на канал зв’язку безпілотного літального апарату // Збірник матеріалів XVI Міжнародної науково-технічної конференції «Перспективи телекомунікацій» (ПТ–2022). — Київ : КПІ ім. Ігоря Сікорського, 2022. — С. 143–145.

3. Кайденко, М. М. Сценарії прихованого впливу навмисних завад на канали зв’язку безпілотних літальних апаратів // Збірник матеріалів XVI Міжнародної науково-технічної конференції «Перспективи телекомунікацій» (ПТ–2022). — Київ : КПІ ім. Ігоря Сікорського, 2022. — С. 140–142.

4. Кайденко, М. М., Роскошний, Д. В., Гетьман, О. В. Оцінка живучості каналу зв’язку БПЛА в умовах впливу навмисних та ненавмисних завад // Збірник матеріалів XVI Міжнародної науково-технічної конференції «Перспективи телекомунікацій» (ПТ–2022). — Київ : КПІ ім. Ігоря Сікорського, 2022. — С. 124–126.

5. Sklar, B. Digital Communications: Fundamentals and Applications. 2nd ed. — Prentice Hall, 2001. — 770 p.

6. Zeng, K., Zhang, H., Lin, J. Jamming-Resistant Communications for UAV Networks: A Survey // IEEE Communications Surveys & Tutorials. — 2020. — Vol. 22, No. 4. — P. 2769–2795. — DOI: 10.1109/COMST.2020.2998101

7. Prasad, M. V. R. K. D., Pathak, S. K. LoRa Technology: A Review // International Journal of Engineering & Technology. — 2018. — Vol. 7, No. 4. — P. 3458–3464.

8. Yan, L., Shi, Y., Li, Y. Frequency-Hopping Spread Spectrum Techniques for Secure UAV Communications // IEEE Access. — 2019. — Vol. 7. — P. 156521–156531. — DOI: 10.1109/ACCESS.2019.2949572

9. Islam, S. M., O’Connor, N. E., Murphy, L. Security and Privacy in UAV Communications: A Survey // IEEE Communications Surveys & Tutorials. — 2021. — Vol. 23, No. 2. — P. 1221–1254. — DOI: 10.1109/COMST.2021.3059538