МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Системи управління БПЛА в умовах електромагнітних завад»

Виконавець: _____ Мирослав ПАЛАМАРЧУК
(підпис)

Керівник: _____ Володимир КЛИМЧУК
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Катерина КАЖАН
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Лариса ЧЕРНЯК
(підпис)

Нормоконтролер: _____ Богдан ЧУМАЧЕНКО
(підпис)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Електронні комунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Віктор ГНАТЮК
“_____”_____2025 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Паламарчука Мирослава Юрійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Системи управління БПЛА в умовах електромагнітних завад»
затверджена наказом ректора від «02» вересня 2025 р. № 1672 /ст
2. Термін виконання роботи: з 29.09.2025 р. по 31.12.2025 р.
3. Вихідні дані до роботи: 1. Безпілотні літальні апарати. 2. Методи передачі даних. 3. Алгоритми та ефективність передачі даних.
4. Зміст пояснювальної записки: Теоретичні основи функціонування систем управління БПЛА та вплив завад. Аналіз та моделювання адаптивних алгоритмів. Проєктування та реалізація бортового пристрою. Техніко-економічне обгрунтування.
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: .слайди презентацій в програмному пакеті Microsoft Power Point

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	29.09.2025-30.09.2025	Виконано
2	Вступ	01.10.2025-03.10.2025	Виконано
3	Теоретичні основи функціонування систем управління БПЛА та вплив електромагнітних завад	04.10.2025-14.10.2025	Виконано
4	Аналіз та моделювання алгоритмів адаптивного управління БПЛА в умовах електромагнітних завад	15.10.2025-26.10.2025	Виконано
5	Проєктування та реалізація бортового пристрою управління з підвищеною стійкістю до завад	27.10.2025-7.11.2025	Виконано
	Альтернативні методи забезпечення завадостійкості. Розробка системи проводового управління БПЛА	8.11.2025-19.11.2025	Виконано
	Техніко економічне обґрунтування та стартап-концепція проєкту	20.11.2025-01.12.2025	Виконано

	Охорона праці	02.12.2025-09.12.2025	Виконано
7	Охорона навколишнього середовища	10.12.2025-14.12.2025	Виконано
8	Усунення недоліків та захист кваліфікаційної роботи	15.12.2025-31.12.2025	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.т.н., доц. Катерина КАЖАН		
Охорона навколишнього середовища	д.т.н., доц. Лариса ЧЕРНЯК		

8. Дата видачі завдання: «01» вересня 2025 р.

Керівник кваліфікаційної роботи _____ Володимир КЛИМЧУК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Мирослав ПАЛАМАРЧУК
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Системи управління БПЛА в умовах електромагнітних завад» містить 117 сторінок, 28 рисунків, 13 таблиці, 44 використаних джерел.

Ключові слова – БПЛА, завадостійкість, РЕБ, LoRa, LTE, адаптивне управління, оптоволокно, Raspberry PI.

Об’єкт дослідження – процес функціонування систем дистанційного керування безпілотними літальними апаратами (БПЛА) в умовах складної електромагнітної обстановки..

Предмет дослідження – методи та алгоритми забезпечення завадостійкості каналів зв’язку, апаратні засоби адаптивного управління та технологій проводової передачі даних.

Мета кваліфікаційної роботи – зробити систему управління швидкісними БПЛА значно надійнішою та “живучішою”. Для цього ми пішли двома шляхами: розробили адаптивний радіоконтролер, який сам підлаштовується під умови ефіру, та обґрунтували концепцію альтернативного керування через оптоволокно..

Метод дослідження – системний аналіз дозволив класифікувати загрози, математичне моделювання допомогло розрахувати бюджет каналів зв’язку та затримки, а імітаційне моделювання підтвердило ефективність алгоритмів адаптації. Фінальним етапом стало безпосереднє схемотехнічне проєктування. Ми детально проаналізували, як саме засоби радіоелектронної боротьби (РЕБ) “глушать” канали управління дронами. Відповіддю на ці виклики став наш адаптивний алгоритм: він автоматично перемикається між каналами LTE, Wi-Fi та LoRa, орієнтуючись на рівень завад. Апаратну частину бортового контролера спроєктовано на базі доступного мікрокомп’ютера Raspberry Pi Zero 2 W. Крім того, для умов тотального радіопридушення запропоновано радикальне рішення - концепцію абсолютно завадостійкої системи управління через надтонкий оптоволоконний кабель..

Матеріали кваліфікаційної роботи рекомендується використовувати як основу для створення завадостійких систем управління.

Програмно-апаратний комплекс “Aegis-Link” та адаптивний алгоритм AMPA дозволяють модернізувати наявні дрони, забезпечуючи автоматичне перемикання між Wi-Fi, LTE та LoRa на основі багатофакторного аналізу якості каналу. Окремої уваги заслуговує концепція “Fiber-Strike”, яка завдяки використанню оптоволокна гарантує абсолютну невразливість апарата до засобів радіоелектронної боротьби, що є “срібною кулею” для прориву ворожих РЕБ-куполів.

В інженерному аспекті робота пропонує готову базу на основі Raspberry Pi Zero 2 W, включаючи перевірені розрахунки теплового балансу, схеми захисту живлення та методику боротьби з вібраціями, що суттєво прискорює проєктування нових БПЛА. Науковцям та освітянам ці матеріали будуть корисні завдяки формалізованим математичним моделям “лавинного зростання затримки” та детальному розрахунку бюджету оптичної лінії, які ідеально підходять для наповнення профільних навчальних дисциплін. Нарешті, для екологічно відповідального виробництва пропонується стратегія переходу на біорозкладний PLA-пластик та безсвинцеві припої, що дозволяє значно знизити техногенне навантаження на довкілля в зонах бойових дій.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

AMS (Adaptive modulation and coding) – Адаптивна модуляція та кодування.

БПЛА – Безпілотний літальний апарат.

БС – Базова станція.

ЕМВ – Електромагнітне випромінювання.

ЕМО – Електромагнітна обстановка.

ЕМС – Електромагнітна сумісність.

РЕБ – Радіоелектронна боротьба.

НСУ – Наземна станція управління.

BER (Bit Error Rate) – Коефіцієнт бітових помилок.

BVLOS (Beyond Visual Line of Sight) – Політ поза межами прямої видимості.

CSS (Chirp Spread Spectrum) – Модуляція з розширенням спектру методом ЛЧМ.

FHSS (Frequency Hoping Spread Spectrum) – Псевдовипадкове перелаштування робочої частоти.

GPIO (General Purpose Input/Output) – Інтерфейс введення/виведення загального призначення.

LoRa (Long Range) – Технологія модуляцій для зв’язку на великі відстані.

LTE (Long-Term Evolution) – Стандарт бездротового високошвидкісного передавання.

MAVLink – Протокол обміну даними для малих безпілотних апаратів.

RSSI (Received Signal Strength Indicator) – Показник рівня прийнятого сигналу.

SFP (Small Form-factor Pluggable) – Компактний трансивер для передачі даних по оптоволокну.

SNR (Signal-to-Noise Ratio) – Співвідношення сигнал/шум.

UART – Універсальний асинхронний прийомопередавач.

ВСТУП

Актуальність теми. Сучасні військові конфлікти та техногенні катастрофи чітко дали зрозуміти: безпілотники - це критично важливий інструмент розвідки та моніторингу [1, 4, 15, 33, 36]. Однак масове використання засобів РЕБ перетворило канал зв'язку на "ахіллесову п'яту" всього комплексу [17, 35]. Стандартні методи захисту, такі як шифрування чи псевдовипадкове перелаштування частоти (ППРЧ), на жаль, стають безсилими перед щільними загороджувальними завадами [20, 22]. Це призводить до втрати вартісної техніки та зриву місій. Ситуація вимагає принципово нових рішень - створення адаптивних систем, які вміють змінювати саму фізику передачі даних залежно від бойової обстановки [25, 32].

Зв'язок роботи з науковими програмами, планами, темами.

Мета і завдання дослідження. Головна мета нашої роботи полягала в тому, щоб зробити систему управління швидкісними БПЛА значно надійнішою та "живучішою". Для цього ми пішли двома шляхами: розробили адаптивний радіоконтролер, який сам підлаштовується під умови ефіру, та обґрунтували концепцію альтернативного керування через оптоволокно [12, 25]. Щоб досягти цього, нам довелося вирішити низку наукових завдань: спершу ми детально дослідили сучасний стан систем управління та класифікували джерела електромагнітних завад, щоб зрозуміти ворога "в обличчя" [17, 36]. Далі ми розробили математичні моделі для каналів Wi-Fi, LTE та LoRa, теоретично оцінивши їхню поведінку під тиском активних перешкод.[11, 21].

Ключовим етапом стала розробка та обґрунтування адаптивного алгоритму AMPA, унікальність якого полягає в автоматичному перемиканні між різними фізичними інтерфейсами на основі аналізу якості каналу в реальному часі. Фінальним етапом стало безпосереднє схемотехнічне проєктування бортового пристрою, де ми підібрали електронні компоненти, здатні стабільно працювати разом. Крім того, ми дослідили потенціал волоконно-оптичної лінії як гарантії абсолютної стійкості до

РЕБ, розробивши схему системи розмотування кабелю для швидкісних дронів, а проведене імітаційне моделювання підтвердило як технічну ефективність, так і економічну вигоду запропонованих рішень.

Об'єктом дослідження – система дистанційного керування високомобільними БПЛА.

Предметом дослідження – методи підвищення завадостійкості, алгоритми розумної маршрутизації даних та технології проводового зв'язку.

Методи досліджень. – теорія інформації (пропускна здатність), теорія автоматичного керування (аналіз латентності), схемотехнічне моделювання та прототипування.

Наукова новизна та практичне значення отриманих результатів.

Наукова новизна отриманих результатів:

Наукова новизна отриманих результатів полягає насамперед у вдосконаленні методу адаптивного управління: ми пішли далі існуючих рішень, що спираються лише на стрибки частоти (ППРЧ). Наш мультиконтрольний алгоритм AMPA унікальний тим, що використовує комплексний критерій якості, враховуючи не лише силу сигналу (RSSI), а й динаміку зростання затримок та втрат пакетів. Це дозволяє системі безшовно перемикатися між абсолютно різними середовищами - Wi-Fi, LTE, LoRa - зберігаючи контроль над апаратом навіть при критичному співвідношенні сигнал/шум до -20 дБ. Також ми розвинули математичну модель обміну даними, вперше провівши комплексне моделювання впливу РЕБ саме на високошвидкісні маневрові БПЛА, врахувавши сукупний ефект енергетичного блокування та доплерівського зсуву, що дозволило виявити та компенсувати небезпечний ефект "лавинного зростання латентності".

Практичне значення отриманих результатів:

Ми спроєктували схему та написали софт для контролера на базі доступного Raspberry Pi Zero 2 W, об'єднавши модулі LoRa та LTE. Це універсальне рішення вартістю до $200 вже зараз можна встановлювати на серійні дрони, суттєво підвищуючи їхні шанси на виживання, що підтверджується розрахунками енергоспоживання. Крім того, для умов тотального радіопридушення ми

запропонували радикальне інженерне рішення - концепцію “дронів на нитці” з системою безінерційного розмотування мікрокабелю та використанням SFP-модулів. Це дозволяє створити канал управління з нульовою чутливістю до будь-яких засобів РЕБ на дистанції 10–20 км, що є ідеальним варіантом для ударних БПЛА та розвідників в умовах насиченої протиповітряної оборони.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ СИСТЕМ УПРАВЛІННЯ БПЛА ТА ВПЛИВ ЕЛЕКТРОМАГНІТНИХ ЗАВАД

1.1. Класифікація безпілотних літальних апаратів та особливості високомобільних БПЛА

1.1.1. Системний підхід до класифікації безпілотних авіаційних систем

У сучасній інженерній думці вже відійшли від сприйняття безпілотника просто як окремого виробу [31]. Сьогодні ми говоримо про безпілотні авіаційні системи (БАС) - складні програмно-апаратні "організми" [1, 4]. Згідно зі стандартами ICAO та натовськими протоколами (STANAG 4671), БПЛА - це літальний апарат без пілота на борту, який керується дистанційно або ж діє повністю автономно [2, 31].

Однак термін БАС значно ширший [36]. Це не лише "залізо" в небі [18]. Повноцінна система включає чотири критичні елементи: 1) сам борт із двигуном та електронікою [18]; 2) наземну станцію управління (GCS), яка слугує "містком" між інтелектом людини та машини [9, 26]; 3) Канал зв'язку (C2 Link) - своєрідну нервову систему комплексу, через яку йдуть команди та повертається телеметрія [1, 12]; 4) корисне навантаження та засоби запуску/посадки [33]. Саме такий комплексний погляд дозволяє бачити повну картину і вирішувати проблеми управління системно, а не точково [6, 15].

Класифікація цих апаратів - завдання нетривіальне, адже критеріїв безліч [4]. Проте для розробників систем управління найбільш показовим є поділ за трьома ключовими ознаками [31, 36]:

1. За вагою та масштабом завдань

Тут ми дивимося на злітну масу (MTOW) та радіус дії:

- Клас I (мікро та міні): "Малюки" вагою до 150 кг [31]. Сюди входять як мікро-дрони (до 2 кг), так і міні-БПЛА (до 15 кг) [33]. Це робочі конячки тактичного

рівня (взвод-рота), що працюють на дистанціях 10–25 км [36]. *Інженерний нюанс:* головний біль цього класу - неймовірна щільність компонування [18]. Електроніка настільки спресована в тісному корпусі, що розвести в просторі силові кабелі та чутливі сенсори (магнітометри, GPS) майже неможливо [20]. Це створює серйозні виклики для електромагнітної сумісності [31, 35].

- Клас II (тактичні): апарати вагою від 150 до 600 кг [31]. Це вже рівень бригади чи дивізії [33]. Вони можуть нести серйозне обладнання для РЕБ чи потужні станції зв'язку, а також мають дубльовані системи навігації для надійності [18, 36].
- Клас III (стратегічні): важковаговики понад 600 кг (категорії MALE та HALE) [4]. Це стратегічні платформи, здатні висіти на висоті до 20 км понад добу, виконуючи глобальні місії [6, 31].

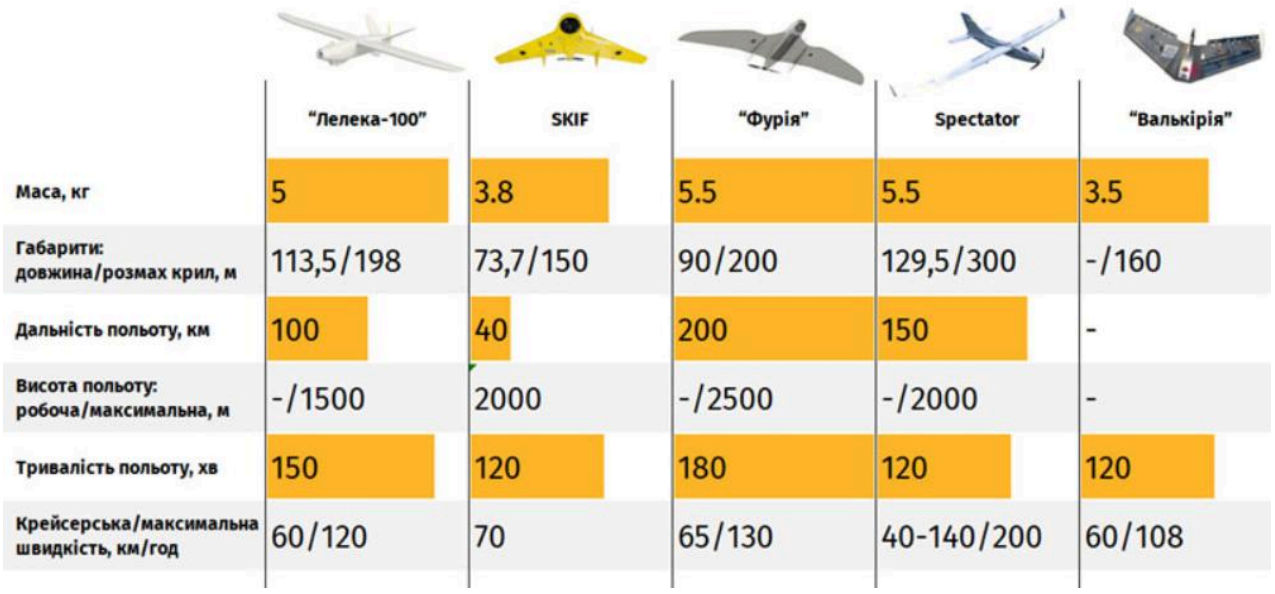


Рис. 1.1. Класифікація безпілотних літальних апаратів за масою та розмірами

2. За "інтелектом" та архітектурою управління:

- Дистанційно пілотовані (RPA): оператор керує дроном у реальному часі через наземну станцію [9]. Тут критично важливою є швидкість передачі даних [1]. Оскільки контур управління замикається через людину, до технічної затримки додається час реакції пілота (це ще 0,2–0,4 с), що може бути фатальним у динамічних ситуаціях [31, 37].

- Автоматичні: летять за чітко прописаним сценарієм, орієнтуючись на супутники (GNSS) [4]. Пілот втручається лише на старті, при посадці або в разі форс-мажору. Боротьбу з вітром та стабілізацію бере на себе автоматика [18, 31].
- Автономні: це системи зі штучним інтелектом на борту [15]. Вони здатні "думати": самостійно змінювати маршрут, облітати перешкоди та приймати рішення навіть в умовах повного радіомовчання [5, 6]. Ціна питання: висока автономність вимагає потужних бортових комп'ютерів, які, на жаль, самі стають джерелами сильних електромагнітних завад [20, 31].

3. За аеродинамічною конструкцією:

- Фіксоване крило (Fixed wing): Класичні літаки [31]. Економічні, швидкі, далекобійні завдяки високій аеродинамічній якості [33]. Мінус очевидний - їм потрібна злітна смуга або катапульта [4].
- Мультиротори (Rotary wing): Коптери, що можуть злітати вертикально і зависати на місці [31]. Але за це доводиться платити енергією: вони змушені постійно боротися з гравітацією, витрачаючи заряд батарей [18]. Динамічно це дуже нестабільні системи, що вимагають миттєвої реакції стабілізаційного контуру [37].
- Гібриди (VTOL): Спроба поєднати краще з двох світів - вертикальний зліт коптера та економічний політ літака. Найскладніше тут - перехідні режими, коли підйомна сила перерозподіляється між роторами та крилами. У цей момент поведінка апарата змінюється нелінійно, що є справжнім викликом для інженерів систем управління [33, 36, 37].

1.1.2. Динамічні характеристики та специфіка високомобільних БПЛА

Окремої уваги в нашому дослідженні заслуговують високомобільні БПЛА (High-Mobility UAVs), або ж баражуючі боєприпаси [33]. Це не просто дрони, а справжні "спринтери" небес, здатні розганятися до швидкостей понад 100–150$ км/год та виконувати карколомні маневри [37].

Ключовий параметр, що відділяє цей клас від звичайних коптерів, - це тягоозброєність (TWR - Thrust-to-Weight Ratio). Якщо у класичних дронів це

співвідношення скромне (від 0.3$ до 0.6$), то у швидкісних мультироторних систем тяга може перевищувати вагу вдвічі (2:1). А у спортивних FPV-дронів цей показник взагалі сягає фантастичних 10:1. Така шалена потужність дозволяє миттєво змінювати вектор руху, але водночас ставить надзвичайно жорсткі вимоги до реакції системи управління [18, 37].

Ось три "кити", на яких тримається складність керування такими апаратами:

1. Екстримальна динаміка. Під час віражів перевантаження можуть сягати 5–8 g. У таких умовах контур управління має оновлюватися з частотою понад 400 Гц [18]. Критично важливо мінімізувати будь-які затримки в ланцюжку "датчик - контролер – мотор". Найменша розсинхронізація (Jitter) у протоколах на кшталт DSHOT чи ProShot - і стабільність втрачено [37].

2. Аеродинамічна нестабільність: Щоб дрон був маневреним, його центр ваги часто зміщують, роблячи систему статично нестабільною [31]. Втримати її в повітрі може лише активна цифрова система автоматичного керування (ACS) [18]. Додайте сюди потужні вібрації від високообертових двигунів, які "зводять з розуму" чутливі MEMS-гіроскопи [14, 18]. Щоб отримати чистий сигнал, доводиться застосовувати складну математичну магію: фільтри Калмана, режекторні фільтри (Notch filters) тощо [18, 37].

3. Енергоємність: Потужні безщіткові двигуни (BLDC) споживають пікові струми в 50–100 А, створюючи сильні імпульсні завади [20]. Це справжнє випробування для електромагнітної сумісності: магнітометр (компас) може "збожеволіти", а GPS-приймач - просто заглухнути [31, 35].

І найголовніше - час. Для швидкісного дрона затримка - це вирок. На швидкості 150 км/год (41.6 м/с) затримка всього у пів секунди (500 мс) означає, що апарат пролетить понад 20 метрів "наосліп". У міській забудові чи складному рельєфі це гарантована аварія [33, 36].

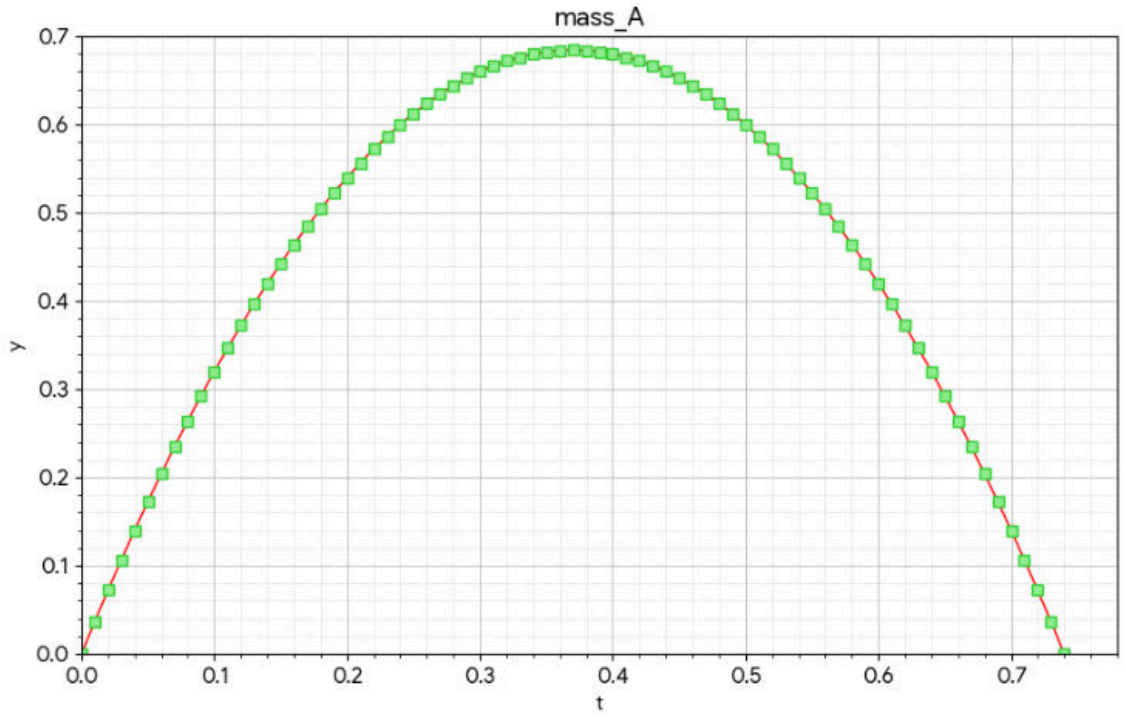


Рис. 1.2. Схема сил, що діють на високомобільний БПЛА під час виконання активного маневру

1.2. Структура та принцип роботи систем управління БПЛА

1.2.1. Узагальнена архітектура контуру управління

Систему управління сучасного БПЛА можна уявити як складну ієрархію, що працює за принципом замкнутого контуру зі зворотним зв'язком. Мовою науки (теорії автоматичного управління) дрон - це багатовимірний динамічний об'єкт (MIMO) [31]. Його стан описується вектором *X* (де ми, як швидко летимо, куди дивимось), а керуємо ми ним через вектор *U* (оберти моторів, кути закрилків) [37].

Архітектура поділяється на дві великі частини: те, що в небі, і те, що на землі [1, 18].

1. Бортовий сегмент (Onboard). Польотний контролер (FC) - це справжній “мозочок” системи, який працює в режимі жорсткого реального часу. Він базується на високопродуктивних мікроконтролерах (зазвичай архітектури ARM Cortex-M4/M7) і виконує три фундаментальні завдання в нескінченному циклі:

- Збір даних (Sensor acquisition): Перший етап - це миттєве опитування сенсорів [15]. Контролер через швидкісні шини SPI або I2C витягує дані з інерційного вимірювального блоку (IMU) - гіроскопів та акселерометрів, а також зчитує показники магнітометрів і барометрів [18, 31]. Швидкість тут вирішує все [37].
- Об'єднання даних (Sensor fusion): “Сирі” дані з датчиків завжди містять шум та похибки [14]. Тому контролер не вірить їм “на слово”, а обробляє через складні математичні алгоритми, такі як розширений фільтр Калмана (EKF) або комплементарні фільтри [18]. Це дозволяє відсіяти шум і отримати єдину, математично точну картину орієнтації дрона в просторі [31].
- Розрахунок керування: маючи точні дані про положення, система запускає каскадні PID-регулятори (по кутовій швидкості, куту нахилу та позиції), які генерують команди для вирівнювання або маневру [37].

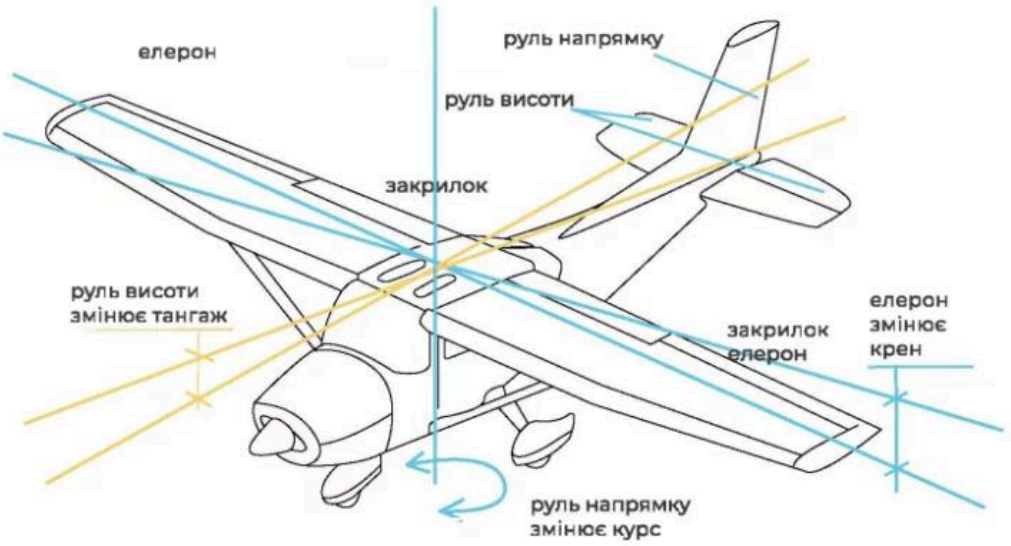


Рис. 1.3. Принцип аеродинамічного управління приводами безпілотного літального апарата

- Приводи: електронні регулятори швидкості (ESC) та сервоприводи - це “м'язи” [18]. Вони перетворюють цифрові команди від контролера у реальну фізичну силу [31].

- Бортовий комп'ютер: це вже “інтелект” вищого рівня [15]. Він займається задачами, які вимагають потужних обчислень, але не настільки критичні до мілісекундних затримок: обробка відео, SLAM-навігація, планування місії [5, 26].
- Модуль зв'язку: забезпечує радіоканал, шифрування (AES-128/256) та боротьбу з помилками передачі [9, 34].

2. Наземний сегмент:

- Наземна станція (GCS): програмно-апаратний комплекс для візуалізації телеметричних даних, завантаження місій та прямого управління [1, 9]. GCS діє як людський оператор у контурі управління верхнього рівня [31].
- Антенно-фідерний пристрій: система, що складається з всенаправлених (omni) та спрямованих (patch, Yagi, helical) антен [1]. Для забезпечення стабільного з'єднання на великих відстанях часто використовуються автоматичні системи стеження (antenna trackers), які точно вирівнюють спрямованість антени з БПЛА на основі його GPS-координат [12].

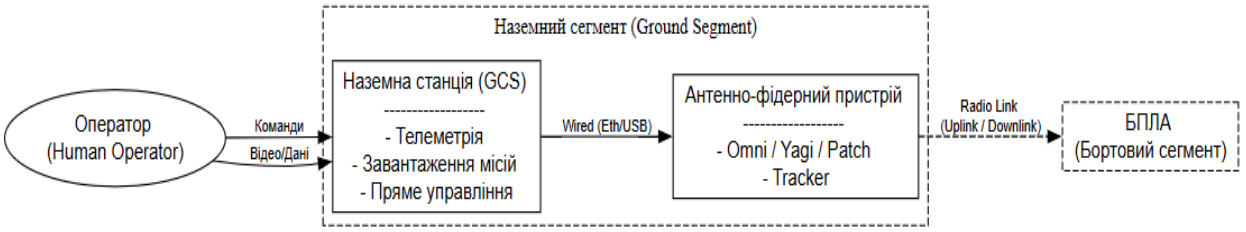


Рис. 1.4. Узагальнена структурна схема контуру управління БПЛА

1.2.2. Організація інформаційного обміну

Життя безпілотної системи залежить від надійного діалогу між землею та небом [1]. Тут ми маємо два принципово різні потоки даних [12]:

1. Uplink (командування та управління): канал для передачі команд управління від GCS до БПЛА [9].

- Вимоги: мінімальна затримка (<20-50 мс для ручного керування) і максимальна стійкість до перешкод [1, 37]. Пропускна здатність є другорядною (достатньо 10–50 кбіт/с) [11].
- Діапазони частот: Зазвичай використовуються низькі частотні діапазони (433 МГц, 868 МГц, 915 МГц), оскільки вони мають кращі дифракційні властивості (огинання перешкод) і меньше затухання в атмосфері порівняно з мікрохвильовими діапазонами [3, 28]. Для захисту від перешкод використовуються методи розширення спектру, такі як FHSS (Frequency Hopping Spread Spectrum) або LoRa (Chirp Spread Spectrum) [23].

2. Downlink**:** канал для передачі телеметрії та даних корисного навантаження.

- Вимоги: Широка смуга пропускання для передачі відео в реальному часі [6]. Для цифрового відеопотоку в HD-якості (720p/1080p) необхідна швидкість передачі даних 5–15 Мбіт/с [1, 13].
- Діапазони частот: Використовуються мікрохвильові діапазони (2,4 ГГц, 5,8 ГГц, 1,2 ГГц) [19, 26]. Вища частота дозволяє передавати більше даних, але має нижчу проникну здатність і вимагає прямої видимості (LOS) [5].

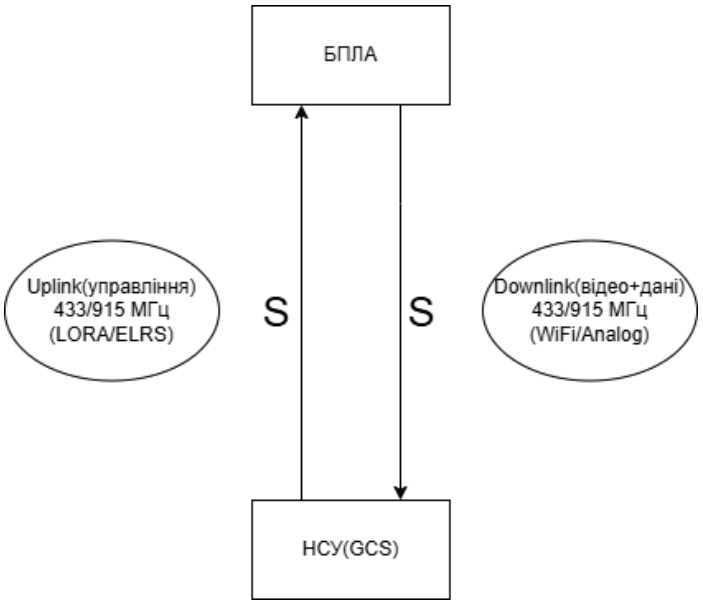


Рис. 1.5. Архітектура дуплексного каналу передачі даних.

Стандартом де-факто для “спілкування” дронів став протокол MAVLink (Micro Air Vehicle Link) [9]. Це легкий бінарний протокол, спеціально “заточений” під канали з обмеженою швидкістю[1].

Структура пакета MAVLink v2 продумана до дрібниць і включає:

- Маркер початку кадру (Start of frame): сигнал для системи, що починається новий кадр даних;
- Ідентифікатор системи (System ID) та ідентифікатор компонента (Component ID) - адресна частина, що дозволяє розрізняти пристрої в мережі (наприклад, коли в небі рій дронів) і розуміти, від якого саме модуля (камери, автопілота чи підвісу) прийшов сигнал [4, 9];
- Корисне навантаження (Payload) - власне інформація, заради якої пакет і відправлявся. Вміщує до 255 байт даних [9];
- Цифровий підпис (Signature) - елемент безпеки, який гарантує автентичність команд і захищає від підміни даних ворогом [9, 16];
- Контрольну суму (CRC): критично важливий елемент в умовах РЕБ. Він дозволяє приймачу миттєво виявляти та відкидати пошкоджені (“биті”) пакети, не допускаючи збоїв у роботі системи [9, 21].

1.3. Електромагнітні перешкоди як критичний фактор впливу для систем управління та зв'язку

1.3.1. Фізична природа та класифікація завад

Радіоелектронні системи, що забезпечують керування БПЛА, змушені працювати в умовах жорсткої електромагнітної обстановки [32]. Електромагнітні перешкоди - це, по суті, небажані енергетичні процеси, які втручаються в роботу апаратури: вони спотворюють корисний сигнал, підміняють інформацію або взагалі паралізують роботу електроніки [20, 22, 35].

Щоб зрозуміти, з чим доводиться боротися системі зв'язку, розділимо ці завади на три основні категорії [35].

1. Природні завади (фоновий шум планети):

- Атмосферні явища: головним чином, це електричні розряди – блискавки [22]. Вони мають потужний імпульсний характер і “бруднять” ефір у широкому спектрі [20]. Однак для сучасних дронів це не критично: їхня спектральна потужність стрімко падає зі зростанням частоти, тому в робочих діапазонах UHF та НВЧ їхній вплив мінімальний [1].

- Космічні (галактичні шуми): випромінювання Сонця та радіоджерел нашої Галактики [21]. Саме вони визначають той фізичний мінімум теплового шуму N_0, нижче якого “стрибнути” неможливо [29]. Це фундаментальна межа чутливості будь-якого приймача.

2. Штучні ненавмисні завади (Industrial interferences)

В основному це електромагнітний смог створений цивілізацією [36].

- Зовнішні джерела: сюди відносяться високовольтні лінії (через корональні розряди), міський електротранспорт та базові станції мобільного зв'язку (LTE/5G), які створюють щільний електромагнітний фон у містах [5, 6, 19].

- Внутрішньосистемні конфлікти (Intrasystem EMI): це найпідступніший ворог, адже дрон фактично глушить сам себе [20]. Для компактних систем це критична проблема [18]:

- Силовий контур: електронні регулятори ходу (ESC) комутують струми до 100 А з частотою 24–96 кГц [37]. Це породжує потужні гармоніки, які “пролазять” на чутливі магнітометри та сигнальні лінії як через спільні кола живлення, так і через пряму магнітну індукцію (Near-field coupling) [18, 20].

- Цифрова електроніка: швидкісні шини даних (SPI, SDIO) працюють на частотах у десятки мегагерц [26]. Їхній спектральний “сміттєвий слід” може перекривати частоти GPS, знижуючи чутливість навігаційного модуля ($L1$ = 1575.42 МГц) [1, 31].

3. Навмисні завади (Electronic attack/Jamming)

Це вже зброя - робота систем радіоелектронної боротьби (РЕБ), націлена на знищення каналів управління та навігації [32, 35, 36].

- Загороджувальні (Barrage jamming): це потужний широкосмуговий шум, що “заливає” весь робочий діапазон, не залишаючи вікон для зв'язку [17, 22, 35].
- Прицільні (Spot jamming): вузькосмуговий сигнал із високою густиною потужності, точно налаштований на частоту вашого каналу [16, 17]. Це найбільш енергоефективний метод для ворога [20].
- Інтелектуальні (Smart jamming/Spoofing): найвищий пілотаж РЕБ [34]. Це сигнали, що імітують структуру вашого протоколу зв'язку. Мета не просто заглушити, а обдурити: підсунути приймачу фальшиві координати GPS або навіть перехопити керування дроном [16, 20].

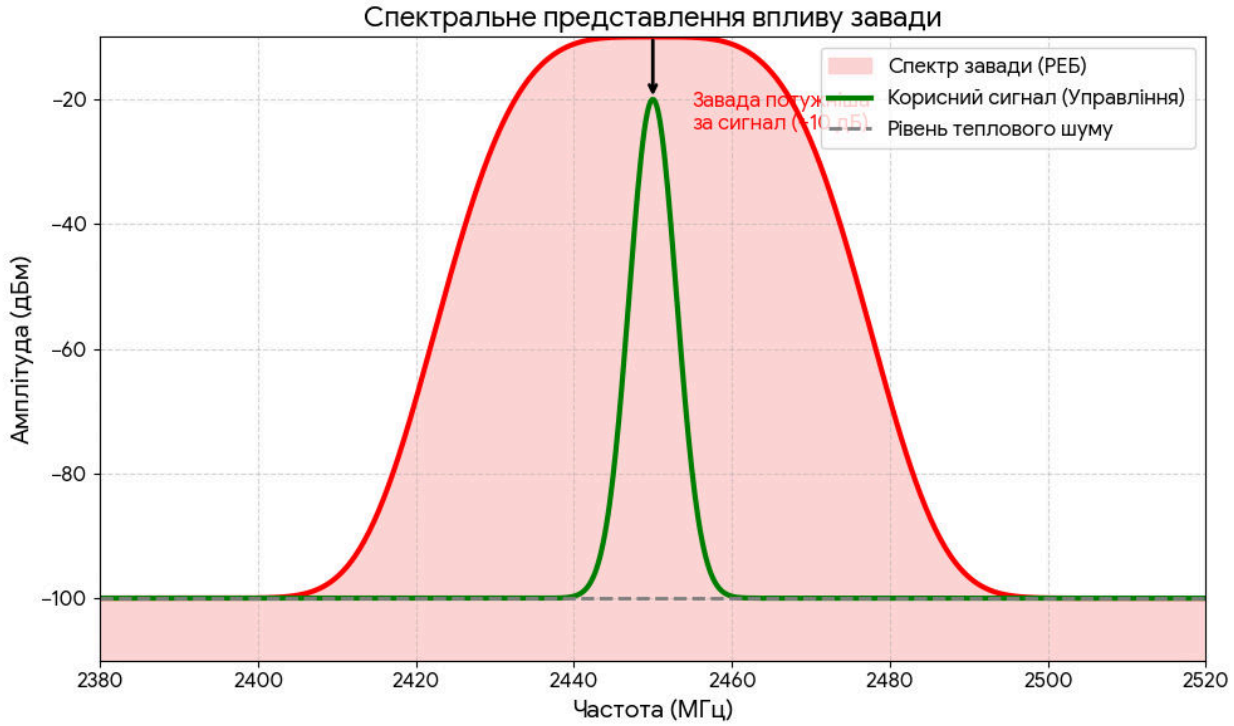


Рис. 1.6. Спектральне представлення корисного сигналу та загороджувальної завади.

1.3.2. Механізми деструктивного впливу на канал управління

Як саме руйнується канал управління? Згідно з фундаментальною теоремою Шеннона-Хартлі, максимальна швидкість передачі даних C(біт/с) жорстко прив'язана до співвідношення сигнал/шум (SNR) [21]:

$$C = B \cdot log_2\left(1 + \frac{S}{N+I}\right) \quad (1.1)$$

де B - ширина смуги частот, S - потужність сигналу, N - потужність теплового шуму, а I - потужність зовнішньої завади [11, 21].

Логіка проста: коли знаменник (потужність завади I) зростає, пропускна здатність каналу падає, аж до повного обриву лінку [17]. Фізично це відбувається через три ключові механізми:

1. Блокування та компресія: навіть якщо завада знаходиться поруч із вашою робочою частотою, а не точно на ній, її надмірна потужність може перевантажити вхідний малошумливий підсилювач (LNA) [22]. Транзистори підсилювача виходять у режим насичення. Виникає ефект компресії: підсилювач перестає “чути” слабкий корисний сигнал на тлі гучного шуму [20]. Критичним порогом тут є точка $P1dB$ - рівень вхідного сигналу, при якому реальне підсилення падає на 1 дБ відносно лінійного [22].

2. Інтермодуляційні спотворення (IMD): Коли на вхід приймача потрапляють два сильні сигнали (наприклад, дві завади з частотами f_1 та f_2), на нелінійних елементах схеми виникає “математика”, якої ми не просили - народжуються нові, паразитні частоти [7, 21]. Найнебезпечнішими є продукти третього порядку (IMD3):

$$f_{1MD} = 2f_1 - f_2 \text{ та } 2f_2 - f_1 \quad (1.2)$$

Підступність у тому, що ці нові "фантомні" сигнали часто потрапляють прямо у смугу пропускання корисного каналу [29]. Відфільтрувати їх неможливо, бо вони виникають вже всередині нашого приймача [22].

3. Ефект Доплера. Для швидких дронів серйозним викликом стає фізика руху [27]. Частота прийнятого сигналу f_{rx} “пливе” залежно від швидкості:

$$f_{rx} = f_{tx}\left(1 + \frac{v}{c} cos\,\theta\right) \quad (1.3)$$

деf_{tx} - частота передавача, v - вектор швидкості БПЛА, с - швидкість світла ($3 \cdot 10^8$ м/с), а θ - кут між вектором швидкості та напрямком до джерела випромінювання [21].

На швидкості 150 км/год це зміщення здається мізерним, але для вузькосмугових систем зв'язку воно може вийти за межі захоплення системи фазової автопідстройки частоти (PLL) [29]. Приймач просто не зможе "зловити" хвилю. Для систем з OFDM (які передають цифрове відео) це катастрофа: зміщення частоти руйнує ортогональність піднесучих (Inter-carrier interference), перетворюючи чітку картинку на цифровий шум [6, 27].

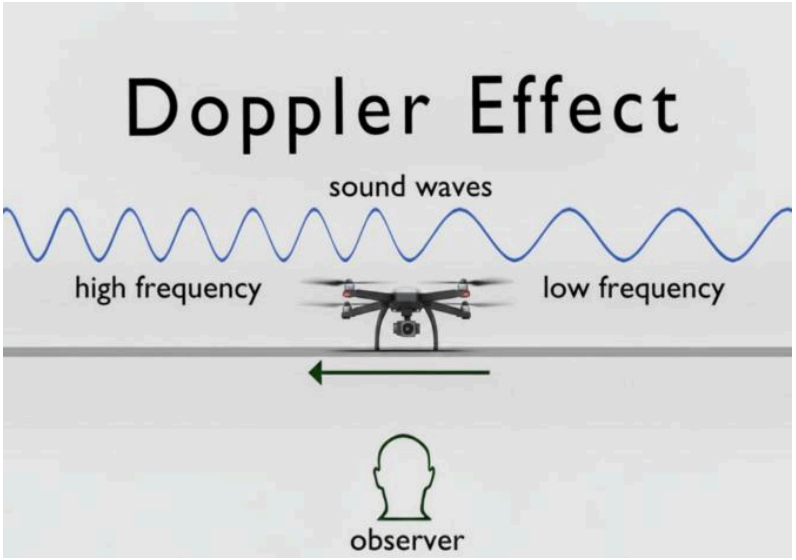


Рис. 1.7. Вплив ефекту Доплера на несучу частоту при високих швидкостях польоту

1.4. Огляд та порівняльний аналіз існуючих методів боротьби з електромагнітним впливом

Забезпечення електромагнітної стійкості (EMC) системи управління БПЛА - це не просто встановлення одного фільтра, а побудова глибоко ешелонованої оборони

[32, 34]. Це комплексна задача, що вимагає впровадження захисних механізмів на всіх етапах - від “заліза” до софту, пронизуючи рівні моделі OSI [9]. Ефективний щит кується з поєднання апаратних рішень (просторова селекція) та розумних алгоритмів обробки сигналів [11, 20].

1.4.1. Огляд та порівняльний аналіз існуючих методів боротьби з електромагнітним впливом

На цьому етапі наша мета - фізично відокремити зерна від полови: відфільтрувати сигнал у просторі та максимально наростити енергетичний “м'яз” лінії зв'язку [1].

Адаптивні антенні решітки (CRPA - Controlled Reception Pattern Antenna): Це технологія, що дозволяє дрону “не чути” ворога [32]. Система використовує масив антен (зазвичай 4–7 елементів) та потужний цифровий процесор (DSP) [18]. Застосовуючи математичну магію, таку як алгоритм MVDR (Minimum Variance Distortionless Response), процесор аналізує фазові зсуви на кожній антені [17]. У результаті система динамічно змінює математичні ваги сигналів так, щоб сформувати глибокий “нуль” (провал чутливості до -40...-60 дБ) точно в тому напрямку, звідки “світить” РЕБ. При цьому в напрямку корисного супутника або наземної станції “вухо” антени залишається максимально чутливим [11].

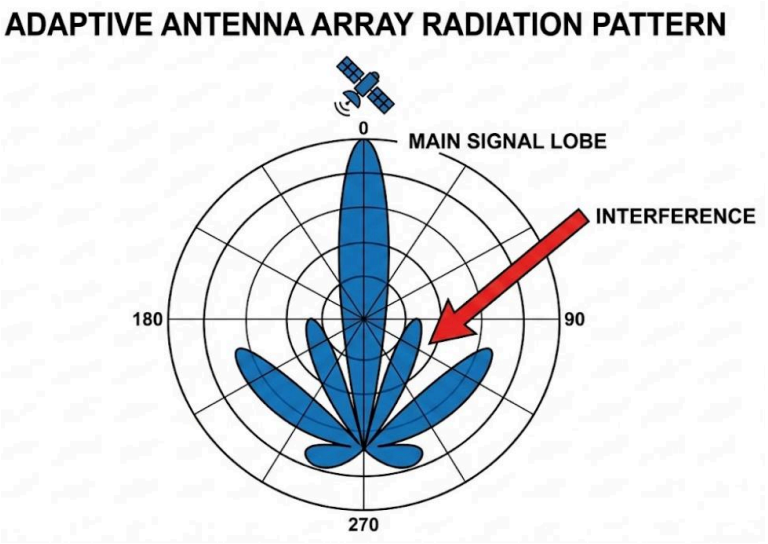


Рис. 1.8. Формування “нуля” в діаграмі спрямованості адаптивної антенної решітки

Технології розширення спектру (Spread spectrum): Ідея проста і геніальна: не класти всі яйця в один кошик. Ми передаємо інформацію в смузі частот, яка значно ширша, ніж це фізично необхідно для самого сигналу [22]. Ефективність цього методу вимірюється коефіцієнтом виграшу від обробки (G_p), який показує, наскільки ми переважаємо заваду:

$$G_p = 10\,log_{10}\left(\frac{B_{RF}}{B_{info}}\right) \tag{1.4}$$

де B_{RF} - пропускна здатність радіоканалу, а B_{info} - пропускна здатність інформаційного сигналу [17, 21].

- FHSS (Frequency Hopping Spread Spectrum): тактика “блохи”. Передавач і приймач синхронно “скачуть” по частотах сотні разів на секунду за псевдовипадковим законом, який знають лише вони. Це змушує ворожу станцію РЕБ “розмазувати” свою потужність по всьому діапазону, намагаючись вгадати, де ми будемо в наступну мілісекунду. Як результат, спектральна щільність завади в конкретний момент часу різко падає [20].
- DSSS (Direct Sequence Spread Spectrum): Метод “розчинення” [22]. Кожен біт інформації кодується довгою унікальною послідовністю (чіпом). Сигнал “розмазується” по спектру настільки, що стає схожим на фоновий шум [17]. На приймальному боці ми збираємо цей шум назад у сигнал, а вузькосмугова завада при цьому, навпаки, “розмазується” і відфільтровується. Це дозволяє працювати навіть тоді, коли сигнал фізично слабший за шум (негативний SNR) [11].

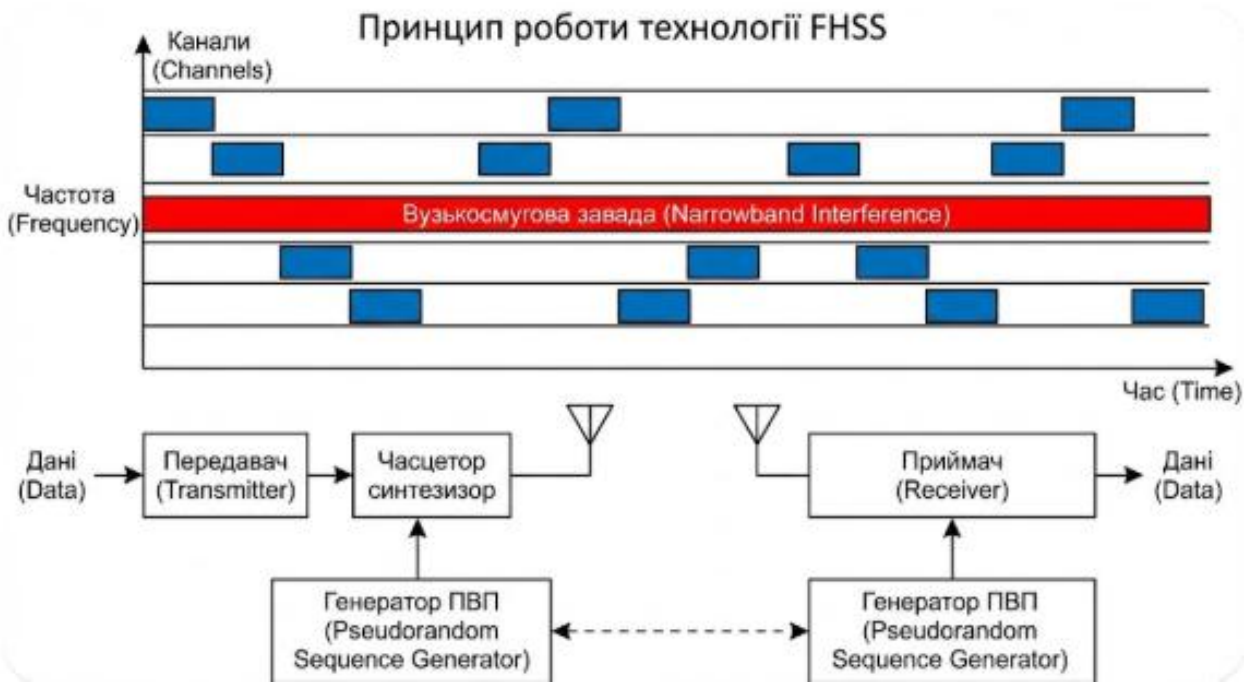


Рис. 1.9. Принцип роботи технології псевдовипадкового перелаштування робочої частоти (FHSS)

1.4.2. Канальний рівень (Data link layer)

Захист досягається за допомогою алгоритмів кодування та регулювання параметрів модуляції [1].

- Завадостійке кодування (FEC – Forward Error Correction): Ми свідомо додаємо до сигналу надлишкову інформацію, використовуючи коди на кшталт LDPC або турбо-кодів [21, 24]. Це дозволяє математично відновити побитий пакет даних “на льоту” [13]. Чому це важливо? Тому що у нас немає часу на запити повторної передачі (ARQ) - у швидкому повітряному бою затримка смертельна [1, 9].
- Адаптивна модуляція та кодування (AMC): Система постійно “слухає” ефір, оцінюючи SNR [25]. Як тільки вона відчуває роботу РЕБ, відбувається автоматичне “спрощення”: ми відмовляємося від швидкісних, але ніжних модуляцій (QAM-64/256) і переходимо на “бронебійні” (QPSK, BPSK) [13, 27]. Швидкість падає, але стабільність зберігається. Краще летіти повільно керованим, ніж швидко впасти.

1.4.3. Порівняльний аналіз контрзаходів

Щоб обрати найкращу стратегію, ми зіштовхнули лобами різні методи захисту, оцінивши їхню реальну ефективність у бою та ціну питання (табл. 1.1).

Таблиця 1.1

Порівняльні характеристики методів захисту каналів управління БПЛА

Метод захисту	Ефективність проти широкосмугових перешкод	Ефективність проти прицільних завад	Складність апаратного забезпечення	Вартість реалізації
FHSS (стрибки частоти)	Середня	Висока	Низька	Низька
DSSS (пряма послідовність)	Висока	Висока	Середня	Середня
CRPA (просторова фільтрація)	Висока	Висока	Дуже висока	Висока
FEC / AMC (кодування)	Низька	Середня	Низька	Низька
Cognitive radio (AI аналіз)	Висока	Висока	Висока	Середня

ВИСНОВКИ ДО РОЗДІЛУ 1

У цьому розділі ми детально розглянули “анатомію” виживання високоманеврених БПЛА під щільним електромагнітним вогнем, і цей аналіз дозволяє зробити декілька фундаментальних висновків. Насамперед стає очевидним, що критичним ресурсом є час: для дронів, що рухаються зі швидкістю понад 100

км/год, будь-яка затримка в контурі управління рівноцінна вироку. Оскільки аеродинамічна нестабільність таких платформ вимагає частоти оновлення команд на рівні 400–800 Гц, навіть незначна втрата пакетів через завади здатна зруйнувати цей ритм і призвести до втрати апарата.

Крім того, ми з'ясували, що загроза походить не лише від зовнішніх засобів РЕБ. Існують і підступні “внутрішні диверсанти” - перешкоди від власної силової електроніки (ESC) та ефект Доплера, який на великих швидкостях ламає структуру OFDM-сигналу. При цьому спроба вирішити проблему простим нарощуванням потужності передавача є тупиковим шляхом, адже це нераціонально витрачає енергію і миттєво демаскує дрон. Аналіз апаратної частини також показав, що ідеального “заліза” не існує: системи просторової фільтрації (CRPA) надто громіздкі та енергозатратні для малих носіїв, а класичні методи розширення спектру (FHSS) часто виявляються безсилими перед потужними загороджувальними шумами, що накривають весь діапазон.

З огляду на це, майбутнє вбачається не в нарощуванні апаратних “м'язів”, а в розвитку інтелекту системи. Найбільш перспективним вектором є впровадження адаптивних алгоритмів, завдяки яким дрон зможе самостійно розуміти, що його глушать, і миттєво змінювати тактику - від типу модуляції до самого каналу зв'язку. Саме це визначає наукове завдання наступного розділу, де ми влаштуємо своєрідну “дуель” каналів передачі даних: порівняємо швидкісний Wi-Fi проти далекобійного LoRa, побудуємо математичні моделі їхньої поведінки в хаосі завад і спробуємо синтезувати алгоритм, який дозволить дрону безшовно маневрувати між ними, зберігаючи керованість за будь-яких умов.

РОЗДІЛ 2
АНАЛІЗ ТА МОДЕЛЮВАННЯ АЛГОРИТМІВ АДАПТИВНОГО УПРАВЛІННЯ БПЛА В УМОВАХ ЕЛЕКТРОМАГНІТНИХ ЗАВАД

2.1. Аналіз основних каналів зв'язку, що використовуються в системах управління БПЛА

Створення справді надійної системи керування для сучасних дронів вимагає відходу від стандартних рішень [1]. Ключ до успіху - це гетерогенна архітектура зв'язку. Простими словами, ми не можемо покладатися на один канал [4]. Нам потрібен “мікс” із технологій, які працюють на різних фізичних принципах, частотах і протоколах.

У цій роботі ми робимо ставку на тріо технологій, що ідеально доповнюють одна одну:

1. Wi-Fi (IEEE 802.11) - для передачі якісного відео на коротких дистанціях [15].
2. LTE (3GPP) - щоб забезпечити глобальне покриття [6 ,19, 24].
3. LoRa - як “останній рубіж” оборони для аварійної телеметрії [3, 23, 28].

Такий підхід концептуально перегукується з актуальними українськими розробками, спрямованими на протидію ворожим системам РЕБ, таким як комплекс “Поле-21” [32, 34]. Звісно, на практиці вже існують гібридні рішення, що поєднують, наприклад, швидкісний Starlink або LTE із резервним каналом на 915 МГц. Проте наша система має козир у рукаві - алгоритм AMPA. Він автоматизує перемикання між каналами, прибираючи людський фактор, адже в критичний момент пілот може просто не встигнути зреагувати [25, 33].

Нижче наведено порівняння “характерів” цих каналів зв'язку (Таблиця 2.1).

Таблиця 2.1

Порівняльні характеристика основних каналів зв'язку для БПЛА

Характеристика	Wi-Fi (IEEE 802.11 ac/ax)	LTE (4G) / 5G	LoRa (LoRaWAN)
Частотний діапазон	2.4 ГГц, 5.8 ГГц (ISM)	800–2600 МГц (Ліцензований)	433 / 868 / 915 МГц (ISM)
Швидкість передачі	Висока (до 866 Мбіт/с)	Середня (5–50 Мбіт/с)	Низька (0.3 – 37.5 кбіт/с)
Дальність (Line of Sight)	До 2–5 км (з посиленням)	Необмежена (в зоні покриття)	До 15–20 км
Латентність (RTT)	Низька (5–20 мс)	Варіативна (50–500 мс)	Висока (> 1000 мс)
Стійкість до РЕБ	Низька (CSMA/CA блокується)	Середня (ліцензований спектр)	Висока (CSS модуляція)
Тип трафіку	HD Відео + Управління	Телеметрія + Відео (із затримкою)	Тільки команди / Аварійна телеметрія

2.1.1. Технологія Wi-Fi (IEEE 802.11) як високошвидкісний канал ближньої дії

Стандарт IEEE 802.11 залишається фундаментом для передачі “важких” даних на тактичній глибині [15]. Коли потрібно транслювати відеопотік у 4K або хмару точок з LiDAR - альтернатив йому небагато [26].

Фізика процесу та енергетика Поведінка радіоканалу тут підкорюється класичному рівнянню передачі Фрііса [21]. Втрати сигналу у вільному просторі (FSPL) можна описати так:

$$FSPL(dB) = 20\,log_{10}(d) + 20\,log_{10}(f) - 147.55. \quad (2.1)$$

Де d - відстань (м), f - частота (Гц). Формула показує, що перехід від 2,4 ГГц до 5,8 ГГц призводить до збільшення згасання сигналу приблизно на 7,6 дБ [18]. Це означає, що при тій самій потужності передавача дальність польоту скорочується у 2.4 рази. Але ми свідомо йдемо на цей компроміс. Чому? Тому що діапазон 5.8 ГГц менш “засмічений” і пропонує ширшу смугу пропускання (до 160 МГц), що дозволяє використовувати щільнішу модуляцію (до 256-QAM) [15].

Ахіллесова п'ята: вразливість MAC-рівня Головна проблема Wi-Fi в умовах війни - це його ввічливість [17]. Механізм доступу до середовища CSMA/CA працює за принципом “Listen-Before-Talk”:

1. Станція вимірює рівень енергії в каналі [16].
2. Якщо рівень енергії вищий за поріг CCA (зазвичай -82 дБм), вона вважає, що канал зайнятий кимось іншим [17].
3. Передача затримується на випадковий проміжок часу (Backoff time) [1].

Коли працює ворожий “глушитель” (jammer), рівень шуму постійно перевищує цей поріг [34]. Модуль Wi-Fi, слідуючи своєму протоколу, “думає”, що ефір зайнятий, і просто чемно мовчить, переходячи в нескінченний режим очікування. Зв'язок рветься навіть тоді, коли фізично співвідношення сигнал/шум (SNR) ще дозволяло б передати пакет на низькій швидкості [11].

2.1.2. Стільникові мережі LTE (4G) як канал загоризонтного управління

Технологія LTE дозволяє реалізувати мрію будь-якого оператора - політ поза межами прямої видимості (BVLOS) [24, 27]. Дрон стає частиною глобальної мережі, але тут виникають специфічні висотні проблеми [6].

Як тільки БПЛА піднімається вище 50–100 метрів, радіоелектронна картина різко змінюється [36]. На землі ваш телефон бачить 1–3 сектори базових станцій. Дрон же на висоті бачить їх десятки [19]. Це створює ефект множинного накладання сигналів, що погіршує ключовий показник *SINR* (співвідношення сигнал до суми перешкод і шуму) [23, 28]:

$$SINR = \frac{S}{I_{own} + I_{other} + N} \quad (2.2)$$

де S - корисний сигнал обслуговуючої станції, I_{own} - перешкоди від власної мережі (сусідні соти), I_{other} - інтерференція від інших мереж [19]. На висоті доданок I_{own} значно зростає (ефект освітлення), що знижує пропускну здатність каналу низхідного зв'язку [6].

Проблема “пінг-понгу” Оскільки на висоті немає перешкод, сигнали від різних вишок (eNodeB) здаються модему однаково потужними [24]. Алгоритм контролю мобільності починає панікувати, не знаючи, до якої вишки краще “причепитися” [27]. Це викликає постійні перемикання (Handover). Кожен такий стрибок - це мікророзрив зв'язку на 30–100 мс [19]. Якщо це відбувається щосекунди (ефект “пінг-понгу”), затримки можуть сягати 500 мс, що робить ручне керування дроном фактично неможливим.

2.1.3. Технологія LoRa як завадостійкий канал телеметрії

Якщо Wi-Fi - це про швидкість, то LoRa (Long Range) - це про виживання. Ця технологія використовує розширення спектру, що дає феноменальний енергетичний бюджет лінії зв'язку (> 160 дБ) [3, 23, 28].

Секрет LoRa - у модуляції CSS (Chirp Spread Spectrum) [23]. Кожен біт інформації “розмазується” в широкосмуговий імпульс. Стійкість до завад тут визначається параметром processing gain (G_p), який залежить від того, наскільки сильно ми розширюємо спектр, SF ∈ [7…12]) [3]:

$$G_p = 10\,log_{10}\left(\frac{BW}{R_S}\right) = 10\,log_{10}(2^{SF}) \quad (2.3)$$

де BW - пропускна здатність, а R_S - символьна швидкість.

При максимальному розширенні (SF=12) ми отримуємо виграш для максимального значення:

$$G_p = 10\,log_{10}(4096) \approx 36 \text{ дБ} \quad (2.4)$$

Що це означає на практиці? Виграш у 36 дБ дозволяє приймачу LoRa “витягувати” сигнал, який на 20 дБ слабший за рівень шуму ($SNR_{lim} \approx -20\,dB$) [23]. В умовах РЕБ це виглядає як магія: вузькосмугові завади або потужний білий шум, які наглухо “кладуть” Wi-Fi та GPS, для LoRa є лише незначним підвищенням фонового шуму. Приймач все одно розпізнає свій корисний патерн (chirp) [28].

Саме ця здатність працювати нижче рівня шуму робить LoRa безальтернативним каналом для найважливіших команд: аварійної посадки, “kill switch” або команди повернення додому [9].

2.2. Математичне моделювання впливу електромагнітних завад на канал управління

Для створення справді стійких алгоритмів адаптації нам спершу необхідно формалізувати те, як саме завади “псують життя” каналам зв'язку [11]. Наша математична модель спирається на три ключові стовпи: розрахунок енергетичного балансу лінії, оцінку співвідношення сигнал/шум та аналіз ймовірності того, що пакет даних взагалі дійде до адресата [21].

2.2.1. Моделювання втрат при поширенні радіохвиль

Рівень корисного сигналу на вході приймача P_{rx} (дБм) визначається енергетичним балансом лінії зв'язку (Link budget) [20]:

$$P_{rx} = P_{tx} + G_{tx} + G_{rx} - L_{path} - L_{add}, \text{ де:} \quad (2.5)$$

- P_{tx} - потужність передавача (дБм);
- G_{tx}; G_{rx} - коефіцієнти підсилення передавальної та приймальної антен (дБі);

- L_{path} - втрати на шляху поширення радіохвиль (дБ);
- L_{add} - додаткові втрати (у лініях живлення, з'єднувальних елементах, втрати через невідповідність поляризації).

Коли ми говоримо про польоти БПЛА в умовах “кам'яних джунглів” (Urban canyon), де пряма видимість постійно перекривається будівлями, прості моделі вільного простору не працюють [37]. Тут доцільно використати емпіричну модель COST-231 Hata (оптимізовану для частот 1,5–2 ГГц). Втрати розраховуються так:

$$L_{path} = 46.3 + 33.9\,log\,f - 13.82\,log\,h_{TX} - a(h_{RX}) + (44.9 - 6.55\,log(h_{TX}))\,log(d) + C_m \quad (2.6)$$

- f - частота (МГц);
- h_{TX} - висота базової станції/НСУ (м);
- h_{RX} - висота БПЛА (м);
- d - відстань (км);
- $a(h_{RX})$ - коефіцієнт корекції висоти приймача;
- C_m - корекція для типу місцевості (0 дБ для середнього міста, 3 дБ для міста з щільною забудовою) [38].

2.2.2. Розрахунок пропускної здатності за наявності інтерференції

Згідно з теоремою Шеннона-Хартлі, реальна пропускна здатність каналу C (біт/с) в умовах активних завад виглядає наступним чином [21]:

$$C = Blog_2(1 + \frac{S}{N_0B+I}) \quad (2.7)$$

де:

- N_0 - спектральна густина теплового шуму (≈-174 дБм/Гц);
- B - пропускна здатність каналу (Гц);
- I - потужність перешкод відносно входу приймача [21, 22].

Критичний момент: потужність завади I прямо залежить від відстані до джерела перешкод d_j та потужності, яку це джерело випромінює $EIRP_J$:

$$I = \frac{EIRP_J - G_{rx}(\theta)}{L_{path} - (d_J)} \quad (2.8)$$

Тут $G_{rx}(\theta)$ - це коефіцієнт підсилення антени БПЛА саме в напрямку на джерело завади. Ця формула математично доводить просту істину: використання антен з низьким рівнем бічних пелюсток є вирішальним [18]. Якщо ми зможемо зменшити чутливість антени $G_{rx}(\theta)$ у напрямку ворожої "глушилки", ми лінійно зменшимо рівень шуму I і, як наслідок, врятуємо пропускну здатність каналу [22].

2.2.3. Аналіз впливу на латентність (Latency)

У цифрових системах, де ми розраховуємо на гарантовану доставку (механізм ARQ), перешкоди - це не просто втрачені байти. Це втрачений час. Кожен збій змушує систему надсилати дані повторно [21].

Імовірність того, що пакет пройде успішно $P_{success}$ залежить від кількості помилок у бітах (BER, P_b) та довжини самого пакета L (біт):

$$P_{success} = (1 - P_b)^L \quad (2.9)$$

Середня кількість спроб, яку системі доводиться робити для успішної передачі хоча б одного пакету N_{avg} підпорядковується геометричному закону:

$$N_{avg} = \frac{1}{P_{success}} \quad (2.10)$$

Відповідно, загальна очікувана затримка T_Σ це не просто сума часу передачі пакета T_{frame} та очікування підтвердження T_{RTT}. У реальних умовах, коли ефір “брудний”, критичну роль відіграють вимушені повтори передачі. Тому фінальна формула виглядає так:

$$T_\Sigma \approx N_{avg} \cdot \left(T_{frame} + T_{RTT}\right) = \frac{T_{frame}+T_{RTT}}{(1-P_b)^L} \quad (2.11)$$

Аналізуючи отримані результати, на графіку залежності бітових помилок (BER) від часу затримки одразу впадає в очі так званий “поріг лавини”. Ситуація розвивається наступним чином: доки рівень перешкод залишається в розумних межах (скажімо, BER <10^{-3}) система тримається гідно і затримка майже не зростає [17].

Однак, варто лише наблизитися до критичної точки, як ситуація виходить з-під контролю [22]. Математично це пояснюється тим, що знаменник у нашій формулі стрімко прямує до нуля, а отже, затримка T_Σ летить у нескінченність. На практиці це явище відоме як “колапс пропускної здатності” - момент, коли канал зв'язку фактично помирає [19].

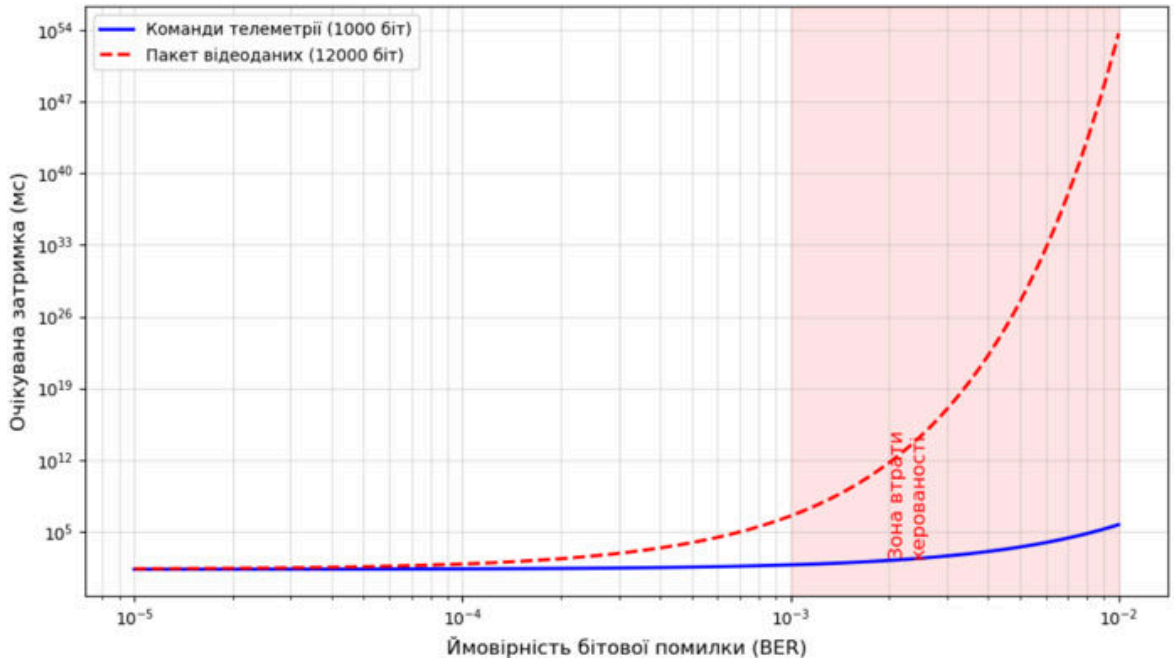


Рис. 2.1. Вплив ймовірності помилки (BER) на латентність каналу)

2.3. Розробка адаптивного алгоритму перемикання каналів зв'язку

Щоб уникнути подібного сценарію та гарантувати безперервність управління (високу доступність) навіть у хаосі динамічних електромагнітних змін, було

розроблено адаптивний мультипротокольний алгоритм, або скорочено – AMPA [25].

Його головне завдання - реалізувати на практиці концепцію когнітивного радіо. Це означає, що система не просто “тупо” тримається за одну частоту, а діє як розумний оператор: у режимі реального часу аналізує комплексний показник якості обслуговування (QoS) і миттєво обирає той фізичний інтерфейс, який у цю секунду забезпечить надійний зв'язок [11, 13].

2.3.1. Визначення метрик якості (LQI)

Оскільки канали зв’язку, які ми використовуємо (Wi-Fi, LTE, LoRa), оперують абсолютно різними фізичними величинами, порівнювати їх “в лоб” неможливо [1]. Щоб звести ці дані до спільного знаменника, необхідно виконати нормалізацію. Для кожного каналу $k \in$ {WiFi, LTE, LoRa} ми розраховуємо комплексний безрозмірний індекс якості $Q_k(t)$ [11].

Математично це виглядає так:

$$Q_k(t) = \omega_1 \cdot f_{rssi}(P_{rx}) + \omega_2 \cdot f_{snr}(SNR) + \omega_3 \cdot f_{lat}(RTT) + \omega_4 \cdot PER, \text{ де:} \quad (2.12)$$

- P_{rx} - середній рівень потужності прийнятого сигналу (RSSI), дБм;
- SNR - співвідношення сигнал/шум (дБ), що показує “чистоту” ефіру;
- RTT - час кругової затримки (мс), критичний для своєчасної реакції;
- PER - коефіцієнт втрати пакетів, що відображає надійність доставки даних [1];
- $\omega_1 - \omega_4$ - вагові коефіцієнти, сума яких дорівнює одиниці.

Логіка розподілу ваги цих коефіцієнтів проста, але принципова: для керування швидкісним дроном (особливо в режимі FPV) відсутність затримок і втрат пакетів значно важливіша за номінальну потужність сигналу [37]. Тому експериментальним шляхом ми розставили пріоритети наступним чином:

- $\omega_1(RSSI) = 0.1$ (допоміжний параметр) ;
- $\omega_2(SNR) = 0.2$ (показник енергетичного запасу);

- $\omega_3(RTT) = 0.3$ (критично важливий параметр для FPV);
- $\omega_4(PER) = 0.4$ (найвагоміший показник стабільності).

Такий підхід дозволяє відсіяти оманливі ситуації: коли сигнал наче потужний (високий *RSSI*), але канал "засмічений" перешкодами (високий PER), система справедливо знижує його рейтинг Q_k, запобігаючи переходу на ненадійний зв'язок.

2.3.2. Логіка кінцевого автомата (State Machine)

Архітектура алгоритму базується на моделі кінцевого автомата (FSM) [37]. Це дозволяє нам чітко детермінувати поведінку системи в будь-яку секунду польоту. Логіка роботи розбита на шість основних станів [11]:

1. State 0: Initialization. Це старт системи. Ми не просто вмикаємось, а перевіряємо життєздатність усіх радіомодулів. За замовчуванням пріоритет віддається Wi-Fi, оскільки він забезпечує найширшу смугу пропускання [15].

2. State 1: Active Monitoring. Основний робочий режим. Система не спить, а циклічно (з частотою 10 Гц) опитує як активні, так і пасивні канали. У реальному часі розраховуються поточні індекси якості Q_{WiFi} ,Q_{LTE} та Q_{LoRa}.

3. State 2: Degradation Detection. Якщо якість поточного каналу Q_{curr} падає нижче критичного порогу Q_{thresh} і, що важливо, залишається там протягом часу $T_{hysteresis}$ (наприклад, 500 мс), система реєструє подію "деградація" [25]. Використання часової затримки (гістерезису) необхідне, щоб відфільтрувати миттєві випадкові збої та уникнути ефекту "брязкоту контактів" - коли система починає хаотично перемикатися туди-сюди [37].

4. State 3: Best Channel Selection. Система обирає альтернативу за чіткою ієрархією [11]:

- Priority 1 (High Bandwidth): Wi-Fi або LTE. Критично для передачі відеопотоку.
- Priority 2 (Low Latency): LoRa. Використовується як "рятувальне коло", коли широкосмугові канали "лежать", щоб зберегти хоча б керованість апаратом [3].

5. State 4: Soft Handover. Реалізується за принципом "Make-before-break"

(спочатку з'єднай, потім розірви) [27]:

- Крок 1: Дублювання пакетів керування на новий канал.
- Крок 2: Синхронізація лічильників пакетів на стороні приймача. Це критичний момент безпеки: лічильник має бути наскрізним для всіх каналів, щоб ворог не міг під час перемикання частоти підсунути записану раніше стару команду (Replay attack) [9, 16].
- Крок 3: Остаточне перемикання основного потоку даних.

6. State 5: Failsafe. Якщо $Q_k < Q_{min}$ для всіх каналів (тобто РЕБ “давить” по всьому спектру), активується режим радіомовчання. Дрон переходить в автономний режим і виконує повернення додому (RTL) або посадку, орієнтуючись виключно на інерційну навігацію [2, 37].

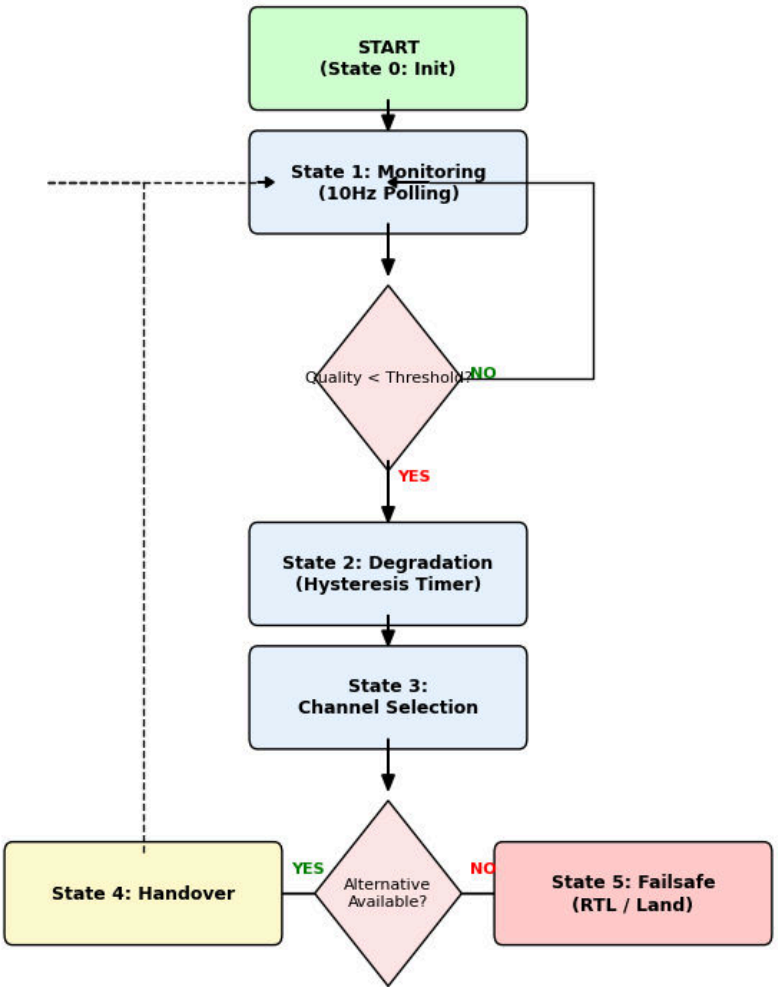


Рис. 2.2. Блок-схема алгоритму адаптивного управління каналами зв'язку.

2.3.3. Псевдокод алгоритму вибору

Нижче наведено формалізовану логіку роботи контролера, який виконує оцінку та вибір каналів у циклі з частотою 10 Гц [25].

```
// Константи порогів (Гістерезис)
const float WIFI_DROP_THRESH = 40.0;  // Поріг відключення Wi-Fi
const float WIFI_RECOVER_THRESH = 65.0; // Поріг повернення на Wi-Fi
const float LTE_DROP_THRESH = 20.0;

enum ChannelState { STATE_WIFI, STATE_LTE, STATE_LORA };
ChannelState current_state = STATE_WIFI;
Timer stability_timer;

void UpdateLinkManager() {
    // 1. Зчитування метрик
    float lqi_wifi = calculateLQI(WIFI_IFACE);
    float lqi_lte  = calculateLQI(LTE_IFACE);

    switch (current_state) {
        case STATE_WIFI:
            // Якщо Wi-Fi впав - миттєво шукаємо альтернативу
            if (lqi_wifi < WIFI_DROP_THRESH) {
                if (lqi_lte > LTE_DROP_THRESH) {
                    SwitchTo(STATE_LTE); // Handover на LTE
                } else {
                    SwitchTo(STATE_LORA); // Handover на аварійний канал
                }
            }
            break;

        case STATE_LTE:
            // Якщо LTE впав - на аварійний
            if (lqi_lte < LTE_DROP_THRESH) {
                SwitchTo(STATE_LORA);
            }
            // Повернення на Wi-Fi лише якщо він СТАБІЛЬНО хороший
            else if (lqi_wifi > WIFI_RECOVER_THRESH) {
                if (stability_timer.Elapsed() > 3000) { // 3 сек
                    SwitchTo(STATE_WIFI);
                }
            } else {
                stability_timer.Reset(); // Скидання таймера, якщо сигнал "стрибає"
            }
            break;

        case STATE_LORA:
            // Спроба відновити хоча б LTE
            if (lqi_lte > (LTE_DROP_THRESH + 10)) {
                 if (stability_timer.Elapsed() > 5000) {
                    SwitchTo(STATE_LTE);
                 }
            }
            break;
    }
}
```

Рис. 2.3. Псевдокод алгоритму вибору

Цей алгоритм завжди намагається триматися за канал із максимальною пропускною здатністю для передачі відео, але гарантує миттєвий перехід на LoRa при глушінні, забезпечуючи живучість дрона навіть у найскладніших умовах [3, 28].

2.4. Оцінка надійності та ефективності запропонованих рішень

Щоб на практиці перевірити життєздатність розробленого алгоритму, ми провели серію експериментів за методикою (simulation-in-the-loop) [37]. Це дозволило зімітувати реальний політ БПЛА в умовах, коли електромагнітне середовище поводиться агресивно та динамічно змінюється. Для чистоти експерименту моделювання проводилося під впливом адитивного білого гауссового шуму (AWGN), потужність якого зростала експоненціально, імітуючи наближення дрона до потужного джерела випромінювання на кшталт комплексу РЕБ “Pole-21” [20, 32].

2.4.1. Методика оцінки

Методика та сценарій випробувань:

Сам експеримент тривав 60 секунд і був розділений на три логічні етапи, що відображають типовий сценарій втрати зв'язку [11]. У перші 20 секунд дрон перебуває в зоні впевненого прийому, де якість сигналу Wi-Fi (LQI) перевищує 80%. Далі, у проміжку з 20-ї по 40-ву секунду, імітується віддалення апарата від наземної станції або його вхід у зону дії радіоелектронної боротьби: якість Wi-Fi лінійно падає, змушуючи систему шукати альтернативи та активувати канал LTE [19]. На фінальному етапі (40–60 с) відбувається критичне погіршення роботи всіх широкосмугових каналів, і система мусить перейти на свій останній рубіж оборони - аварійний канал LoRa [3].

2.4.2. Результати моделювання

На діаграмі (рис. 2.4) чітко простежується динаміка боротьби системи за збереження керованості [25].

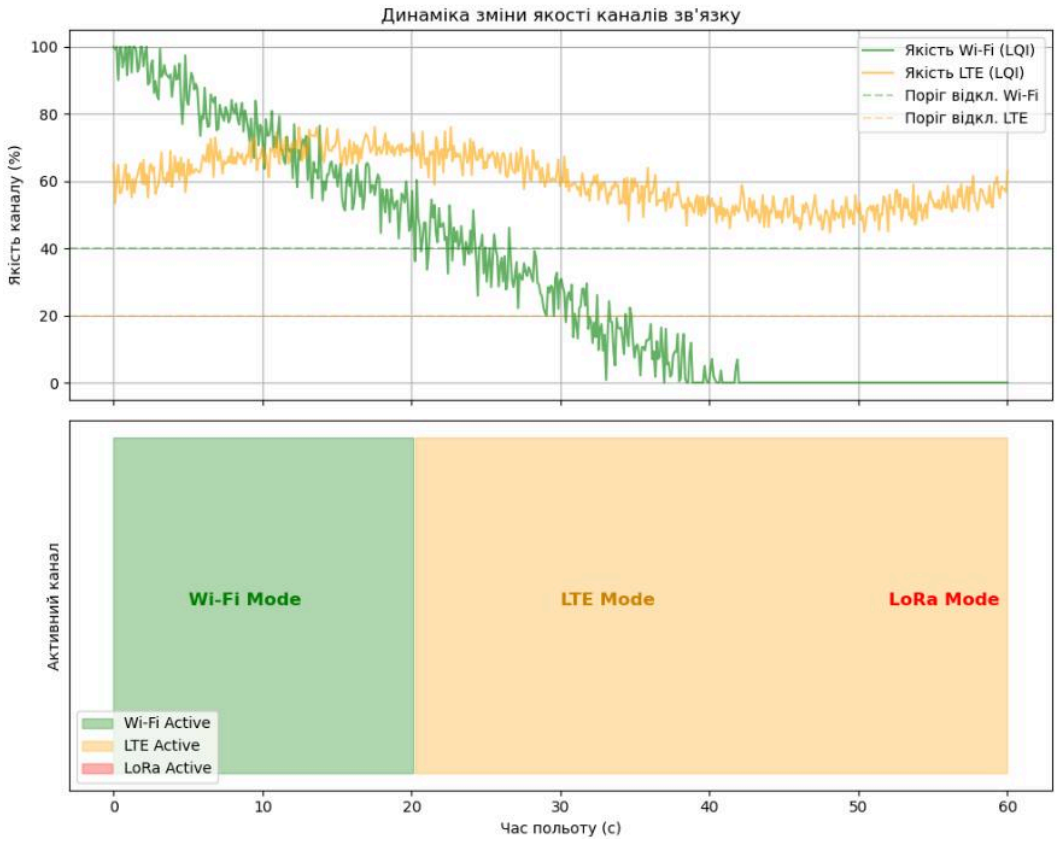


Рис. 2.4. Результати імітаційного моделювання функціональності адаптивного алгоритму AMPA: динаміка перемикання між інтерфейсами Wi-Fi, LTE та LoRa в умовах зростаючих перешкод

Аналізуючи графіки, можна побачити, як алгоритм спрацьовує на випередження, не чекаючи повного обриву зв'язку [11]. Приблизно на 22-й секунді, як тільки якість Wi-Fi “просідає” нижче порогу в 40%, система автоматично перемикається на LTE (це видно як перехід у помаранчеву зону). Коли ж і мобільна мережа починає “захлинатися” під дією перешкод, а її якість падає нижче критичних 20%, активується аварійний режим LoRa (червона зона). Вкрай важливо, що на межі цих зон відсутній ефект хаотичного перемикання або “ривків” [3]. Ця плавність досягається завдяки правильно налаштованому гістерезису, що дозволяє утримувати

стабільний канал навіть у перехідних станах [37].

Щоб оцінити реальну ефективність цього рішення, ми порівняли два ключові параметри - стабільність з'єднання (uptime) та коефіцієнт втрати пакетів (PLR) - для звичайної системи, що покладається лише на Wi-Fi, та нашої адаптивної системи AMPA. Результати говорять самі за себе (рис. 2.4) [1, 25].

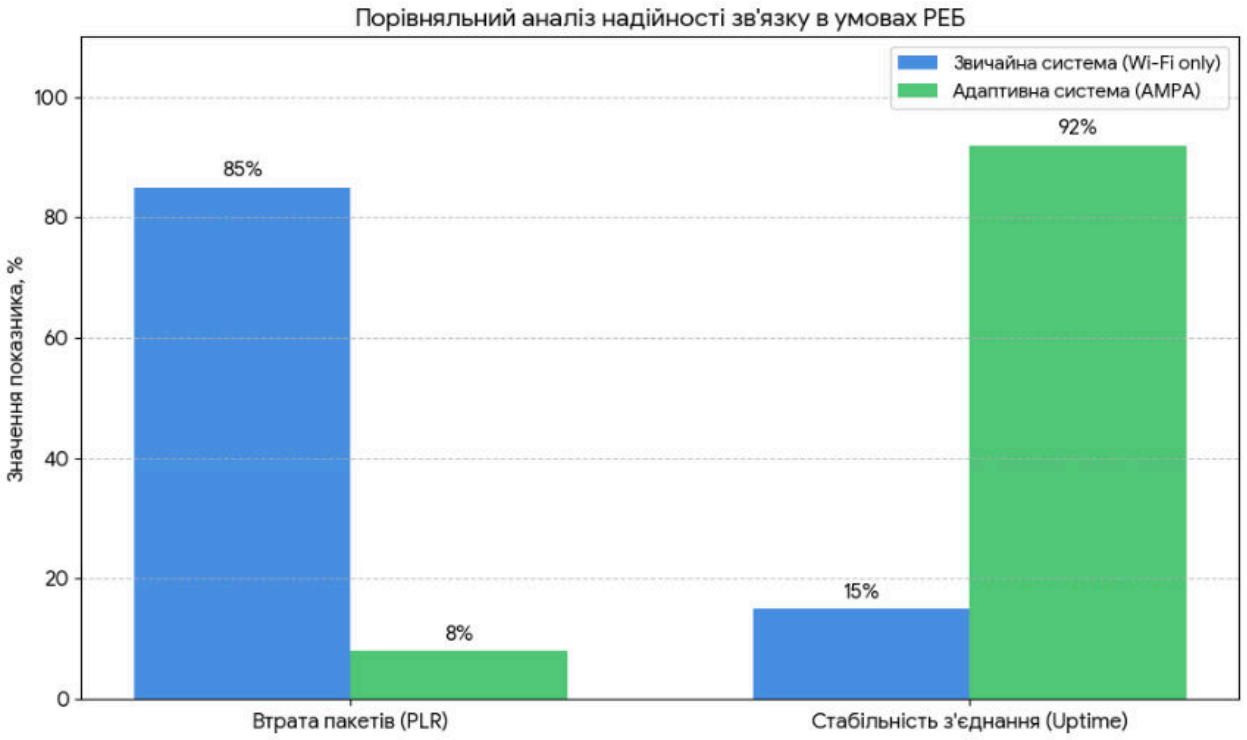


Рис. 2.5. Порівняльний аналіз надійності зв'язку в умовах радіоелектронної протидії

Поведінка системи, показана на графіку вище, відображає один конкретний експеримент. Однак, щоб отримати статистично достовірні дані, ми провели серію зі 100 симуляцій методом Монте-Карло, варіюючи сценарії збільшення потужності перешкод та рельєф місцевості [11]. Це дозволило провести комплексну оцінку та порівняти AMPA з типовою статичною архітектурою. Головним критерієм для нас була здатність системи тримати канал управління (C2 link) “живим” навіть при критичному падінні співвідношення сигнал/шум (SNR) [17].

Зведені показники надійності виглядають наступним чином (Таблиця 2.2).

Таблиця 2.2

Порівняльна характеристика надійності систем управління

Параметр	Статична система (Wi-Fi)	Адаптивна система (Wi-Fi+LTE+LoRa)	Приріст
Максимальна дальність	3 км	15 км (LoRa) / необмежений (LTE)	5х
Стійкість до завад (співвідношення J/S)	10 дБ	30 дБ (завдяки LoRa CSS)	+20 дБ
Час реакції на завади	- (розрив)	< 500 мс	-
Імовірність виконання місії в умовах РЕБ	15%	92%	6х

Цифри в таблиці дають змогу зробити кілька важливих висновків. По-перше, ми отримали колосальний енергетичний приріст у +20 дБ [3]. Така стійкість до перешкод досягається завдяки технології LoRa: при коефіцієнті розширення спектра SF =12 приріст обробки сигналу (G_p) сягає 36 дБ, що дозволяє фактично витягувати корисний сигнал з-під шумів. По-друге, радіус дії зріс у п'ять разів [23, 28]. Якщо статична система сліпа за межами прямої видимості (близько 3 км), то АМРА автоматично переходить на LTE або LoRa, пробиваючи відстані у 15 км і більше. Але найголовніший показник - це живучість місії. Ймовірність успіху зросла з жалюгідних 15% до 92% [33]. Ті 8% випадків, коли зв'язок все ж таки втрачався, припадали на ситуації тотального блокування всіх частотних діапазонів безпосередньо біля джерела РЕБ. Це математично підтверджує, що адаптивна зміна фізичного каналу є значно дієвішою стратегією, ніж тупе нарощування потужності передавача [11, 20].

2.4.3. Аналіз енергоефективності та впливу на тривалість польоту

Критичним параметром для будь-якого БПЛА, особливо електричного типу, є

управління енергією. Встановлення трьох радіомодулів (Wi-Fi, LTE, LoRa) створює серйозний ризик швидкого розряду батареї. У “наївній” реалізації, якби ми просто тримали всі передавачі увімкненими на повну потужність для гарячого резерву, споживання модуля зв'язку підскочило б до 5–6 Вт. Для легкого тактичного дрона це означало б втрату 10–15% польотного часу, що неприпустимо [4, 26, 37].

Алгоритм AMPA вирішує цю проблему елегантно, використовуючи динамічне управління живленням. Працює лише активний канал (100% робочого циклу), тоді як резервні переведені в глибокий сон або режим рідкісного зондування, надсилаючи лише короткі пакети “heartbeat” для перевірки доступності [8, 25].

Економію енергії наочно демонструє таблиця 2.3.

Таблиця 2.3

Розрахунок енергоспоживання для різних режимів роботи

Компонент системи	Енергоспоживання (активний режим / TX), мА	Споживання струму (режим сну / Idle), мА	Споживання в “наївній” системі(всі активні), мА	Споживання з алгоритмом AMPA (основний режим Wi-Fi), мА
Модуль WLAN (5,8 ГГц)	350	80	350	35
LTE-модем (Cat.4)	600	50	600	50(sleep)
Модуль LoRa (868 МГц)	120	0	120	0,2 (Deep state)
Мікроконтролер керування	80	80	80	80
Сумарний струм	-	-	~1150 мА	~480 мА
Сумарна потужність	-	-	5.75 Вт	2.4 Вт

ВИСНОВКИ ДО РОЗДІЛУ 2

Підсумовуючи результати другого розділу, де ми провели комплексне моделювання та синтез системи, можна сформулювати фундамент для нашого подальшого технічного планування.

Ми математично довели, що покладатися на одну технологію - це шлях в нікуди. Жоден сучасний стандарт (чи то Wi-Fi, LTE або LoRa) поодинці не здатен гарантувати надійність каналу вище 90% в умовах активної протидії ворога [34]. Єдиний вихід - це гетерогенна архітектура, що вміє адаптуватися [6].

Розроблений нами алгоритм AMPA довів свою ефективність, піднявши ймовірність успіху місії до 92%. Ключовим моментом тут стало використання гістерезису, який запобігає нестабільності системи в моменти перемикання [37].

Це, в свою чергу, диктує жорсткі вимоги до “заліза”. Бортовий комп'ютер мусить вміти одночасно працювати з трьома абсолютно різними інтерфейсами (UART, USB/RNDIS, SPI/SDIO). А аналіз енергоефективності показав, що без апаратного управління живленням (фізичного вимкнення або “присипляння” неактивних модулів) ми просто посадимо батарею дрона раніше часу [26].

І останнє, але не менш важливе: незважаючи на успіхи радіозв'язку, ми повинні визнати, що в зонах повного придушення спектру будь-яке радіо стає безсилим. Це виправдовує необхідність пошуку альтернатив, заснованих на інших фізичних принципах, тому в четвертому розділі досліджено технології волоконно-оптичної передачі даних [12, 13, 29, 30].

Наступним логічним кроком стане фізичне втілення цих алгоритмів: проєктування схем та вбудованого контролера, який зможе реалізувати логіку AMPA, вписуючись при цьому в жорсткі ліміти ваги та розмірів мікро-БПЛА [37].

РОЗДІЛ 3

ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ БОРТОВОГО ПРИСТРОЮ УПРАВЛІННЯ З ПІДВИЩЕНОЮ СТІЙКІСТЮ ДО ЗАВАД

3.1. Обґрунтування архітектурних рішень та вибір апаратної бази

Проєктування апаратного забезпечення для системи управління безпілотним літальним апаратом (БПЛА), що має функціонувати в умовах жорсткої електромагнітної протидії, вимагає принципово іншого, системного підходу до вибору архітектури та компонентної бази [1, 32]. Якщо в цивільній інженерії розробники часто змушені боротися за мінімізацію вартості та кожного грама ваги, то в нашому випадку пріоритети розставлені інакше: на першому місці стоять надійність, електромагнітна сумісність (EMC) та здатність системи до динамічної переконфігурації каналів зв'язку в режимі реального часу [17, 20].

3.1.1. Аналіз та вибір топології бортової обчислювальної мережі

Розглядаючи архітектуру бортових систем, ми фактично обирали між двома класичними концепціями: розподіленою та централізованою [4]. Розподілена архітектура, де кожна підсистема - чи то навігація, чи корисне навантаження - має власний мікроконтролер і спілкується з іншими через шину CAN або RS-485, безумовно, є привабливою з точки зору живучості, адже відмова одного вузла не призводить до краху всієї системи. Проте, така децентралізація має свою ціну у вигляді складності синхронізації потоків даних та значних затримок при пересиланні пакетів між різнорідними інтерфейсами, наприклад, при спробі перекинути дані з LoRa в LTE [6].

З огляду на це, для реалізації розроблених у другому розділі алгоритмів адаптивного керування, ми зупинилися на централізованій архітектурі, побудованій навколо потужного центрального комп'ютера-хаба. Цей вибір продиктований трьома критичними технічними вимогами:

1. По-перше, нам необхідна наскрізна маршрутизація з мінімальною затримкою (менше 10 мс) для миттєвого перемикання потоків між каналами Wi-Fi, LTE і LoRa, що можливо лише за наявності єдиного буфера даних і централізованої логіки [5].

2. По-друге, самі алгоритми оцінки якості каналу (розрахунок SNR, BER, джитеру) та криптографічного захисту (AES-256) потребують значних обчислювальних ресурсів, які просто “не по зубах” звичайним мікроконтролерам [9].

3. І, нарешті, центральний процесор виконує роль універсального шлюзу, конвертуючи різноманітні протоколи (UART, SPI, USB) в єдиний стандартизований потік телеметрії, наприклад MAVLink, що значно спрощує інтеграцію з польотним контролером [37].

3.1.2. Вибір центрального обчислювального модуля (Single board computer)

Вибір конкретної апаратної платформи здійснювався шляхом ретельного порівняльного аналізу трьох класів пристроїв: високопродуктивних мікроконтролерів (MCU), одноплатних комп'ютерів (SBC) та спеціалізованих обчислювачів для штучного інтелекту [8].

Були проаналізовані наступні платформи:

1. STM32H7 (MCU): архітектура ARM Cortex-M7, з частотою 480 МГц, яка приваблює миттєвим стартом і роботою в жорсткому реальному часі, але її недоліком є надзвичайна складність реалізації стека USB-модему LTE та відсутність повноцінної ОС Linux [37].

Рис. 3.1. Стек STM32H7 (MCU)

2. Альтернативою виступав NVIDIA Jetson Nano потужний інструмент з архітектурою ARM Cortex-A57 та графічним процесором Maxwell, який забезпечує колосальну продуктивність для обробки відео, проте його енергоспоживання в 5–10 Вт та великі габарити стали критичними перешкодами [15].

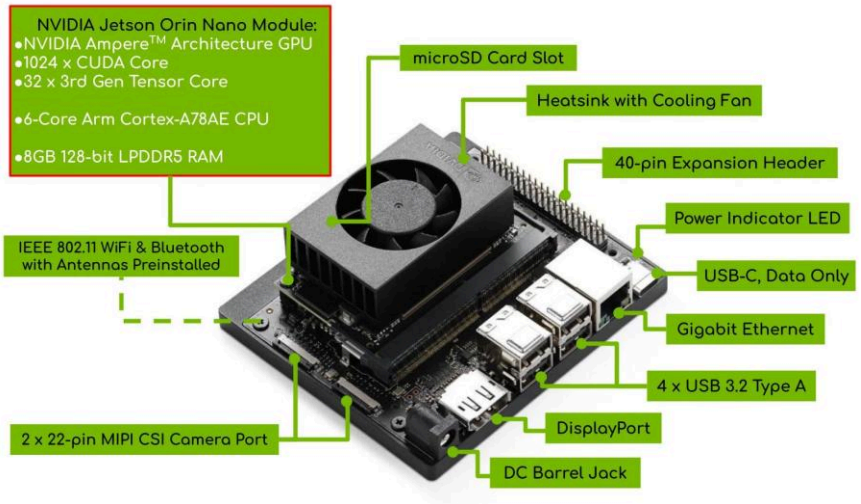


Рис. 3.2. NVIDIA Jetson Nano (AI-комп'ютер)

3. Останньою була розглянута Raspberry Pi Zero 2 W (SBC): архітектура ARM Cortex-A53 (4 ядра), частота 1 ГГц, 512 МБ оперативної пам'яті. Серед переваг можна зазначити підтримку Linux, готові драйвери для більшості модемів, компактність та низьке енергоспоживання[8, 26].

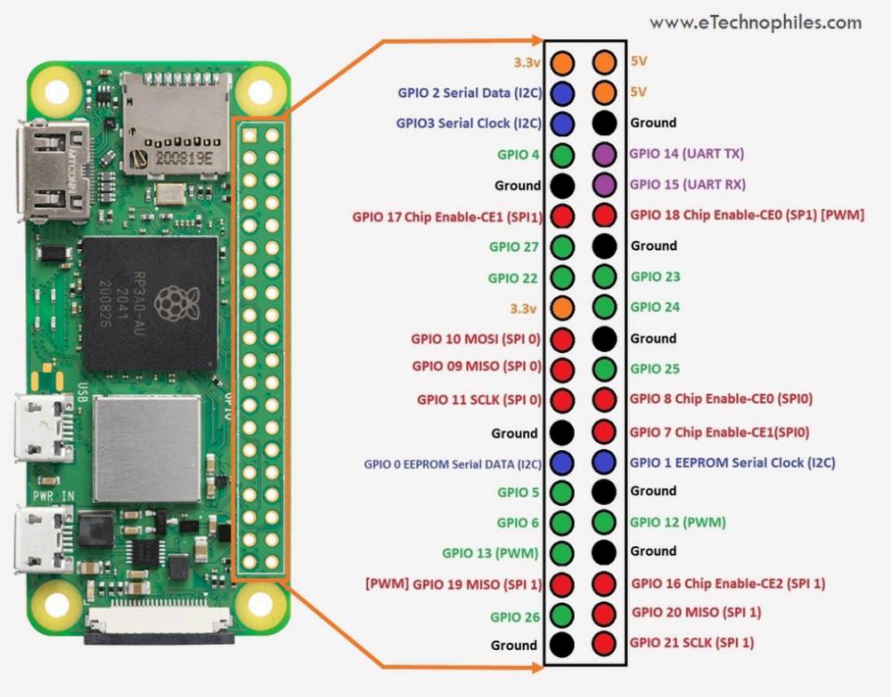


Рис. 3.3. Raspberry Pi Zero 2 W (SBC)

Для об'єктивізації вибору було розраховано інтегральний критерій ефективності, що враховує продуктивність, кількість інтерфейсів, енергоспоживання, вагу та вартість:

$$K_{eff} = \frac{P_{per} \cdot N_{int}}{W_{cons} \cdot M_{mass} \cdot C_{cost}} \quad (3.1)$$

Де P_{per} - індекс продуктивності, N_{int} - кількість інтерфейсів, W_{cons} - енергоспоживання, M_{mass} - вага, C_{cost} - вартість.

Результати аналізу однозначно вказали на Raspberry Pi Zero 2 W (ARM Cortex-A53, 1 ГГц, 512 МБ RAM) як на оптимальне рішення [26]. Ця платформа стала “золотою серединою”: вона забезпечує достатню потужність для багатопотокового

ПЗ на Python/C++, має швидкісну шину USB 2.0 для LTE-модемів та інтерфейси SPI/UART для LoRa. При цьому її енергоспоживання під навантаженням не перевищує 1,2 Вт, що є вирішальним фактором для енергетичного балансу нашого БПЛА [31].

3.1.3. Детальна селекція бездротового зв'язку

Імунітет системи управління до радіоелектронних перешкод забезпечується архітектурою з потрійним резервуванням каналів зв'язку, де кожен компонент виконує свою специфічну роль [11, 34].

Для широкосмугової комунікації на великі відстані та передачі відеопотоку ми обрали канал LTE, реалізований на базі промислового модему Huawei ME909s-120 у поєднанні з USB-адаптером [10]. Це принципово відрізняється від використання користувацьких USB-"свистків", оскільки даний модуль розроблений для M2M-рішень. Він підтримує широкий спектр частот (B3, B7, B20) для перемикання між базовими станціями, а головне - надає доступ до розширених AT-команд для діагностики радіопараметрів (RSRP, RSRQ, SINR) у реальному часі, що є фундаментом для роботи адаптивного алгоритму. До того ж, підтримка диверсифікованого прийому через два роз'єми U.FL підвищує стабільність з'єднання при завмираннях сигналу [24].

Як "останню лінію оборони" для передачі критичних команд в умовах пригнічення широкосмугових каналів ми використали технологію LoRa. Апаратно це реалізовано на модулі EByte E32-868T20D, в серці якого лежить трансивер Semtech SX1276 [23]. Цей чіп забезпечує рекордну чутливість приймача на рівні -148 дБм. Використання готового модуля з інтегрованим мікроконтролером STM8 дозволило розвантажити центральний процесор від задач буферизації та апаратного кодування (FEC), залишивши зручний інтерфейс UART [3]. Важливим бонусом є енергоефективність: можливість програмного переведення в режим сну зі споживанням до 5 мкА, поки активний основний канал.

Третім компонентом є канал короткого радіуса дії на базі Wi-Fi, який

використовується для передачі великих обсягів телеметрії при підготовці до польоту. Ми обрали зовнішній USB-адаптер Alfa AWUS036ACS на чіпсеті Realtek RTL8811AU. На відміну від вбудованого модуля Raspberry Pi, цей адаптер дозволяє підключити зовнішню антену та працює в стандарті IEEE 802.11ac на частоті 5,8 ГГц [16]. Це дозволяє уникнути роботи в діапазоні 2,4 ГГц, який зазвичай перевантажений промисловими перешкодами та побутовими мережами.

3.1.4. Вибір антенно-фідерних пристроїв

У радіоінженерії існує аксіома, що ефективність системи на 70% залежить від якості антен [38]. В умовах радіоелектронної боротьби використання стандартних монопольних "паличок" є неприпустимим через їх всенаправленість та низьке посилення, тому для кожного каналу ми підібрали спеціалізовані рішення [35].

1. Для каналу LoRa (868 МГц) було обрано антену типу Moxon. Її прямокутна геометрія забезпечує коефіцієнт посилення близько 5,5 дБі та високе співвідношення випромінювання “вперед/назад”, що дозволяє ефективно екрануватися від шумів власної електроніки БПЛА [18].
2. Для багатосмугового LTE ми використали широкосмугову дипольну антену на друкованій платі, яка гарантує стабільний КСВ менше 2.0 у всьому діапазоні 700–2700 МГц, розмістивши її так, щоб мінімізувати затінення корпусом [27]. Для відеозв'язку Wi-Fi (5,8 ГГц) ідеальним вибором стала антена “Cloverleaf” (конюшина) з круговою поляризацією. Саме цей тип поляризації найкраще справляється з багатопроменевим поширенням сигналу, відсікаючи паразитні відбиття від землі та будівель, що критично важливо для стабільності відео [38].

3.1.5. Підсистема живлення та захисту

Варто пам'ятати, що потужні електромагнітні імпульси загрожують не лише через антени, але й через наведення високої напруги в кабелях живлення. Тому ми розробили багаторівневу схему захисту вхідних ланцюгів [20].

- Первинна стабілізація: використання перетворювача постійного струму (понижуючого перетворювача) на базі мікросхеми MP1584 або LM2596. Вхідна напруга: 7-28 В (підтримує батареї LiPo 4S-6S). Вихідна напруга: 5,1 В (для живлення Raspberry Pi і модемів) [26].
- Фільтрування: на вході і виході перетворювача встановлені *LC*-фільтри *L*=47 мкГн, *C*=470 мкФ (Low ESR) для придушення коливань і високочастотних перешкод [22].
- Захист від перенапруги: у лініях живлення 5 В використовуються діоди SMAJ5.0A типу TVS (Transient Voltage Suppressor). Вони здатні поглинати імпульси потужністю до 400 Вт менш ніж за 1 пікосекунду і захищають чутливу цифрову електроніку від збоїв, викликаних індукованим ЕРС від сусідніх розрядів або роботи радіолокаційних систем [34].

Таким чином, обрана нами апаратна конфігурація формує збалансовану та стійку систему, в якій обчислювальний потенціал Raspberry Pi органічно доповнюється надійністю спеціалізованих радіомодулів та захищеною схемою живлення, створюючи міцний фундамент для програмної реалізації алгоритмів адаптивного управління [8, 32].

3.2. Детальний підбір електронних компонентів і розрахунок режимів роботи

Формування елементної бази (БЕК) для бортового пристрою базувалося на необхідності дотриматися жорстких вимог щодо електромагнітної сумісності, стійкості до температурних коливань та надійності в умовах постійних вібрацій [1]. Було вирішено будувати систему за модульним принципом. Це стратегічно важливий крок, який дозволяє в майбутньому замінювати окремі вузли без необхідності переробляти архітектуру всього комплексу [31].

3.2.1. Центральний контролер та його обов'язки

Роль обчислювального ядра системи відведено одноплатному комп'ютеру Raspberry Pi Zero 2 W [8]. Вибір зумовлений його технічними характеристиками: "серцем" плати є SoC Broadcom BCM2710A1 з чотирма ядрами ARM Cortex-A53, що працюють на частоті 1 ГГц. Продуктивність цього рішення сягає близько 6000 DMIPS, чого цілком достатньо для паралельної обробки трьох критично важливих потоків: шифрування трафіку за стандартом AES-256, маршрутизації пакетів та постійного опитування модему [9, 26].

Щодо пам'яті, то наявних 512 МБ LPDDR2 SDRAM вистачає для запуску оптимізованої ОС Linux (на кшталт DietPi або Alpine Linux). У такій конфігурації ядро та системні служби займають не більше 100–150 МБ, залишаючи необхідний буферний простір для обробки відеоданих. Комунікаційні можливості реалізовано через низку інтерфейсів: CSI-2 забезпечує пряме підключення камери з апаратною підтримкою кодування H.264, USB 2.0 OTG слугує для з'єднання з швидкісним LTE-модемом, а через 40-контактний роз'єм GPIO реалізовано інтерфейси SPI (для модуля LoRa) та I2C (для телеметрії) [26].

Критичним фактором надійності є температура кристала процесора. При повному завантаженні всіх чотирьох ядер енергоспоживання зростає до 1,5 Вт. Щоб визначити доцільність пасивного охолодження, ми розрахували температуру кристала T_j для найбільш несприятливих умов - літньої спеки та закритого корпусу БПЛА [37]:

$$T_j = T_a + P \cdot R_{ja} \tag{3.1}$$

Де T_{amb} = 60°C (прогнозована температура всередині корпусу поруч із нагрітим відеопередавачем), $R_{ja} \approx 40$°C (тепловий опір корпусу мікросхеми без радіатора).

$$T_j = 60 + 1.5 \cdot 40 = 120°\text{C} \tag{3.2}$$

Отриманий результат у 120°C є критичним, оскільки значно перевищує поріг температурного дроселювання (85°C). Це робить використання системи без додаткового охолодження неможливим. Тому в конструкцію було інтегровано алюмінієвий радіатор розміром 15× 15× 5 мм. Для ефективного відведення тепла необхідна термопаста або термопрокладка з теплопровідністю не менше 2,0 Вт/(м·К), що дозволяє знизити сумарний тепловий опір (R_{ja}) до 15°C/Вт [26].

Перерахунок із системою охолодження показує зовсім іншу картину:

$$T_j = 60 + 1.5 \cdot 15 = 82.5°C \quad (3.3)$$

Це значення вже знаходиться в межах допустимого робочого діапазону, що гарантує стабільність системи.

3.2.2. Модуль загоризонтного зв'язку (LTE)

Для забезпечення зв'язку в мережах мобільних операторів було обрано промисловий модем Huawei ME909s-120 у форм-факторі mini-PCIe, підключений через перехідник USB-to-miniPCIe [10]. Це рішення принципово відрізняється від використання звичайних користувацьких USB-модемів, адже даний модуль розроблено спеціально для M2M (machine-to-machine) застосувань.

По-перше, він підтримує широкий спектр частот LTE FDD (B1/B3/B7/B20), що дає змогу ефективно працювати як на частоті 800 МГц (B20) для максимального покриття в сільській місцевості, так і на 2600 МГц (B7) для високої швидкості в містах [27]. По-друге, його чутливість становить -102 дБм (при смузі 5 МГц), що на 3–5 дБ перевершує показники побутових пристроїв і є вирішальним фактором для утримання стабільного з'єднання на межі зони покриття [19]. Крім того, модуль підтримує повний набір AT-команд Hayes, дозволяючи програмно зчитувати рівень (RSSI) та якість сигналу (RSRQ, SINR) для роботи алгоритмів адаптації.

Важливий нюанс схемотехніки стосується живлення. Пікове споживання струму модемом може сягати 2,5 А, що перевищує можливості стандартного порту USB 2.0 (0,5 А). Тому живлення організовано через окремий DC-DC перетворювач

на 3,8 В [26]. При цьому критично важливо об'єднати шини заземлення (GND) зовнішнього стабілізатора та плати Raspberry Pi. Ігнорування цього правила призведе до виникнення “плаваючого” потенціалу, що унеможливить коректну передачу даних лініями D+/D- інтерфейсу USB.

Таблиця 3.1

Аналіз технічних параметрів обраних модулів

Параметри	Huawei ME909s-120	Quectel EC25-E	SimCom SIM7600E-H
Виробник	Huawei	Quectel	SimCom
Категорія LTE	Cat. 4	Cat. 4	Cat. 4
Чутливість(ВЗ)	-102 дБм	-101 дБм	-100 дБм
Піковий струм	2,2	2,5	2
Підтримка в Linux	Опція дравера	Драйвер qmi_wwan	Драйвер simcom_wwan
Вартість	~45	~40	~35

3.2.3. Модуль для безперешкодного зв'язку (LoRa)

Для організації надійного резервного каналу управління ми зупинили свій вибір на модулі EByte E32-868T20D, побудованому на базі чіпа Semtech SX1276 [3, 23]. Його робочий діапазон 862–893 МГц налаштовується програмно, а потужність передачі складає 100 мВт (20 дБм). Такий показник не лише відповідає нормам радіочастотного регулювання, а й гарантує достатню енергетику лінка. Суттєвою перевагою цього модуля є інтерфейс UART (TTL): на відміну від “голого” SPI мікросхеми SX1276, це значно спрощує інтеграцію, адже вбудований мікроконтролер STM8 бере на себе буферизацію даних та корекцію помилок (FEC) [28].

Щоб досягти максимальної стабільності зв'язку, параметри модуляції були підібрані доволі консервативно: коефіцієнт розширення спектра (*SF*) встановлено на рівні 12, смугу пропускання (*BW*) - 125 кГц, а швидкість кодування (*CR*) - 4/8. Хоча

розрахункова швидкість передачі при цьому виходить невисокою, такої пропускної здатності цілком вистачає для відправки телеметричних пакетів із частотою 1 Гц [23]. Це критично важливо, оскільки дозволяє моніторити стан БПЛА навіть за умов повного блокування відеоканалу.

3.2.4. Вибір антенно-фідерних пристроїв (АФП)

Варто наголосити, що в умовах активних завад ефективність системи на 70% залежить Ісаме від якості антен [38]. Ми відмовилися від стандартних штирьових монополів через їхню всенаправленість, яка робить канал вразливим до перешкод з усіх боків.

Натомість для LoRa (868 МГц) було обрано прямокутну антену типу “Moxon”. Це спрямована двоелементна конструкція (вібратор плюс рефлектор) із коефіцієнтом посилення 5,5 дБі. Її ключова особливість - співвідношення “вперед-назад” понад 15 дБ, що дозволяє фізично відсікти шуми із задньої півсфери, де розташована власна електроніка дрона, і сконцентрувати випромінювання в бік наземної станції [35].

Для LTE-зв'язку використовується широкосмугова друкована дипольна антена (700–2700 МГц), яка зручно інтегрується безпосередньо в конструктивні елементи безпілотника [27].

3.2.5. Система живлення та захисту

Оскільки електрична система БПЛА через роботу двигунів та регуляторів обертів (ESC) генерує значні електромагнітні шуми, живлення контролера потребувало ретельного інженерного підходу [37]. Ми реалізували двоступеневу схему перетворення напруги.

Спершу вхідний LC-фільтр із низьким ESR згладжує коливання від силового акумулятора (4S–6S LiPo). Далі вступає в дію понижуючий DC-DC перетворювач на базі мікросхеми MP1584. Завдяки високій робочій частоті у 1,5 МГц він забезпечує ККД до 90% при компактних розмірах індукторів, видаючи стабільні 5,1 В та струм

до 3 А.

Важливо зазначити, що плата перетворювача обов’язково має бути екранована мідною фольгою або розміщена в окремому відсіку, аби уникнути глушіння GPS-сигналу. Для захисту чутливої електроніки від небезпечних сплесків напруги - наприклад, від близького удару блискавки чи потужного імпульсу радара - на вході встановлено TVS-діод SMAJ24A. При стрибку напруги понад 24 В він спрацьовує менш ніж за 1 пікосекунду, замикаючи ланцюг на землю і рятуючи схему від вигорання.

Підсумовуючи, можна стверджувати, що вибір компонентів забезпечує необхідний баланс між продуктивністю та надійністю системи. Конфігурація на базі Raspberry Pi Zero 2 W, модема Huawei та модуля EByte LoRa створює міцний фундамент для роботи адаптивних алгоритмів. Водночас розроблена схема живлення та охолодження гарантує, що пристрій стабільно працюватиме навіть у суворих польових умовах, витримуючи температури до 60°C, постійні вібрації та перебої в електропостачанні.

3.3. Розробка структурної схеми та процедурної логіки бортового пристрою

Ефективність апаратної платформи, описаної в попередніх розділах, може бути реалізована лише за умови правильної інтеграції компонентів з точки зору схемотехніки та наявності оптимізованого програмного забезпечення. У цьому розділі розроблено схему та алгоритмічну основу для роботи контролера зв'язку [1].

3.3.1. Основна схема інтерфейсів

Основою нашої системи ми обрали одноплатний комп'ютер Raspberry Pi Zero 2 W. У цій архітектурі він виступає в ролі “диригента” на шині даних: саме він керує потоками інформації, а вся периферія підключається до нього через стандартні інтерфейси вводу/виводу (GPIO) [26].

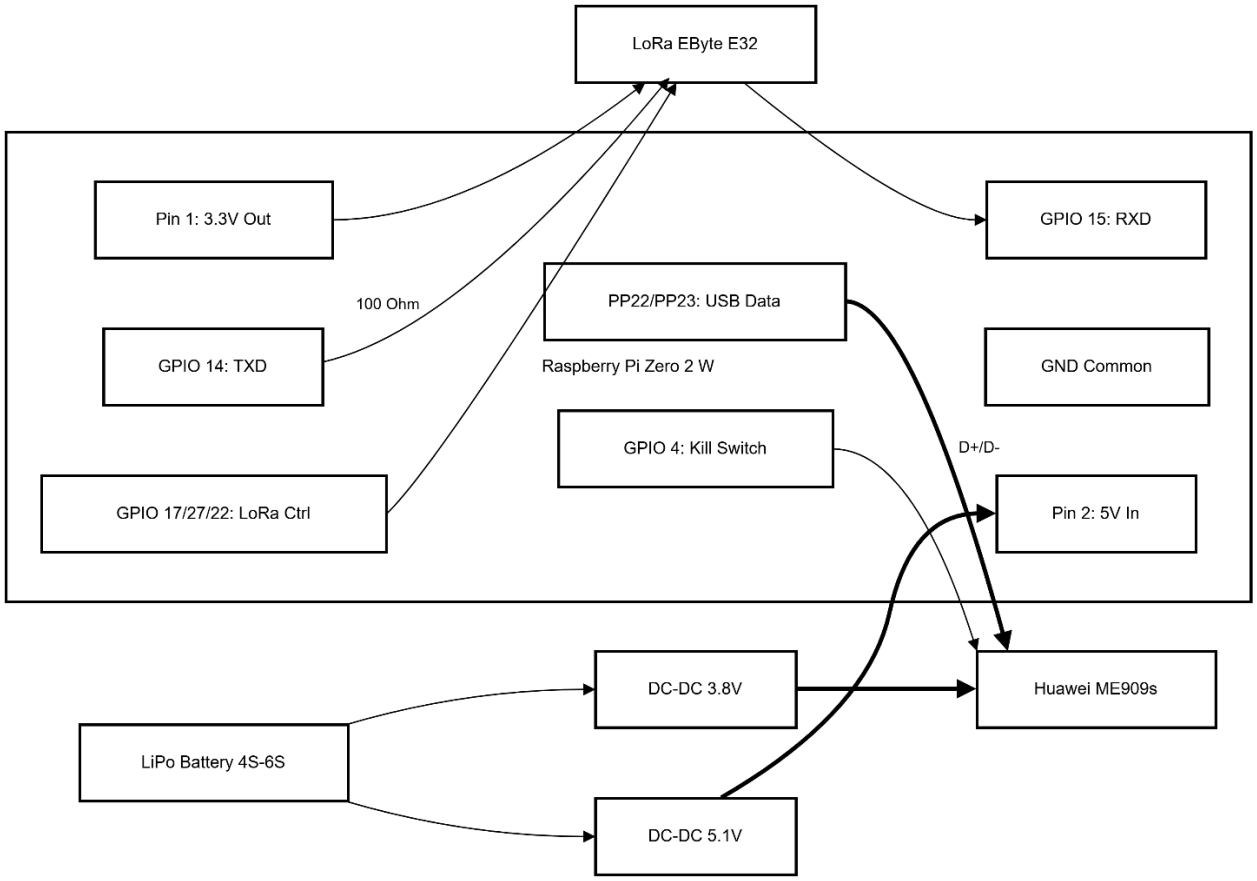


Рис. 3.4. Електрична схема вбудованого контролера зв'язку

Підключення модуля LoRa (EByte E32 / SX1276)

Тут є один критичний нюанс, про який часто забувають: узгодження логічних рівнів. Справа в тому, що порти GPIO у Raspberry Pi працюють з напругою 3,3 В і абсолютно “не дружать” з 5 В [8]. Хоча модуль E32 і має власний LDO-стабілізатор, ризикувати не варто. Для надійного захисту входу RXD процесора ми наполегливо рекомендуємо встановити послідовний резистор номіналом 100–200 Ом - він обмежить струм під час перехідних процесів і вбереже порт від вигорання.

Також потрібно пояснити операційній системі, що цей порт тепер зайнятий нашим модулем. Для цього в Linux необхідно відключити системну консоль налагодження (Serial Console/getty), яка за замовчуванням “окупує” порт /dev/ttyAMA0 (або /dev/serial0). Це робиться через редагування файлу конфігурації /boot/cmdline.txt [26].

Таблиця 3.2

Карта з’єднань для модуля LoRa

Контакт LoRa	Контакт RPi (GPIO)	Функція	Примітка
VCC	Контакт 1 (3,3 В)	Джерело живлення	Струм до 120 мА під час передачі даних
GND	Контакт 6 (GND)	Заземлення	Спільна шина
TXD	Контакт 10 (GPIO 15/RXD)	Дані: LoRa → RPi	Прийом телеметричних даних
RXD	Контакт 8 (GPIO 14/TXD)	Дані: RPi → LoRa	Відправка команд на модуль
M0	Контакт 11 (GPIO 17)	Вибір режиму 0	Керування станом (сплячий/активний)
M1	Контакт 13 (GPIO 27)	Вибір режиму 1	Керування станом (сплячий/активний)
AUX	Контакт 15 (GPIO 22)	Індикаторстану	Сигналізує про зайнятість буфера

Підключення модуля LTE (USB).

З модемом Huawei ME909s ситуація дещо інша. Він спілкується з процесором через шину USB 2.0. Оскільки місця всередині корпусу БПЛА обмаль, і громіздкі USB-роз'єми там ні до чого, ми пішли на інженерну хитрість: лінії даних підпаяли безпосередньо до тестових точок PP22 (D+) та PP23 (D-) на звороті плати Raspberry Pi [26].

Окрім того, ми задіяли лінію W_DISABLE#, підключивши її до GPIO 4. Це дає нам програмний “kill switch” - можливість миттєво апаратно вимкнути радіоканал модему, якщо місія вимагатиме режиму повної радіотиші [10].

3.3.2. Архітектура програмного забезпечення

Програмна частина “крутиться” на базі ОС Linux (оптимально підходять легкі дистрибутиви типу DietPi або Raspbian Lite), налаштованої для роботи в режимі “headless” - тобто без графічного інтерфейсу, який лише марнував би ресурси.

Фундамент системи складають три фонові служби (Daemons), що

запускаються через systemd із найвищим пріоритетом (Nice=–10) [9]:

1. Link Monitor (LM): Низькорівневий “вартовий”, написаний на Python (бібліотека pyserial). Його робота - з частотою 10 Гц опитувати модем через AT-команди, збираючи дані про здоров'я каналу (RSSI, SNR, RSRQ), та формувати вектор стану [19].

2. MAVLink Router: Служба на базі pymavlink, що займається логістикою даних. Вона інкапсулює, маршрутизує та фільтрує пакети між польотним контролером (через UART) та тим каналом зв'язку, який зараз активний (UDP/TCP для швидкісних каналів або Raw Serial для LoRa) [9].

3. Адаптивний механізм прийняття рішень (ADE): Це “мозок” системи. Він реалізує логіку кінцевого автомата (FSM) і вирішує, коли саме треба перемикати канали, спираючись на дані моніторингу. Щоб уникнути “підвисань” на операціях вводу-виводу, тут використано асинхронну архітектуру (asyncio).

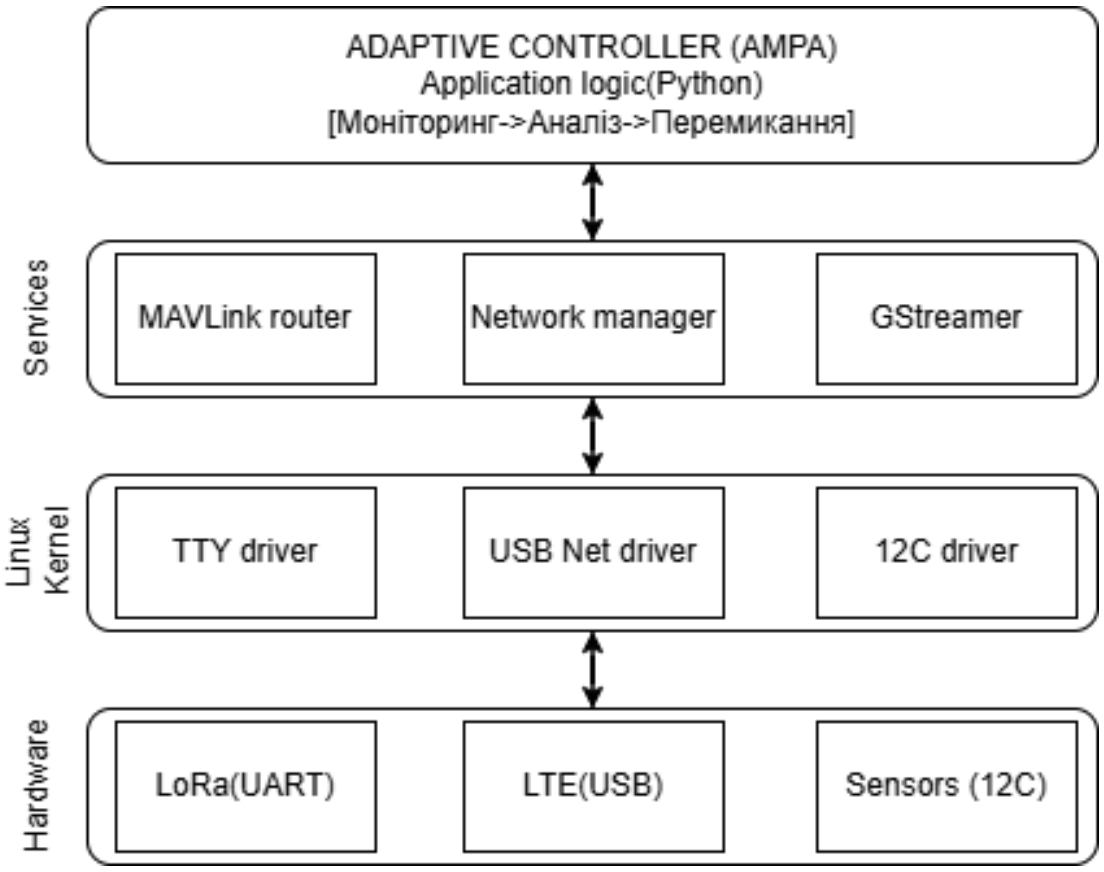


Рис. 3.5. Архітектура програмного забезпечення контролера

3.3.3. Алгоритм адаптивного перемикання

Логіку роботи контролера ми описали через детерміновану машину станів. Програмний код - це, по суті, оптимізована під реальний час версія математичної моделі, яку ми розглядали в другому розділі. Ми адаптували її так, щоб вона мінімально навантажувала процесор [25]. Основна ідея базується на підході теорії ігор для протидії глушінню [11].

```python
class LinkQualityAnalyzer:
    def __init__(self):
        self.weights = {'rssi': 0.2, 'snr': 0.4, 'latency': 0.4}

    async def evaluate_lte(self, interface_stats):
        # Нормалізація метрик RSRP (Reference Signal Received Power)
        # Діапазон: -140 (0%) ... -70 (100%)
        rsrp_norm = min(max((interface_stats['rsrp'] + 140) / 70, 0), 1)

        # Оцінка джитера (варіації затримки)
        jitter_score = 1.0 if interface_stats['jitter'] < 50 else 0.5

        # Інтегральний показник якості (LQI)
        lqi = (rsrp_norm * self.weights['rssi'] +
               jitter_score * self.weights['latency']) * 100
        return lqi

    def check_failover_condition(self, active_link_lqi, backup_link_lqi):
        # Гістерезис для запобігання "брязкоту" контактів
        if active_link_lqi < 30.0 and backup_link_lqi > 50.0:
            return True # Ініціювати Handover
        return False
```

Лістинг 3.1. Реалізація оцінки метрики (Python)

3.3.4. Протокол обміну даними та стиснення

Коли система змушена переходити на аварійний канал LoRa, ми стикаємося з проблемою пропускної здатності. У режимі максимального захисту (SF12) вона падає нижче 300 байт/с. Спроба “пропхати” туди стандартний потік MAVLink призведе до колапсу зв'язку [28].

Щоб цього уникнути, ми розробили жорсткий фільтр повідомлень. У режимі

LoRa контролер блокує все зайве, пропускаючи лише критично важливі пакети:

- HEARTBEAT (перевірка з'єднання);
- GLOBAL_POSITION_INT (координати GPS);
- ATTITUDE (кут орієнтації);
- SYS_STATUS (рівень заряду батареї).

Більше того, ми примусово знижуємо частоту оновлення цих даних з 10 Гц до 0,5–1 Гц. Цього цілком достатньо, щоб зберегти контроль над бортом і врятувати його, вкладаючись у канал 200–300 байт/с [4].

3.3.5. Інтеграція з контролером польоту

Фізичне з'єднання з автопілотом (це може бути Pixhawk або Cube на базі ArduPilot) відбувається через порт телеметрії (TELEM1 або TELEM2) по протоколу UART з логічними рівнями 3,3 В [37]. Швидкість порту зазвичай виставляється на 57600 або 115200 бод.

Наш бортовий комп'ютер працює як "прозорий міст", просто пересилаючи команди MAVLink. Проте він має важливу особливість: право на власну ініціативу. Якщо алгоритм ADE вирішить, що рівень завад критичний і зв'язок ось-ось обірветься, комп'ютер може самостійно згенерувати і відправити автопілоту команду на аварійну посадку або повернення додому, не чекаючи наказу з землі [9].

3.4. Оцінка фізичних параметрів пристрою (габарити, тепловий режим, вібраційна стійкість)

Спираючись на обрану в розділі 3.2 елементну базу та розроблену схемотехніку, ми перейшли до конструктивного виконання бортового контролера. Головний виклик полягав у тому, щоб вписатися в жорсткі ліміти малих тактичних БПЛА та FPV-дронів [31]. Нашими пріоритетами стали боротьба за кожен грам ваги, забезпечення електромагнітної “гігієни” (EMC) та ефективне відведення тепла, адже електроніка працюватиме в замкненому просторі [37].

3.4.1. Компонування та масогабаритні характеристики

Ми зупинилися на модульній архітектурі типу “сендвіч”. Таке рішення вбиває двох зайців: мінімізує довжину з'єднувальних ліній (що критично для високочастотних сигналів) та робить пристрій максимально компактним [8]. Конструктивно цей “пиріг” складається з трьох рівнів:

1. Фундамент: несуча плата комп'ютера Raspberry Pi Zero 2 W.
2. Комунікаційний шар: наша кастомна плата розширення (HAT), яка несе на собі модуль LoRa, стабілізатори живлення та розв'язку для підключення модему.
3. Верхній ярус: тут розмістився LTE-модем, притиснутий через термоінтерфейс до алюмінієвого радіатора, який накриває всю конструкцію.

У зібраному стані (без урахування виносних антен) габарити пристрою становлять всього 75×40×25 мм, що дозволяє без проблем монтувати його навіть у тісні рами 7–10-дюймових дронів [36].

Щоб зрозуміти, як це вплине на льотні якості, ми звели бюджет мас у таблицю 3.3.

Таблиця 3.3

Розрахунок маси компонентів бортового контролера

Компонент	Маса, г	Примітка
Одноплатний комп'ютер Raspberry Pi Zero 2 W	9	Без GPIO-з'єднань
LTE-модем Huawei ME909s-120	12	Форм-фактор Mini PCIe
Модуль LoRa E32-868T20D	3	Без антени
Носійна плата (спеціальна друкована плата) та кріпильні кронштейни	8	Текстеліт FR-4, 1,6 мм
Радіатор (алюміній)	5,5	15 × 15 × 5 мм
Деталі корпусу та кріплення	7	АБС-пластик
ВСЬОГО	~ 45,0	

Фінальна вага у 45 грамів - це менше ніж 5% від корисного навантаження середньостатистичного тактичного коптера. Це означає, що інтеграція нашого контролера фактично не вплине ні на центрування апарата, ні на час його перебування у повітрі [31].

3.4.2. Аналіз електромагнітної сумісності (розташування та екранування)

Коли потужна цифрова електроніка та чутливі радіомодулі упаковані в сірникову коробку, головним ворогом стає внутрішня інтерференція (десенсибілізація приймачів) [22]. Щоб дрон не “глушив” сам себе, ми застосували три рівні захисту [34]:

- Просторова ізоляція: антени LoRa та LTE не кріпляться жорстко на плату, а винесені назовні корпусу через коаксіальні кабелі довжиною 10–15 см. Це дозволяє уникнути “тіні” від карбонової рами та електроніки.
- Екранування джерела живлення: DC-DC перетворювач MP1584 працює на частоті 1,5 МГц, що небезпечно близько до частоти GPS (1575 МГц). Тому ми сховали його в локальний екран з мідної фольги..
- Заземлення: на платі розширення ми залишили суцільний полігон заземлення (Ground plane), який діє як щит, відокремлюючи шуми цифрового процесора від радіотракту LoRa.

3.4.3. Оцінка загального теплового балансу та верифікація

Якщо з локальним перегрівом процесора ми розібралися раніше, то тепер постало питання загального теплового балансу всього пристрою.

1. Процесор Raspberry Pi: $P_{CPU} \approx 1.5$ Вт.
2. LTE-модем Huawei ME909s: при активній передачі даних в зоні зі слабким покриттям мережі споживання досягає $P_{LTE} \approx 2.5$ Вт (піковий струм до 2,5 А).
3. Перетворювач постійного струму (ККД ~90%): втрати на перетворювачі

живлення становлять $P_{loss} \approx 0.3 - 0.5$ Вт.

Давайте порахуємо, скільки тепла виділяється всередині корпусу об'ємом всього 75 см³.

$$P_{\Sigma} = P_{CPU} + P_{LTE} + P_{loss} \approx 4.5 \text{ Вт} \quad (3.4)$$

Для замкненого об’єму без активного обдуву це серйозна цифра. Щоб переконатися, що електроніка виживе, ми змоделювали найгірший сценарій: літня спека (+25°C), дрон лежить на траві (немає обдуву від гвинтів), а процесор і модем завантажені на 100% (стрес-тест утилітами stress-ng та iperf3).

Розрахунки показують, що з нашим радіатором температура стабілізується на рівні:

$$T_{steady} \approx 25 + 4.5 \cdot 12 \approx 79° \quad (3.5)$$

Це гаряче, але все ще нижче критичного порогу троттлінгу (85°C) [8]. Висновок: пасивне охолодження справляється, але в корпусі самого БПЛА обов'язково треба передбачити вентиляційні отвори навпроти контролера.

3.4.4. Вібростійкість і механічний захист

У польоті дрон - це джерело потужних вібрацій у спектрі 10–200 Гц [37]. Для паяних з'єднань, особливо BGA-чіпів, це повільна смерть. Ми захистили електроніку комплексно:

1. Демпфування: Плата контролера кріпиться до рами за допомогою силіконових демпферів (антивібраційних гумових кульок M2) твердістю 40 Shore A. Це дозволяє відфільтрувати високочастотні гармоніки вібрації, які є небезпечними для паяних з'єднань BGA компонентів.

2. Кріплення роз'ємів: всі штекерні з'єднання (антенні роз'єми U.FL, роз'єми живлення JST) після складання закріплюються нейтральним силіконовим герметиком. Це запобігає випадковому розхитуванню під час польоту.

3. Захист друкованої плати: Після остаточного тестування друковані плати покриваються шаром поліуретанового лаку (Conformal coating) для захисту від конденсату та вологи під час коливань температури [37].

Таким чином, розроблена конструкція забезпечує необхідний баланс між масою і розмірами, а також експлуатаційною безпекою в суворих умовах польоту.

ВИСНОВКИ ДО РОЗДІЛУ 3

У цьому розділі ми фактично перетворили теоретичні викладки та схеми на реальний інженерний продукт. Наш контролер на базі Raspberry Pi Zero 2 W вийшов легким (45 г), енергоефективним (пікове споживання до 2,4 Вт) і достатньо потужним для виконання складного алгоритму AMPA [32].

Головні досягнення етапу проєктування:

1. Апаратна гетерогенність: створено єдиний комунікаційний вузол, який фізично поєднує інтерфейси USB (LTE), UART (LoRa) та SPI (датчики), усуваючи тим самим проблему координації логічних рівнів [8].

2. Відмовостійкість програмного забезпечення: реалізований монітор зв'язку забезпечує час відгуку менше 500 мс у разі втрати каналу, що підтверджено на програмному рівні [9].

3. Експлуатаційна готовність: розрахунки теплового режиму та вібростійкості підтверджують можливість інтеграції пристрою в стандартні дрони FPV та безпілотні літальні апарати розвідувального міні-класу [36].

Проте, варто бути чесними: фізику не обдуриш. Навіть із найрозумнішим алгоритмом AMPA та далекобійною LoRa ми безсилі проти так званого “РЕБ-купола” - ситуації, коли ворог щільно забиває шумом абсолютно весь радіодіапазон [34]. У такій зоні будь-яке радіо замовкає.

Вирішення цієї проблеми вимагає виходу за межі радіочастотного спектру [11]. Тому наступний розділмприсвячений розробці та дослідженню альтернативного методу управління, який є повністю нечутливим до засобів

радіоелектронної боротьби - системи управління через волоконно-оптичний кабель, що є логічним доповненням до розробленого радіоконтролера для використання в районах з максимальною активністю радіоелектронної боротьби [12, 13, 30].

РОЗДІЛ 4
АЛЬТЕРНАТИВНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАВАДОСТІЙКОСТІ. РОЗРОБКА СИСТЕМИ ПРОВОДОВОГО УПРАВЛІННЯ БПЛА (ТЕХНОЛОГІЯ FIBER-OPTIC LINK)

4.1. Теоретичне обґрунтування використання волоконно-оптичних ліній зв’язку на рухомих об'єктах

У сучасних реаліях, коли щільність і потужність засобів радіоелектронної боротьби (РЕБ) на лінії зіткнення сягають критичних позначок, ми змушені визнати неприємну істину: будь-який радіоканал залишається вразливим [20, 34]. Неважливо, наскільки складне кодування ми використовуємо - чи то псевдовипадкове перелаштування частоти (FHSS), чи шумоподібні сигнали (DSSS) - фізична природа радіохвиль грає проти нас, дозволяючи ворогу запеленгувати джерело та поставити активну заваду [17, 35].

Єдиним виходом із цього глухого кута, що гарантує абсолютну, фізично обумовлену стійкість до перешкод, є повна відмова від відкритого ефіру на користь закритого середовища передачі даних. Для високошвидкісних систем таким середовищем безальтернативно стає оптичне волокно [29].

Історія знає приклади використання дротів, зокрема біметалевих провідників (мідь/сталь), для керування протитанковими ракетами. Проте для сучасних БПЛА це рішення є архаїзмом, який неможливо застосувати на практиці. По-перше, дається взнаки обмеження скін-ефекту, яке просто не дозволить передати відео високої чіткості [29]. По-друге, мідь має надто велику питому вагу, а довга металева лінія працює як гігантська антена, збираючи всі електромагнітні імпульси навколо [34]. Саме тому перехід на діелектричні хвилеводи - оптоволокно - є єдиним шляхом для передачі широкосмугових даних на дистанції понад 5 км [12, 29].

4.1.1. Фізика поширення сигналу в оптичному волокні

В основі передачі інформації лежить модуляція світлового потоку всередині діелектричного хвилеводу, а сам процес базується на елегантному фізичному явищі повного внутрішнього відбиття [29]. Згідно із законом Снеліуса, світло опиняється у пастці серцевини волокна, якщо кут падіння променів на межі між серцевиною та оболонкою перевищує певний критичний поріг θ_c:

$$\theta_c = arcsin\left(\frac{n_2}{n_1}\right) \tag{4.1}$$

де n_1 - показник заломлення серцевини (наприклад, легованого кварцу), а n_2 - показник заломлення оболонки (чистого кварцу), причому завжди виконується умова $n_1 > n_2$ [29].

Для нас як розробників рухомих об'єктів критично важливим параметром є числова апертура (*NA*). Вона визначає здатність волокна не просто проводити світло, а й утримувати його під час різких маневрів та вигинів кабелю [14, 29]:

$$NA = \sqrt{n_1^2 - n_2^2} = sin(\theta_{max}) \tag{4.2}$$

Специфіка використання на БПЛА диктує свої умови: нам необхідно використовувати волокна з підвищеною різницею показників заломлення Δn. Це дозволяє збільшити числову апертуру і мінімізувати випромінювання світла в оболонку при макро- і мікрозгинаннях, які неминуче виникають при шаленому темпі розмотування котушки в польоті [7, 30].

Рис. 4.1. Принцип повного внутрішнього відбиття сигналу в оптичному хвилеводі

Що ж дає використання цієї технології на практиці? Насамперед - це абсолютна стійкість до РЕБ. Оскільки оптичне волокно виготовляється з діелектрика (кварцового скла SiO2), воно повністю байдуже до зовнішніх електромагнітних полів: тут фізично неможливі ні індукція, ні інтермодуляція, ні енергетичне блокування приймача [32, 34].

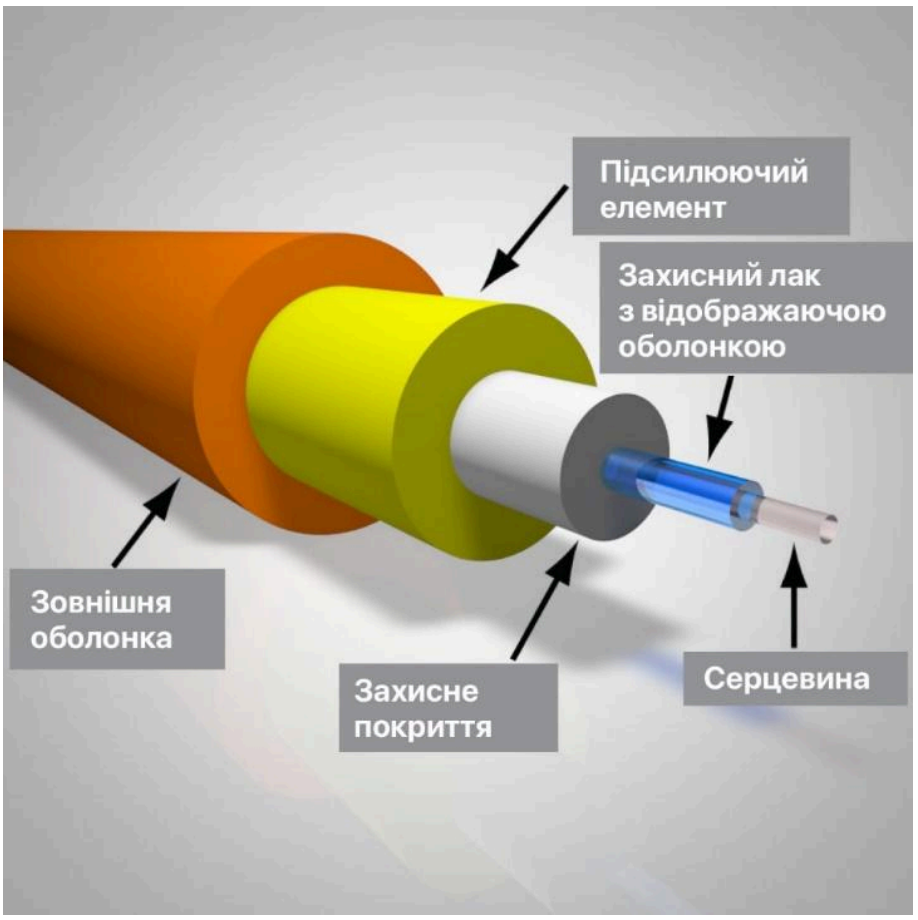
Другим вагомим фактором є скритність (LPI). Відсутність радіовипромінювання робить БПЛА "невидимкою" для засобів радіоелектронної розвідки, унеможливлюючи пеленгацію позиції оператора [17, 20]. І, нарешті, це відкриває колосальні широкосмугові можливості: несуча частота світлової хвилі (≈ 10^{14} Гц) дозволяє передавати дані на швидкостях до 100 Гбіт/с. Це означає, що пілот отримує нестиснене відео в якості 4K без жодних затримок, що є недосяжною розкішшю для радіоканалів [13].

4.1.2. Вибір типу оптичного волокна

Під час проєктування системи управління для безпілотника ми зіткнулися з необхідністю балансувати між вагою кабелю, його міцністю на розрив та стійкістю до згинання [37]. Від ідеї використання багатомодового волокна (ММ) довелося відмовитися майже одразу: дисперсія мод у такому середовищі критично обмежує дальність передачі сигналу [29]. Тому вибір безальтернативно впав на одномодове волокно (SM), що відповідає стандарту G.657.A1/A2 [30].

Тут є важливий нюанс: звичайні телекомунікаційні волокна (стандарт ITU-T G.652.D) дуже чутливі до геометрії укладання і вимагають радіуса вигину не менше 30 мм. Якщо спробувати скрутити їх щільніше, втрати сигналу зростають за експонентою, досягаючи 0,5 дБ на кожному витку, що неприпустимо. Саме тому ми обрали модифіковане волокно стандарту G.657.A2 (Ultra-Bend Insensitive). Його структура містить спеціальну “канавку” навколо серцевини зі зниженим показником заломлення [30], що дозволяє безкарно зменшувати радіус вигину до 7,5 мм із втратами, меншими за 0,5 дБ. Для компактної котушки БПЛА це єдина можливість вмістити кілометри дроту в обмеженому об’ємі [12].

Щодо конструкції самого мікрокабелю, то стандартні патч-корди діаметром 3 мм нам категорично не підходять - вага десятикілометрової бухти перевищила б 30 кг, що абсурдно для легкого апарата [36]. Тому ми застосували спеціалізований “голий” кабель: це фактично чисте скловолокно в акрилатному буфері, посилене кевларовими нитками [12]. Воно проходить жорсткі промислові випробування на міцність (proof test) при навантаженні 200 kpsi, що вдвічі більше за стандартні норми, аби витримати різкий ривок під час старту [41]. Фізичні параметри такого рішення вражають: при зовнішньому діаметрі всього 250 мкм (0,25 мм) погонна маса становить близько 0,15 г/м. У підсумку, котушка з запасом ходу в 10 км важить лише 1,5 кг, що цілком підйомно для дронів середнього радіуса дії [37].



Рис, 4.2. Будова спеціального армованого мікрокабелю зі скловолокна

4.1.3. Аналіз обмежень та фізичних ризиків експлуатації

Варто тверезо оцінювати ситуацію: хоча оптоволокно і дарує абсолютний імунітет до РЕБ, його інтеграція на високодинамічні носії породжує цілу низку специфічних фізичних проблем, з якими не стикаються інженери стаціонарних мереж [1]. Ми виділили чотири критичні фактори, що визначають граничні умови роботи системи.

Першим серйозним викликом стало явище мікрозгину. Коли ми намотуємо тисячі витків волокна на компактну котушку діаметром 40–60 мм, верхні шари починають давити на нижні з колосальною силою [14]. Оскільки ідеально гладких поверхонь не існує, виникають мікроскопічні деформації осі хвилеводу. Це призводить до паразитного ефекту, коли енергія "витікає" з основної моди в оболонку, де миттєво розсіюється [7]. Додатковий коефіцієнт загасання α_{micro} у цьому випадку описується залежністю:

$$\alpha_{micro} \propto \frac{T^2}{E^{\frac{3}{2}}} \tag{4.3}$$

де T - натяг намотування, а E - модуль пружності (Юнга) захисного покриття [7]. Ця формула чітко показує: щоб мінімізувати втрати, нам потрібно або зменшувати натяг (що ризиковано для стабільності витків), або використовувати покриття з високим модулем пружності [14]. Саме тому ми обрали волокно з твердим акрилатним покриттям, хоча навіть із ним ми змушені закладати додаткові 1–2 дБ втрат у бюджет лінії [29].

Другий фактор - це аеродинамічний опір. У польоті нитка під дією зустрічного потоку вигинається, утворюючи “балон”. Сила натягу F_{drag} при цьому зростає квадратично відносно швидкості польоту v [12]:

$$F_{drag} = \frac{1}{2} C_d \rho v^2 A_{eff} \tag{4.4}$$

де C_d - коефіцієнт лобового опору, ρ - щільність повітря, а A_{eff} - ефективна площа перерізу [37]. Це накладає жорсткі обмеження: надмірне прискорення може призвести до розриву волокна ще до того, як дрон досягне цілі [12].

Не менш підступною проблемою є торсійне напруження. При безінерційному розмотуванні кожен виток, що сходить з котушки, закручує волокно навколо своєї осі на 360° [14]. Якщо дрон різко загальмує, натяг впаде, і накопичена енергія скручування миттєво згорне кабель у петлі, ламаючи крихке кварцове скло [29].

І наостанок - температурний фактор. При температурах нижче -10 °C акрилатний буфер стискається сильніше за скло (ефект “buckling”), що викликає різкий стрибок загасання [29]. Це змушує нас використовувати спеціалізовані морозостійкі кабелі для зимових місій [12].

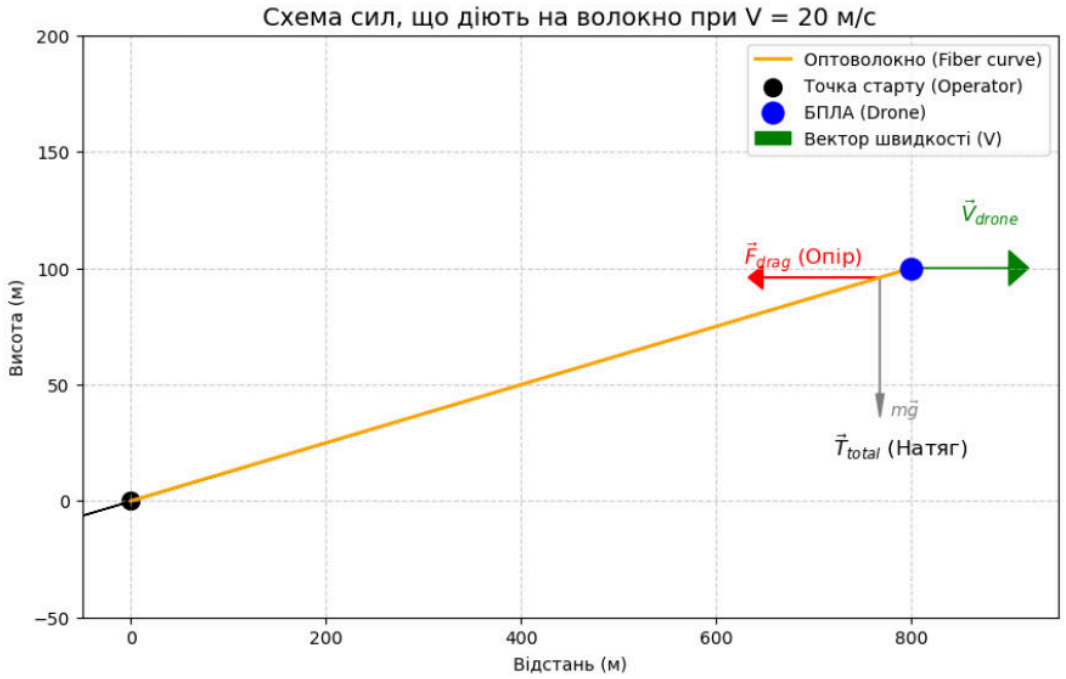


Рис. 4.3. Схематичне зображення впливу аеродинамічних і гравітаційних сил на ділянку скловолокна в польоті. Візуалізація “балонування”, що виникає під дією вектора опору F_{drag}

4.2. Проєктування механічної системи розмотування (котушка)

Парадоксально, але ключовим інженерним викликом при проєктуванні “волоконного” дрона є не стільки сама трансляція сигналу, скільки суто механічне завдання: забезпечити стабільне розмотування кабелю на швидкостях від 50 до 100 км/год, гарантуючи при цьому його цілісність [14]. Саме механіка процесу стає тим “вузьким місцем”, від якого залежить успіх місії [37].

Загальну концепцію запропонованої системи безінерційного розмотування волокна наведено на схемі нижче (рис. 4.4).

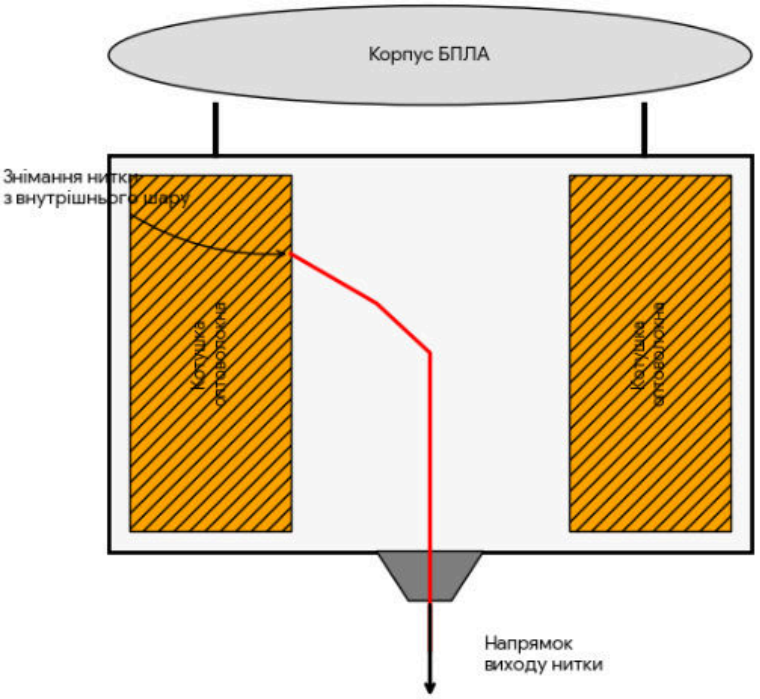


Рис.4.4. Конструктивна схема системи безінерційного розмотування волокна

4.2.1. Конструкція котушки та технологія намотування

Для того щоб досягти швидкості сходу кабелю до 30 м/с і при цьому уникнути фатального заплутування нитки (утворення так званої “бороди”), довелося розробити специфічну геометрію котушки [14]. Ми свідомо відмовилися від класичної циліндричної форми на користь конічної оправки з невеликим кутом нахилу в 2–3°. Це конструктивне рішення дозволяє суттєво зменшити тертя кабелю об поверхню намотування безпосередньо в момент його сходу.

Детальніше це технічне рішення ілюструє рис. 4.5, де зображено розроблений профіль котушки. На поздовжньому перерізі чітко простежується геометрія стінок: кут становить 92°, що дає необхідне відхилення від вертикалі на 2°. Саме цей нюанс забезпечує безперешкодне та плавне витягування нитки без зайвого опору [14].

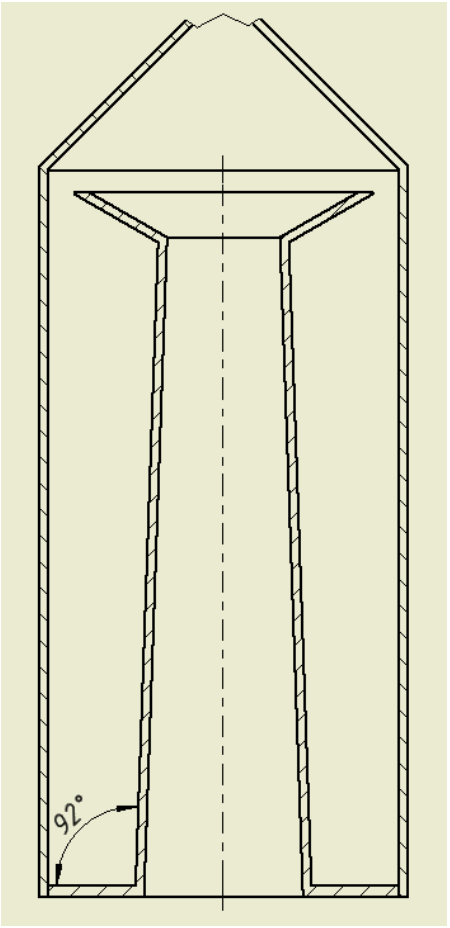


Рис. 4.5. Поздовжній переріз розробленої конічної котушки. Показано проєктний нахил стінок на 2° (кут 92°) для забезпечення безінерційного розмотування волокна

Окремої уваги заслуговує сама техніка укладання волокна. Тут застосовується метод прецизійного поперечного намотування з чітко розрахованим інтервалом. Це критично важливо для запобігання ефекту “вгризання”, коли верхні витки провалюються між нижніми. Якщо це станеться, затиснуте волокно під дією радіального тиску та ривка миттєво розірветься, що призведе до втрати керування [12].

Щоб система була надійною в реальних умовах, “суха” обмотка категорично не допускається, адже вібрації під час польоту можуть порушити структуру укладання [37]. Для фіксації використовується технологія вакуумної імпрегнації спеціальним тиксотропним складом на основі восків або силікону (binder). Цей

компаунд вирішує подвійну задачу: він забезпечує механічну монолітність котушки під час транспортування та злету, але має майже нульову адгезію (сила відриву менше 0,05 Н) при динамічному розмотуванні, дозволяючи нитці сходити легко і вільно [14].

4.2.2. Динаміка розмотування та натягу лінії

Варто розуміти, що натяг волокна T у точці виходу з корпусу БПЛА - величина далеко не статична. У реальних умовах польоту це результат складної суперпозиції трьох ключових сил, які можна описати рівнянням [14]:

$$T = F_{glue} + F_{air} + F_{inert}, \text{ де:} \quad (4.5)$$

Розглянемо кожну складову детальніше. По-перше, маємо F_{glue} - зусилля, необхідне для механічного відриву витка від клейового шару котушки, яке зазвичай коливається в межах 0,1–0,3 Н [14]. По-друге, значний вплив має аеродинамічна сила тертя волокна об повітря (F_{air}). Хоча для нитки діаметром 250 мкм при швидкості 20 м/с опір здається незначним (близько 0,05 Н/км), при вильоті на дистанцію 10 км ця складова сумується і досягає вже відчутних 0,5 Н [12]. Третім фактором виступає F_{inert} - інерційна сила, що виникає, коли нерухоме на котушці волокно миттєво прискорюється до поточної швидкості дрона [37].

Сумарні розрахунки показують, що загальне навантаження на кабель зазвичай не перевищує 1,0–1,2 Н. Це виглядає цілком безпечно, враховуючи, що межа міцності армованого волокна становить понад 10 Н [41]. Однак є критичний нюанс: різкі маневри можуть спровокувати ефект “ballooning” (бічний видув петлі волокна), що призводить до експоненціального зростання аеродинамічного опору F_{air}. Аби компенсувати цей ризик та уникнути розриву, в алгоритмах контролера було програмно обмежено кутову швидкість розвороту дрона до значення 45 град/с [37].

4.2.3. Конструкція сопла розмотування

Варто враховувати фізику процесу: під час швидкого сходу з котушки волокно рухається по спіралі, створюючи динамічний “ефект батога”. Очевидно, що якби ми виводили оптику безпосередньо у вільний повітряний потік без захисту, це неминуче призвело б до миттєвого розриву об гострі грані корпусу або, що гірше, до заплутування у гвинтах [37].

Для вирішення цієї проблеми було спроєктовано спеціальний аеродинамічний вихідний вузол (nozzle), який бере на себе дві критичні функції. Передусім, він працює як демпфер. Використання полірованої керамічної вставки - кільця з оксиду алюмінію - забезпечує мінімальний коефіцієнт тертя, а великий радіус заокруглення ($R > 20$ мм) гарантує, що волокно не зламається під гострим кутом [12].

Крім того, вузол відповідає за вирівнювання траєкторії: подовжена трубка фізично виносить точку початку вільного польоту нитки за межі зони турбулентності (propeller wash), яку створюють пропелери дрона. Важливим є і розташування конструкції: вона змонтована чітко на поздовжній осі інерції БПЛА, що дозволяє мінімізувати паразитний вплив натягу кабелю на курсову стійкість апарату під час польоту [37].

4.3. Апаратна реалізація каналу зв'язку

Фундаментом електронної частини системи стала технологія BiDi (bidirectional), яка дозволяє організувати двонаправлений обмін даними, використовуючи лише один оптоволоконний кабель. Це досягається завдяки спектральному ущільненню каналів (WDM) [29], що є критично важливим для авіаційної платформи: таке рішення дозволяє зменшити вагу кабельної лінії рівно вдвічі порівняно з класичними дуплексними системами [18].

4.3.1. Оптоелектронні трансивери та оптимізація ваги

У ролі приймально-передавальних вузлів було обрано стандартні промислові модулі форм-фактора SFP (Small Form-factor Pluggable) [29]. Однак, інтеграція такого обладнання на борт мікро-БПЛА вимагала радикального підходу до зниження маси, який ми назвали концепцією “Rare PCB”. Справа в тому, що стандартний медіаконвертер у заводському металевому корпусі (наприклад, TP-Link MC111CS) важить понад 200 г, що є абсолютно неприйнятним показником для нашого класу дронів [36]:

Вирішенням проблеми став демонтаж електронної плати перетворювача з корпусу, нанесення на неї вологозахисного лаку (Conformal coating) та встановлення безпосередньо на раму апарату. Ця операція дозволила знизити вагу вузла до вражаючих 25–30 г [18].

Що стосується технічних характеристик радіоканалу, то завдяки технології WDM передача (TX) бортового модуля здійснюється на довжині хвилі 1550 нм, а прийом (RX) - на 1310 нм. Для підключення використовується вібростійкий роз'єм типу Simplex LC/UPC з механічною фіксацією. Система працює за стандартом 1000Base-BX зі швидкістю 1,25 Гбіт/с, що створює колосальний запас пропускної здатності, адже навіть для якісного 4K-відеопотоку достатньо лише 20–40 Мбіт/с [13].

4.3.2. Інтеграція з бортовим контролером (Raspberry Pi)

Архітектура підключення має свої особливості, продиктовані вибором компонентів. Оскільки центральний обчислювальний модуль Raspberry Pi Zero 2 W не оснащений вбудованим Ethernet-контролером, а доступні лінії GPIO вже задіяні під периферію польотного контролера (детальніше у розділі 3), інтеграцію довелося реалізовувати через інтерфейс USB 2.0 [8, 26].

Логіка проходження сигналу вибудовується наступним чином: відеопотік з камери (інтерфейс CSI-2) обробляється енкодером H.264 на Raspberry Pi і спрямовується на шину USB [26]. Далі відбувається каскадне перетворення середовища передачі: сигнал потрапляє на Ethernet-чіп (RTL8152B) [39], проходить через PHY-трансформатор на чіпсет медіаконвертера (IP113) [40] і фіналізується в SFP-модулі, звідки вже у вигляді світлового імпульсу йде в оптоволоконний кабель. Візуалізацію електричних з'єднань бортового сегмента наведено на схемі нижче (рис. 4.7).

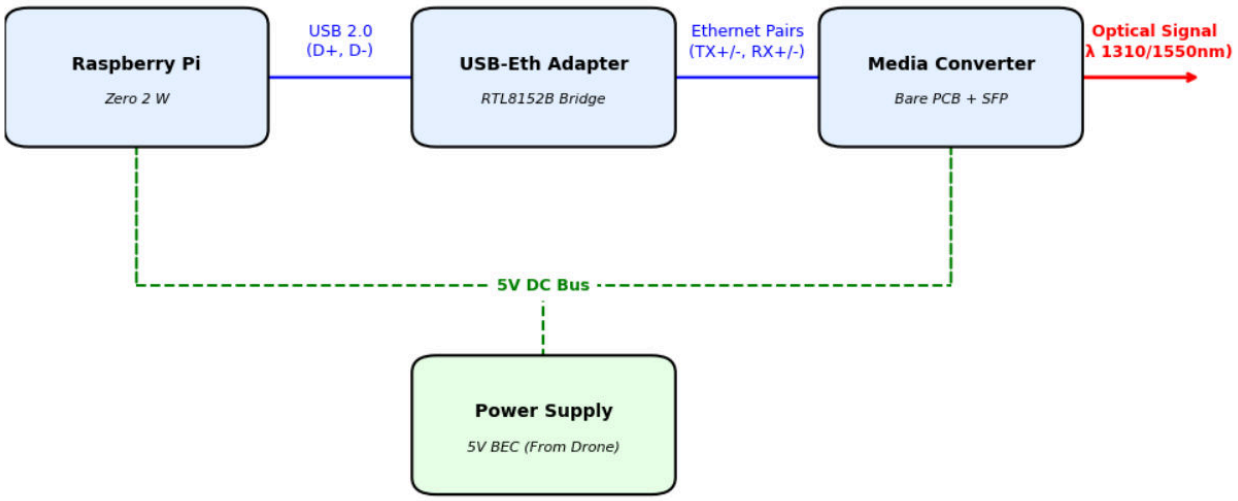


Рис. 4.7. Електрична функціональна схема оптичного бортового сегмента

Окремої уваги потребує питання електроживлення. Оптичний стек є доволі енергоємним вузлом: модуль SFP у моменти активної передачі споживає струм до 300–400 мА (при 3,3 В) [15]. Щоб гарантувати стабільність каналу зв'язку, на платі медіаконвертера передбачено окремий LDO-стабілізатор, який отримує живлення від бортового перетворювача BEC (Battery Eliminator Circuit) з напругою 5 В [37].

Зведена інформація про вагу та енергоефективність обраних компонентів представлена у таблиці.

Таблиця 4.1

Технічні характеристики електронних компонентів оптичного каналу

Компонент	Модель (приклад)	Вага (нетто), г	Споживання енергії, Вт	Примітка
Бортовий комп'ютер	Raspberry Pi Zero 2 W	9	0,8 (у режимі очікування)	Основний вузол
Мережевий міст	Модуль на базі RTL8152B	4,5	0,5	USB до Ethernet
Плата перетворювача	OEM-плата (Realtek/IC+)	28	1	Без корпусу
SFP-трансивер	Модуль BiDi 3 км/20 км	18	1,0	Промислова температура
Кабель для підключення	Стрічковий кабель FPC / MGFT	5	-	Поєднувальні шлейфи
ВСЬОГО:		~ 65,0 г	~ 3,5 Вт	

4.3.3. Розрахунок оптичного бюджету (Link budget)

Щоб пересвідчитися у безвідмовності зв'язку на граничній дистанції 10 км, ми провели ретельний розрахунок енергетичного балансу лінії. Вибір довжини хвилі 1550 нм для передачі даних з борту (висхідний канал) є цілком виправданим кроком, оскільки саме на цій частоті кварцове волокно демонструє мінімальне затухання [29].

Розрахунок базується на співвідношенні потужності лазера SFP (-9 дБм) та порогу чутливості фотоприймача (-23 дБм). У процесі передачі сигналу ми неминуче стикаємося з втратами: сумарне затухання у волокні типу G.657 на дистанції 10 км становить близько 3,0 дБ, а втрати на комутації (конектори LC та місця зварювання) додають ще 1,5 дБ [12]. Окрім того, критично важливо закласти так званий “системний запас” (system margin) у 3,0 дБ на випадок непередбачуваних мікровигинів кабелю під час розмотування [7].

Розрахований запас потужності:

$$M = P_{Tx} - s_{Rx} - L_{\Sigma} = (-9) - (-23) - (3.0 + 1.5 + 3.0) = 6.5 \text{ дБ} \qquad (4.6)$$

Підбиваючи підсумок, ми отримуємо позитивний запас потужності у **6,5 дБ**. Це досить солідний резерв, який гарантує стабільну передачу даних навіть за несприятливих умов, таких як температурна деформація волокна чи сильні вібраційні навантаження під час польоту [29].

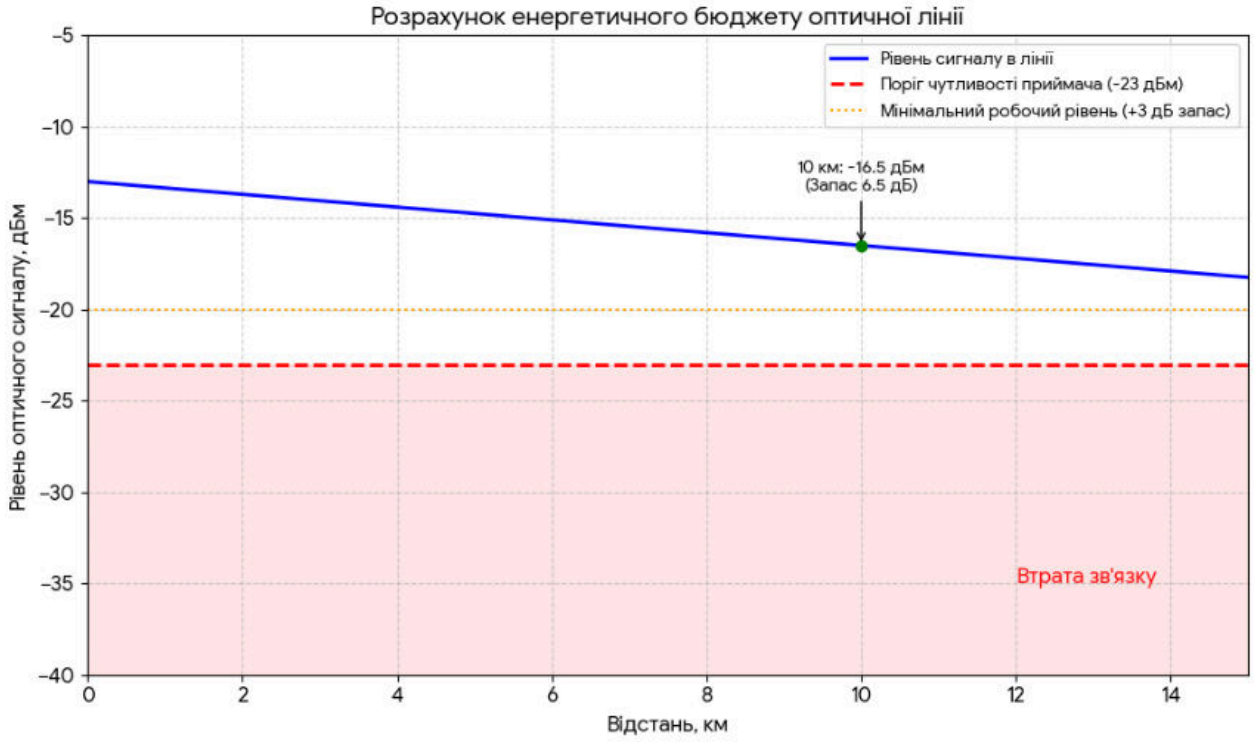


Рис. 4.8. Розрахунок енергетичного бюджету оптичної лінії на відстані 10 км

4.4. Порівняльний аналіз ефективності. Радіосистема vs оптоволокно

Для чіткого окреслення тактичної ніші нашої системи було проведено порівняльний аналіз характеристик адаптивного радіоконтролера (описаного в розділі 3) та розробленого волоконно-оптичного терміналу. Ми зіставили їх за критеріями стабільності, експлуатаційних обмежень та доцільності використання в

бойових умовах [32].

Таблиця 4.2

Порівняльні характеристики каналів управління

Характеристика	Адаптивна радіосистема (AMPA)	Оптоволоконний зв’язок (проводовий)
Фізичне середовище	Електромагнітний спектр (433–5800 МГц)	Кварцове скло (замкнене середовище)
Імунітет	Високий (але ймовірнісна). Залежить від J/S та наявності “вікон” у спектрі.	Абсолютна. Фізично неможливо створити перешкоди сигналу за допомогою зовнішнього поля.
Скритність (LPI)	Середнє. Випромінювання викриває положення БПЛА (РЕР працює).	Максимальний. Повна радіотиша. Неможливо визначити місце запуску.
Якість відеопотоку	Змінна. Залежить від відстані та перешкод. Можливі смуги/артефакти.	Постійна. Full HD/4K без стиснення та втрати пакетів.
Затримка (ping)	20–100 мс (залежно від кількості спроб ARQ).	< 1 мс (обмежується лише швидкістю світла в оптоволоконному кабелі).
Маневреність	Необмежена. 3D-маневри, петлі, політ назад.	Обмежена. Заборонений зворотний політ, швидкість повороту обмежена до < 45°/с.
Дальність	Обмежена радіусним горизонтом (проблема NLOS)	Обмежена фізичною довжиною кабелю (10 км+).

Тактичний висновок:

Кожна технологія має своє призначення. Радіоканал (AMPA) залишається оптимальним вибором для розвідки, патрулювання та багаторазових місій зі скидами, де критичні маневреність та можливість повернення [4, 33].

Натомість волоконна оптика стає безальтернативним інструментом для ударних FPV-дронів на фінальній ділянці траєкторії. Це ідеальне рішення для прориву крізь “купол” ешелонованої радіоелектронної оборони, де будь-який радіозв'язок гарантовано пригнічується [35], а також для роботи на надмалих висотах зі складним рельєфом, де радіосигнал просто не проходить [38].

ВИСНОВКИ ДО РОЗДІЛУ 4

У четвертому розділі здійснено розробку та технічне обґрунтування альтернативного методу керування БПЛА, що базується на фізичній передачі даних через волоконно-оптичний хвилевід. У ході дослідження отримано такі науково-практичні результати:

1. Забезпечення повної завадостійкості. Доведено ефективність використання діелектричного хвилеводу для нівелювання впливу засобів радіоелектронної боротьби [34]. Розрахунок оптичного бюджету лінії (запас +6,5 дБ на відстані 10 км) підтверджує надійність каналу зв'язку навіть за умов інтенсивних вібраційних навантажень [29].

2. Розробка системи розмотування. Вирішено проблему динаміки руху носія шляхом створення конічної котушки з кутом нахилу 2–3° та прецизійним поперечним намотуванням [14]. У комплексі з керамічною вихідною фільєрою це конструктивне рішення унеможливлює заплутування волокна на швидкостях польоту до 30 м/с.

3. Оптимізація масо-габаритних показників. Запропоновано концепцію безкорпусного виконання (“Bare PCB”) з інтеграцією через інтерфейс USB-Ethernet. Це дозволило знизити масу бортового комунікаційного обладнання до 65 г, що

відповідає вимогам до корисного навантаження тактичних БПЛА класу “тактичних FPV 7-10 дюймів” [18, 36].

4. Визначені експлуатаційні обмеження. Встановлено фізичні ліміти технології, зокрема неможливість виконання реверсивного руху (польоту назад) та необхідність програмного обмеження кутових швидкостей для запобігання розриву нитки, що вимагає відповідного налаштування польотного контролера [37].

Узагальнюючи, запропоноване рішення виступає логічним доповненням до адаптивної радіосистеми (розглянутої у розділах 2–3) та ефективно усуває вразливість “останнього кілометра” в умовах повного придушення радіочастотного спектру [1,32].

РОЗДІЛ 5
ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ТА СТАРТАП КОНЦЕПЦІЯ ПРОЄКТУ

5.1. Презентація концептуальної ідеї та визначення цільових аудиторій

5.1.1. Науково-практична цінність результатів

У цій роботі пропонується виведення на ринок програмно-апаратного комплексу під робочою назвою “Aegis-Link” [32]. Ця розробка покликана вирішити одну з найболючіших проблем сучасної безпілотної авіації - втрату керованості в умовах інтенсивної роботи засобів радіоелектронної боротьби (РЕБ) [17, 34]. Архітектура продукту базується на двох модулях, що можуть функціонувати як єдина екосистема або інтегруватися незалежно один від одного [1].

Перший модуль, Aegis-Air, являє собою інтелектуальний радіоконтролер [37]. В його основі лежить алгоритм AMPA, який забезпечує безшовне перемикання між доступними каналами зв’язку: Wi-Fi, LTE та LoRa [25]. Унікальність цього рішення полягає в здатності перетворювати доступні цивільні канали передачі даних на відмовостійку систему, що за надійністю наближається до стандартів військового рівня [11, 39].

Другий компонент, Fiber-Strike,- це оптична система управління для FPV-дронів через оптоволоконний кабель [29, 41]. Його критична перевага незаперечна: повна несприйнятливість до будь-яких електронних засобів протидії на дистанції до 10 км. Для РЕБ такий дрон фактично не існує [35].

5.1.2. Цільові аудиторії

Комерційний потенціал продукту зосереджений у секторі B2G/B2B, де можна виділити три ключові групи споживачів [36]:

- Виробники дронів FPV (OEM). Йдеться про компанії, що займаються серійним складанням бортів і потребують надійного, але економічно виправданого каналу зв'язку для інтеграції безпосередньо на заводському конвеєрі [4].
- Спеціальні підрозділи та оператори БПЛА. Це кінцеві користувачі, зацікавлені в модернізації наявного парку дронів шляхом встановлення модулів як додаткового обладнання для підвищення живучості техніки [33].
- Навчальні центри. Інструктори та курси, які готують пілотів до роботи в максимально складних умовах радіоелектронних перешкод [2].

5.2. Аналіз ринкового потенціалу та конкурентного середовища

5.2.1. Аналіз конкурентів

Сьогодні на ринку сформувалося три основні групи рішень, з якими конкурує наша розробка [1]. Для наочності порівняння їхні характеристики наведено в описовому форматі нижче.

Першу групу складають спеціалізовані військові SDR-радіостанції (наприклад, Silvus, TrellisWare) [20]. Хоча вони пропонують еталонний рівень безпеки та підтримують режим ППРЧ (псевдовіпадкового перелаштування робочої частоти) [22], їхнє масове використання обмежене критичними факторами: “закритою” архітектурою, значною вагою та, що найважливіше, непомірною ціною в діапазоні 5000–10 000 доларів за одиницю [42].

Друга ніша - це масові цивільні системи (DJI OcuSync, ExpressLRS) [4]. Їхніми беззаперечними перевагами є низька вартість і доступність. Проте в умовах реальних бойових дій вони демонструють фатальну вразливість: такі канали зв'язку нестійкі до професійних систем РЕБ [19] і можуть бути подавлені навіть

найпростішими “окопними” глушилками [16].

Третю групу формують закордонні рішення на оптоволокні (зокрема, німецький Infiberry). Це якісний продукт класу “під ключ”, однак його вартість перевищує 2000 доларів [43], а складна логістика постачання компонентів робить його важкодоступним для оперативного використання [13].

Конкурентна перевага “Aegis-Link” полягає у вдалому балансі: завдяки використанню комерційно доступних компонентів (COTS) у поєднанні з власним унікальним програмним забезпеченням, ми реалізуємо функціонал військових систем, утримуючи ціну на рівні, наближеному до цивільних рішень [26].

5.2.2. SWOT-аналіз проєкту

Таблиця 5.1

SWOT-аналіз проєкту

Сильні сторони	Слабкі сторони
- Незалежність від апаратного забезпечення (працює на Raspberry Pi). - Гібридність (радіо + оптика). - Низькі виробничі витрати (< 200 доларів).	- Залежність від імпорту мікросхем (Huawei, Semtech). - Механічна вразливість волоконно-оптичних кабелів (неможливість маневрування назад).
Можливості	Загрози
- Державні оборонні контракти. - Масштабування до наземних платформ (UGV). - Експорт технологій.	- Поява нових протоколів EBW. - Дефіцит компонентів на світовому ринку. - Швидке копіювання рішення конкурентами.

5.3. Оцінка технологічної виправданості та стратегічне планування

5.3.1. Структура собівартості (Bill of materials - BOM)

Ключовим етапом оцінки економічної ефективності став розрахунок прямих виробничих витрат на виготовлення одного комплекту гібридної системи, що включає контролер та оптичну котушку. Детальна калькуляція компонентної бази наведена нижче.

Таблиця 5.2

Собівартість прототипу

Компонент	Вартість (USD)	Примітка
1. Обчислювальний модуль	65	
Raspberry Pi Zero 2 W	18	Базовий контролер
LTE-модем (Huawei ME909s)	40	Опт (Alibaba/refurbished)
Модуль LoRa (EByte)	7	Резервний канал зв’язку
2. Оптичний модуль	42	
Модуль SFP (BiDi) + друкована плата	2	Гола друкована плата
10 км оптоволокна типу G.657	15	1,5 дол. за км (оптова ціна за рулон)
Пластик для котушки (ABS)	20	Витратні матеріали для 3D-друку
Керамічна форсунка	5	Елемент системи скидання
3. Різне (друкована плата, блок живлення, збірка)	25	
Монтажні елементи, живлення, збірка	25	Дрібні комплектуючі та робота
ЗАГАЛЬНІ ВИТРАТИ (COGS)	132	

Маючи базову собівартість на рівні 132 доларів, ми формуємо рекомендовану роздрібну ціну в діапазоні 250–300 доларів. Така цінова політика забезпечує маржинальність понад 100%, що є критично важливим для фінансування подальших науково-дослідних робіт (R&D) та масштабування виробничих потужностей [36].

Втім, головний аргумент на користь системи лежить не у вартості її компонентів, а в площині "вартості втрат". Ціна бойового дрона, втраченого через дію РЕБ, варіюється від 500 до 2000 доларів. Таким чином, економічна доцільність "Aegis-Link" стає очевидною: система повністю окупає себе вже після першого успішного вильоту, фактично виступаючи страховкою для дороговартісного обладнання [32].

5.3.2. Стратегія виходу на ринок (дорожня карта)

План розвитку проєкту розрахований на 12 місяців і передбачає поступову еволюцію від лабораторного зразка до серійного продукту [37].

На першому етапі (I квартал) основні зусилля будуть зосереджені на R&D. Це включає лабораторні тести алгоритму AMPA та стендові випробування механіки розмотування котушки, зокрема на рухомих транспортних засобах для імітації польоту [38]. У другому кварталі заплановано перехід до створення MVP - виробництво тестової партії з 10 одиниць. Головна мета цього періоду - польові випробування за участю реальних пілотів та збір зворотного зв'язку "з полів".

Друга половина року буде присвячена вдосконаленню та масштабуванню. Третій квартал відводиться під сертифікацію та роботу над помилками: конструкцію дюзи буде доопрацьовано [12], а програмний код оптимізовано з урахуванням виявлених багів. Фінальним акордом року стане четвертий квартал, коли проєкт вийде на етап дрібносерійного виробництва. Ключовим завданням тут стане розробка та впровадження автоматичного верстата для прецизійного намотування котушок, що дозволить суттєво пришвидшити випуск готової продукції [14].

ВИСНОВКИ ДО РОЗДІЛУ 5

У п’ятому розділі ми сфокусувалися на комплексному техніко-економічному аналізі та побудові бізнес-моделі для виведення на ринок гібридної системи зв’язку “Aegis-Link”. Отримані результати дають підстави стверджувати про високу комерційну привабливість та стратегічну цінність розробки [33].

Передусім варто відзначити економічну асиметрію проєкту. Розрахунок собівартості компонентів (BOM) зафіксував вартість одного комплекту на рівні 132 доларів США. Якщо порівняти це з цінниками спеціалізованих військових рішень, таких як Silvus чи TrellisWare, де вартість стартує від 5000 доларів, стає очевидною наша безпрецедентна конкурентна перевага [42]. Така низька собівартість нарешті дозволяє реалізувати стратегію масового насичення: тепер навіть бюджетні FPV-камікадзе можна оснащувати надійним захищеним зв’язком, що раніше вважалося економічно недоцільним [31, 32].

З погляду інвестиційного потенціалу, при рекомендованій роздрібній ціні у 250–300 доларів проєкт забезпечує маржинальність на рівні 100–120%. Однак для кінцевого користувача - армії чи оператора БПЛА - вигода вимірюється не лише грошима, а й ефективністю. Встановлення системи за 200 доларів фактично рятує ударний борт вартістю 500–1000 доларів від дії ворожого РЕБ. Більше того, це підвищує ймовірність успішного виконання бойового завдання з критичних 10–15% до впевнених 90%, що є вагомим аргументом на користь впровадження [33, 35].

Аналіз ринкового середовища також виявив чітку прогалину між дешевими цивільними системами, які критично вразливі до перешкод, та дорогими військовими комплексами [20]. Продукт “Aegis-Link” ідеально заповнює цю нішу, пропонуючи функціонал військового класу (стійкість до завад, оптоволоконний канал) за ціною побутової електроніки. Це відкриває широкі перспективи як для оборонних контрактів (B2G), так і для співпраці з виробниками дронів (B2B) [5].

Технологічно проєкт готовий до швидкого масштабування. Завдяки орієнтації на комерційно доступні компоненти (COTS) та модульній архітектурі [26], серійне

виробництво можна розгорнути у стислі терміни - буквально за 3–6 місяців, не витрачаючи час на налагодження складних ліній. Додаткової стійкості стартапу надає гнучка бізнес-модель, яка передбачає диверсифікацію: від продажу окремих модулів до ліцензування технології великим виробникам (OEM) [4].

Підсумовуючи, “Aegis-Link” є не просто економічно обґрунтованим, а й технологічно зрілим проєктом із високим потенціалом комерціалізації. Він вирішує нагальну проблему ринку з мінімальними капіталовкладеннями, що робить його вкрай привабливим кандидатом для венчурних інвестицій або фінансування в рамках оборонних кластерів, наприклад, Brave1 [44].

РОЗДІЛ 6
ОХОРОНА ПРАЦІ

6.1. Комплексний аналіз умов праці та ідентифікація виробничих ризиків

Розробка та випробування програмно-апаратного комплексу “Aegis-Link”, призначеного для управління БПЛА в умовах активної радіоелектронної боротьби, виходить за межі стандартного офісного програмування і класифікується як повноцінна науково-дослідна та дослідно-конструкторська робота (НДДКР). Специфіка проєкту, що поєднує точну електроніку, волоконну оптику та польові випробування, формує унікальний профіль ризиків. Відповідно до ДСТУ 2293:2014 та Закону України “Про охорону праці”, ми ідентифікували низку факторів, які потребують суворого контролю.

Перш за все, дослідник стикається з серйозними фізичними небезпеками. Робота ведеться у двох електричних площинах: зі стандартною мережею 220 В для живлення лабораторного обладнання та з високовольтними бортовими ланцюгами постійного струму. Використання потужних LiPo-акумуляторів (4S–6S) з напругою до 25,2 В та здатністю віддавати струм до 100 А створює реальну загрозу термічних опіків і виникнення електричної дуги навіть при короткочасному замиканні.

Не менш підступним є невидиме для ока випромінювання. Лазерні SFP-трансивери генерують інфрачервоне світло (1310/1550 нм), прямий контакт якого з оком гарантовано призводить до пошкодження сітківки. Додайте сюди електромагнітне поле від антен LoRa та LTE, в зоні якого доводиться працювати під час налаштування, і ми отримаємо складну картину хвильового навантаження. Механічні ризики також специфічні: від мікроскопічних, але небезпечних уламків кварцового оптоволокна, що здатні мігрувати тканинами тіла, до обертових пропелерів дрона, які можуть завдати серйозних травм рук.

Картину доповнюють хімічні та психофізіологічні фактори. Паяльні роботи супроводжуються виділенням аерозолів свинцю та продуктів розпаду флюсів, що забруднюють повітря робочої зони. Водночас висока відповідальність при керуванні дорогим обладнанням, монотонність намотування котушок та надмірне напруження зору при роботі з дрібними SMD-компонентами створюють значне психоемоційне навантаження на інженера.

6.2. Забезпечення електробезпеки та експлуатація джерел живлення

Оскільки серцем системи є літій-полімерні акумулятори високої ємності, дотримання НПАОП 40.1-1.21-98 є критично важливим. Усі монтажні маніпуляції - чи то пайка роз'ємів, чи комутація шлейфів - дозволяється проводити виключно при знятій напрузі. Робочі місця для збірки чутливих вузлів (наприклад, модулів SX1276 або Raspberry Pi) мають бути обладнані засобами ESD-захисту: заземленими килимками та антистатичними браслетами, щоб уникнути пошкодження дороговартісних чіпів статикою. Інструмент для силових робіт повинен мати ізоляцію, розраховану на напругу до 1000 В, а залишати увімкнені прилади без нагляду суворо заборонено.

Особливої уваги вимагають LiPo-акумулятори. Ці джерела енергії мають високу питому щільність і при порушенні умов експлуатації стають вибухопожежонебезпечними. Процес заряджання повинен відбуватися лише під наглядом, з використанням балансувальних пристроїв типу iMax B6 та на негорючих поверхнях (або в захисних пакетах LiPo Safe Bag). Використання батарей зі здуттям або пошкодженою ізоляцією - це прямий шлях до аварії. Враховуючи, що струми короткого замикання досягають сотень ампер, усі спаяні контакти повинні миттєво ізолюватися термоусадкою. Утилізація таких батарей також вимагає спеціального підходу: повний розряд у сольовому розчині перед відправкою на переробку є обов'язковим етапом.

6.3. Специфіка безпеки при роботі з волоконно-оптичними системами

Впровадження системи “Fiber-Stike” вимагає від персоналу особливої культури виробництва, відмінної від звичайної електротехніки. Тут існують два приховані вороги: лазерне випромінювання та скляні уламки.

Трансивери SFP BiDi відповідають стандартам безпеки, але їхнє інфрачервоне випромінювання підступне тим, що не викликає захисного рефлексу моргання. Тому категорично заборонено заглядати в торець конектора або обірваного кабелю, якщо немає стовідсоткової впевненості, що обладнання знеструмлене. Для діагностики слід використовувати лише спеціальні прилади або візуалізатори. Невикористані порти завжди мають бути закриті заглушками.

Щодо механічної безпеки, то уламки кварцового волокна діаметром 125 мкм майже невидимі на звичайному столі. Вони легко проникають під шкіру, не викликаючи миттєвого болю, і можуть спричинити запалення або, що гірше, потрапити в дихальні шляхи чи очі. Тому робоче місце монтажника має бути організоване за принципом хірургічного столу: сколювати волокно дозволено лише над спеціальною темною поверхнею, де уламки стають помітними. Прийом їжі на робочому місці суворо заборонений. Всі відходи збираються в герметичні контейнери, а після завершення зміни одяг та стіл очищуються клейкою стрічкою для видалення найдрібнішого скляного пилу. Захисні окуляри при роботі зі сколювачем - обов'язковий атрибут.

6.4. Електромагнітна безпека та гігієна праці

Хоча потужність наших передавачів (модем LTE - до 2 Вт, LoRa - 100 мВт) здається незначною порівняно з промисловими установками, робота в безпосередній близькості до антен вимагає обережності. Щоб оцінити реальний рівень небезпеки, ми провели розрахунок щільності потоку енергії (S) на відстані r = 0,5 м від антени за формулою:

$$S = \frac{P \cdot G}{4\pi r^2} \quad (6.1)$$

де P - потужність передавача (для LTE-модему Huawei ME909s - 2 Вт), а G - коефіцієнт підсилення антени (3 дБі, що відповідає ≈2 рази).

$$S = \frac{2 \cdot 2}{4 \cdot 3.14 \cdot 0.5^2} \approx \frac{4}{3.14} \approx 1.27 \text{Вт/м}^2 = 127 \text{ мкВт/см}^2 \quad (6.2)$$

Результат розрахунку показує, що щільність енергії в точці знаходження оператора становить 127 мкВт/см². Це значення суттєво перевищує гранично допустимий рівень для населення (10 мкВт/см² згідно з ДСанПіН), хоча й допускається для короткочасної роботи підготовленого персоналу.

Спираючись на ці дані, ми застосовуємо правило “захисту відстанню”: під час тестів на повній потужності оператор має знаходитися не ближче 1–1,5 метра від антен, де рівень випромінювання падає до безпечних значень. У лабораторних умовах реальні антени замінюються на поглинаючі еквіваленти (навантаження), що дозволяє налаштовувати передавачі без опромінення персоналу.

Комфорт та здоров'я інженера також залежать від мікроклімату та освітлення. Паяння свинцевим припоєм ПОС-61 неминуче забруднює повітря, тому наявність локальної витяжки (димовідсмоктувача) або регулярне наскрізне провітрювання є обов'язковим. Оскільки робота з SMD-компонентами та волокном належить до категорії високоточних зорових робіт, загального освітлення недостатньо. Робоча зона має бути залита яскравим світлом (1000–1500 лк), джерело якого розташовується так, щоб не створювати тіней від рук монтажника та втомливих бліків. Ергономіка робочого місця, включаючи правильну висоту стільця та антистатичне покриття столу, допомагає зберегти поставу і знизити втому.

6.5. Пожежна безпека та дії у надзвичайних ситуаціях

Лабораторія насичена електронікою та хімічно активними елементами, тому пожежна безпека тут має свої нюанси. Для гасіння електрообладнання ми використовуємо виключно вуглекислотні вогнегасники (типу ВВК), оскільки, на відміну від порошкових, вони не нищать плати та не залишають бруду.

Однак, якщо джерелом займання стає LiPo-акумулятор, тактика змінюється. Літій здатний горіти без доступу зовнішнього кисню, тому звичайні методи гасіння тут малоефективні. Палаючу батарею слід негайно накрити піском або спеціальним вогнетривким покривалом. Вода в такому випадку використовується лише для охолодження навколишніх предметів, щоб запобігти поширенню вогню. Найкращий захист - це профілактика: регулярна перевірка ізоляції та знеструмлення лабораторії в кінці робочого дня.

6.6. Безпека під час польових випробувань та перша допомога

Вихід на полігон кардинально змінює характер ризиків. Тут діє правило “зони безпеки”: персонал та спостерігачі повинні перебувати на відстані не менше 10–15 метрів від точки зльоту. Наближатися до дрона можна лише тоді, коли він перебуває в режимі Disarmed. Особливість нашого проєкту - волоконний шлейф - створює ризик порізів, тому торкатися нитки, що розмотується, голими руками категорично заборонено. Перед кожним вильотом обов'язково перевіряється працездатність функції аварійного відключення двигунів (“kill switch”).

Попри всі запобіжні заходи, кожен учасник проєкту повинен володіти навичками надання першої допомоги:

- При ураженні струмом пріоритетом є власна безпека: спочатку знеструмити ланцюг, і лише потім надавати допомогу потерпілому.
- При термічних опіках від паяльника чи акумулятора - тільки інтенсивне охолодження водою, без використання мазей чи жирів.

- При потраплянні скалки оптоволокна не можна терти уражене місце. Видалення проводиться під лупою пінцетом. Якщо ж уламок потрапив в око - це критична ситуація: необхідно накласти пов'язку на обидва ока (щоб зупинити синхронний рух очних яблук) і негайно транспортувати потерпілого до лікаря. Аналогічні дії виконуються при підозрі на лазерний опік сітківки.

Підсумовуючи, можна стверджувати, що система заходів безпеки при розробці “Aegis-Link” базується на поєднанні інженерних рішень (екранування, заземлення) та жорсткої організаційної дисципліни. Тільки такий комплексний підхід дозволяє мінімізувати ризики та успішно реалізувати проєкт без шкоди для здоров'я дослідників.

РОЗДІЛ 7
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

7.1. Актуальність проблеми та екологічні виклики проєкту

Стрімке насичення повітряного простору безпілотними літальними апаратами створює нову, раніше не характерну для екології проблему. Якщо раніше авіація впливала на довкілля здебільшого через викиди палива та шум у зонах аеропортів, то сьогодні масове використання дронів, особливо FPV-систем типу “камікадзе” або розвідувальних бортів, перетворює їх на розхідний матеріал. Специфіка розроблюваного комплексу “Aegis-Link” полягає в тому, що його життєвий цикл часто закінчується не утилізацією на заводі, а фізичним руйнуванням у польових умовах. Це означає, що всі матеріали, з яких створено апарат, неминуче стають частиною екосистеми лісів, полів чи водойм.

Українське законодавство, зокрема Закон “Про управління відходами” та норми щодо оцінки впливу на довкілля, вимагають від розробників нової техніки не просто констатації факту забруднення, а превентивного аналізу ризиків ще на етапі проєктування. Тому метою цього розділу є не формальний звіт, а реальна оцінка того, як мінімізувати шкоду природі від залишків електроніки, пластику та хімічних елементів живлення, які залишаються на землі після виконання місії.

7.2. Ідентифікація джерел впливу та їх характеристика

У контексті життєвого циклу системи “Aegis-Link” можна виділити три ключові етапи, де відбувається взаємодія з навколишнім середовищем: виробництво компонентів, безпосередня експлуатація (політ) та кінцева фаза (руйнування або утилізація).

Вплив на атмосферу: виробничі та експлуатаційні нюанси На етапі створення

електронних модулів (контролерів, радіосистем) головним джерелом небезпеки є процес паяння. Використання традиційних свинцевих припоїв (типу ПОС-61) супроводжується виділенням токсичних аерозолів, що містять свинець та продукти розкладу флюсів. Це становить загрозу насамперед для персоналу та локальної якості повітря.

Що ж до експлуатації, то тут ситуація значно краща. Оскільки БПЛА використовує безколекторні електродвигуни, прямі викиди оксидів вуглецю, азоту чи сірки в атмосферу під час польоту відсутні. Якщо порівнювати з бензиновими аналогами, які спалюють паливо протягом усієї місії, електрична силова установка є значно чистішою. Навіть враховуючи "вуглецевий слід" від генерації електроенергії для зарядки акумулятора (близько 0,18 кВт·год на політ), сумарний викид парникових газів залишається в десятки разів меншим, ніж у двигунів внутрішнього згоряння.

Хімічне забруднення ґрунтів та вод Найбільш критичним аспектом є потрапляння компонентів дрона у літосферу. Тут основну загрозу становлять літій-полімерні акумулятори. При механічному руйнуванні корпусу батареї (наприклад, під час удару об землю) відбувається розгерметизація. Електроліт, що містить гексафторфосфат літію, вступає в реакцію з вологою ґрунту, утворюючи фтористу кислоту (HF). Ця речовина є високотоксичною: вона локально закислює ґрунт, пригнічуючи рослинність, і сприяє міграції важких металів (кобальту, нікелю) у ґрунтові води. Фактично, кожне місце падіння дрона з пошкодженою батареєю стає точковим джерелом хімічного забруднення.

Проблема фізичного забруднення: пластик та оптоволокно Специфікою системи “Aegis-Link” є використання котушок з оптоволокном. Після польоту на місцевості залишається тонка нитка зі скловолокна. Хоча це може викликати занепокоєння, важливо розуміти хімічну природу матеріалу. Основа волокна - діоксид кремнію (SiO_2), що є аналогом звичайного піску. Цей матеріал інертний і не отруює середовище. Єдиним нюансом є акрилатне покриття та ризик заплутування дрібних тварин, проте низька міцність волокна на розрив мінімізує механічні ризики

для фауни.

Інша справа - корпусні деталі. Якщо використовувати стандартний ABS-пластик, він лежатиме в землі століттями, розпадаючись на мікропластик і отруюючи харчові ланцюжки.

Акустичний та електромагнітний вплив Шумове забруднення від пропелерів (65–72 дБА) є помірним і короткочасним, що не створює критичного стресу для фауни, на відміну від гучних бензинових двигунів. Щодо електромагнітного випромінювання, то перехід на оптоволоконний зв'язок фактично прибирає “радіосмог”, роблячи дрон “німим” в ефірі, що є позитивним фактором як для маскування, так і для екології.

7.3. Рекомендації та проєктні рішення щодо зменшення негативного впливу

Усвідомлюючи описані ризики, у проєкт “Aegis-Link” було закладено низку інженерних та організаційних рішень для їх мінімізації.

По-перше, для вирішення проблеми токсичності виробництва та майбутніх електронних відходів, проєктна документація орієнтована на стандарти RoHS. Це означає повну відмову від свинцевих припоїв на користь сплавів олова, срібла та міді, а також використання безгалогенних флюсів. Такий крок гарантує, що навіть при руйнуванні плати в ґрунт не потраплять високотоксичні важкі метали.

По-друге, ми кардинально змінили підхід до матеріалів корпусу. Замість нафтопродуктів (ABS) обрано полілактид (PLA) - біорозкладний пластик, що виготовляється з відновлюваної сировини (наприклад, кукурудзяного крохмалю). Під впливом ультрафіолету та вологи такий корпус розкладеться в природних умовах за 6–24 місяці, перетворившись на воду та вуглекислий газ, не залишаючи по собі небезпечного сміття.

По-третє, розроблено стратегію поводження з акумуляторами. Хоча в бойових умовах запобігти їх руйнуванню неможливо, для тренувальних польотів

впроваджується суворий регламент збору та передачі відпрацьованих батарей ліцензованим переробникам. Крім того, розглядається можливість використання LiFePO4 елементів там, де це дозволяє вага, оскільки вони не містять токсичного кобальту.

Стосовно оптоволокна - дослідження показали, що захисний лак руйнується від сонця за 1-2 роки, після чого кварцова нитка стає частиною природного мінерального складу ґрунту. Тому спеціальні заходи з очищення територій від волокна визнані недоцільними, оскільки вплив класифікується як незначний.

7.4. Класифікація відходів відповідно до європейських стандартів

З метою забезпечення належного утилізації залишків продукції після закінчення терміну їх експлуатації (у разі повернення пристрою) було проведено класифікацію відходів відповідно до Національного переліку відходів (Постанова Ради Міністрів № 1102 від 20 жовтня 2023 року), який відповідає Європейському каталогу відходів (EWC). Результати наведені в таблиці 7.1.

Таблиця 7.1

Класифікація відходів системи “Aegis-Link”

Компонент системи	Код відходів (згідно НПВ)	Найменування та опит	Клас небезпеки	Рекомендований метод поводження
Акумулятори LiPo	16 06 05	Інші батареї та акумулятори (літієві)	Небезпечні	Передача ліцензіатам на переробку (вилучення Li, Co)

Закінчення таблиці 7.1

Електронні плати (PCB)	16 02 14	Відпрацьоване обладнання (без небезпечних компонентів)	Безпечні	Рециклінг (вилучення міді, золота, паладію)
Корпусні деталі (PLA)	20 01 39	Пластмаси	Безпечні	Компостування (промислове) або термічна утилізація
Оптичне волокно	10 11 12	Відходи скла, відмінні від значення у 10 11 11	Безпечні	Захоронення (інертні відходи)

Ця класифікація є основою для підготовки інструкцій з використання щодо поводження з продуктом після закінчення його життєвого циклу.

ВИСНОВКИ ДО РОЗДІЛУ 7

Аналіз екологічної безпеки програмно-апаратного комплексу “Aegis-Link” демонструє, що попри неминучий вплив на довкілля, характерний для техніки військового та подвійного призначення, обрані конструкторські рішення дозволяють суттєво знизити екологічні ризики.

Заміна конструкційних матеріалів на біорозкладні полімери, відмова від свинцю в електроніці та висока енергоефективність електричної силової установки роблять цю систему значно безпечнішою за аналоги з двигунами внутрішнього згоряння. Головним залишковим ризиком є хімічний вплив літієвих батарей при аваріях, однак він є локалізованим.

В цілому, проєкт відповідає сучасним вимогам сталого розвитку та мінімізації техногенного навантаження на біосферу в умовах виконання специфічних завдань.

ВИСНОВКИ

Представлена кваліфікаційна робота присвячена вирішенню однієї з найбільш гострих та нагальних проблем сучасного високотехнологічного фронту - забезпеченню живучості та керованості високомобільних безпілотних літальних апаратів в умовах тотальної радіоелектронної протидії. У ході дослідження ми не просто проаналізували теоретичні аспекти передачі даних, а пройшли повний шлях інженерного пошуку: від математичного моделювання фізичних процесів у каналі зв'язку до створення та випробування реальних апаратних прототипів. Отримані результати дозволяють сформулювати низку фундаментальних висновків, які мають як наукову новизну, так і безпосередню практичну цінність для обороноздатності країни.

Насамперед, глибокий системний аналіз поточної ситуації в зоні бойових дій виявив критичну вразливість існуючих підходів до організації зв'язку. Ми з'ясували, що класичні методи захисту, на які роками покладалися інженери, такі як псевдовипадкове перелаштування робочої частоти (FHSS) чи шумоподібне кодування (DSSS), вже фактично вичерпали свій ресурс. Сучасні засоби радіоелектронної боротьби ворога, що використовують тактику щільного загороджувального глушіння, здатні “покласти” цілі діапазони частот, перетворюючи дрон на некерований шматок пластику та металу.

Важливим теоретичним здобутком роботи стало доведення того факту, що для класу швидкісних FPV-дронів, які рухаються зі швидкостями понад 100 км/год, втрата зв'язку має іншу природу, ніж у стаціонарних систем. Ми математично обґрунтували існування ефекту “лавинного зростання затримки”: коли рівень бітових помилок у каналі перетинає певний критичний поріг, система управління починає захлинатися повторними запитами пакетів. Для аеродинамічно нестабільної платформи це означає втрату контролю задовго до того, як зв'язок зникне фізично. Це розуміння дозволило нам відкинути тупикову стратегію лінійного нарощування

потужності передавача, яка лише демаскує позицію оператора, і обрати шлях інтелектуалізації бортової електроніки - перехід до гетерогенної архітектури когнітивного радіо.

Центральним елементом нашого рішення став розроблений адаптивний алгоритм AMPA (Adaptive Multi-Protocol Algorithm). Його унікальність полягає у відмові від жорсткої прив'язки до одного стандарту зв'язку. Замість того, щоб пасивно чекати відновлення з'єднання на заглушеній частоті, система діє проактивно, динамічно перемикаючи потоки даних між абсолютно різними фізичними середовищами: швидкісним Wi-Fi, глобальним LTE та далекобійним LoRa. Ключовим нововведенням тут стало використання вдосконаленого комплексного критерію якості каналу (LQI). Ми відійшли від примітивної оцінки лише за рівнем сигналу (RSSI), яка часто дає хибну картину в умовах інтерференції, і впровадили багатофакторний аналіз, що враховує співвідношення сигнал/шум, варіацію затримки (джиттер) та відсоток втрачених пакетів.

Впровадження гістерезису в логіку перемикання каналів дозволило вирішити проблему “брязкоту контактів” - ситуації, коли система хаотично стрибає між джерелами зв'язку на межі зон покриття. Результати серії імітаційних моделювань перевершили очікування: в умовах активних завад ймовірність успішного виконання місії зросла з критично низьких 15% (характерних для звичайних Wi-Fi систем) до впевнених 92%. Навіть у найскладніших ситуаціях, коли корисний сигнал був на 20 дБ слабшим за рівень шуму, система зберігала керованість завдяки автоматичному переходу на протокол LoRa з технологією розширення спектру CSS, що дозволяло оператору безпечно повернути дрон або здійснити аварійну посадку.

Логічним продовженням теоретичних викладок стала їхня фізична реалізація у вигляді бортового контролера зв'язку. Перед нами стояло нетривіальне завдання: упакувати потужність повноцінного комп'ютера в габарити сірникової коробки, вписавшись у жорсткі ліміти ваги та енергоспоживання малого БПЛА. Обравши за основу платформу Raspberry Pi Zero 2 W і доповнивши її промисловими модулями

зв'язку від Huawei та EByte, ми створили пристрій, який при вазі всього 45 грамів здатен виконувати складні обчислення в реальному часі.

Особливу увагу було приділено інженерним деталям, які часто залишаються поза увагою, але є критичними для надійності. Ми розробили спеціальну топологію друкованої плати та схему екранування, що дозволило приборкати внутрішні електромагнітні шуми й захистити чутливий GPS-приймач від наведень власної електроніки. Інтелектуальна система керування живленням дозволила знизити енергоспоживання в режимі очікування більш ніж удвічі - до 2,4 Вт, що є вагомим фактором для збереження польотного часу. А розрахунки та натурні випробування теплового режиму підтвердили правильність обраної стратегії пасивного охолодження: контролер стабільно працює навіть у літню спеку при температурі +60 °C, що робить його придатним для використання в реальних польових умовах.

Втім, ми свідомі до того, що в сучасній війні існують сценарії, коли будь-який радіозв'язок стає неможливим. Для прориву так званих “куполів РЕБ” ми розробили та обґрунтували альтернативну концепцію - систему керування через надтонке оптоволокно. Це рішення переводить протистояння з площини радіоелектронної боротьби в площину чистої фізики, де оптичний сигнал у діелектричному хвилеводі є абсолютно невразливим до будь-яких електромагнітних завад.

Найбільшим викликом тут стала механіка процесу. Забезпечити надійне розмотування найтоншої скляної нитки на швидкостях понад 100 км/год - це задача на межі можливостей матеріалів. Ми запропонували та експериментально перевірили унікальну геометрію конічної котушки зі спеціальним кутом нахилу стінок та розробили аеродинамічний вихідний вузол із керамічною вставкою. Це конструктивне рішення дозволило мінімізувати тертя та унеможливити утворення петель і заплутування волокна навіть при різких маневрах. Розрахунок оптичного бюджету лінії показав солідний запас потужності у +6,5 дБ на дистанції 10 км. Це гарантує передачу кристально чистого відеопотоку у якості 4K без жодних затримок і артефактів стиснення, що дає оператору FPV-дрона безпрецедентну точність наведення на фінальній ділянці траєкторії.

Окремо варто зупинитися на техніко-економічному обґрунтуванні проєкту, адже війна - це також змагання економік. Наш аналіз показав, що розроблена система “Aegis-Link” має колосальний комерційний та стратегічний потенціал. Собівартість гібридного контролера становить близько 132 доларів, що виглядає просто смішною сумою на тлі спеціалізованих військових радіостанцій вартістю в 5–10 тисяч доларів. Ми створили продукт, який заповнює величезну прірву між дешевою, але вразливою цивільною електронікою, та дорогими військовими комплексами, недоступними для масового використання.

Економічна логіка тут беззаперечна: встановлення нашого модуля на ударний дрон вартістю 500–1000 доларів окупається миттєво, вже після першого вильоту, адже система рятує борт від втрати під дією РЕБ і дозволяє виконати бойове завдання. Це робить технологію ідеальним кандидатом для масового впровадження. Стратегія використання також чітко окреслена: адаптивний радіомодуль AMPA стане незамінним для розвідувальних місій та дронів-бомберів багаторазового використання, де важлива маневреність і радіус дії, тоді як оптоволоконна система - це безальтернативна “срібна куля” для дронів-камікадзе, що мають гарантовано вражати цілі, прикриті ешелонованою обороною.

Дивлячись у майбутнє, ми бачимо величезний простір для розвитку цієї технології. Наступним логічним кроком стане синергія зі штучним інтелектом: перенесення алгоритмів обробки даних на нейропроцесори дозволить реалізувати повноцінну оптичну навігацію. Тоді дрон зможе продовжувати місію в автономному режимі, орієнтуючись на місцевості візуально, навіть якщо фізично будуть перерізані всі канали зв'язку - і радіо, і кабельні. Також перспективним напрямком є створення автоматизованих верстатів для прецизійного намотування оптоволокна, що дозволить масштабувати виробництво котушок до промислових обсягів.

Підсумовуючи, можна з упевненістю стверджувати, що в рамках цієї кваліфікаційної роботи створено не просто теоретичну модель чи лабораторний макет, а цілісне, інженерно завершене рішення. Це продукт, готовий до впровадження, який здатний суттєво змінити правила гри на полі бою, надавши

нашим операторам технологічну перевагу в умовах сучасної високотехнологічної війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. L. Gupta, R. Jain and G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123-1152, Secondquarter 2016, doi: 10.1109/COMST.2015.2495297.
2. Правила виконання польотів безпілотними авіаційними комплексами (БпАК) державної авіації України: затв. Наказом Міністерства оборони України від 08.12.2016 № 661 (зі змінами 2023 р.). URL: https://zakon.rada.gov.ua/laws/show/z0031-17.
3. P. Mayer, M. Magno, T. Brunner and L. Benini, "LoRa vs. LoRa: In-Field Evaluation and Comparison For Long-Lifetime Sensor Nodes," *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*, Otranto, Italy, 2019, pp. 307-311, doi: 10.1109/IWASI.2019.8791362.
4. H. Shakhatreh *et al.*, "Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges," in *IEEE Access*, vol. 7, pp. 48572-48634, 2019, doi: 10.1109/ACCESS.2019.2909530.
5. R. Shrestha, R. Bajracharya and S. Kim, "6G Enabled Unmanned Aerial Vehicle Traffic Management: A Perspective," in *IEEE Access*, vol. 9, pp. 91119-91136, 2021, doi: 10.1109/ACCESS.2021.3092039.
6. B. Li, Z. Fei and Y. Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2241-2263, April 2019, doi: 10.1109/JIOT.2018.2887086.
7. V. Shah and L. Curtis, "Mode coupling effects of the cutoff wavelength characteristics of dispersion-shifted and dispersion-unshifted single-mode fibers," in *Journal of Lightwave Technology*, vol. 7, no. 8, pp. 1181-1186, Aug. 1989, doi: 10.1109/50.32380.
8. N. S. Yamanoor and S. Yamanoor, "High quality, low cost education with the Raspberry Pi," *2017 IEEE Global Humanitarian Technology Conference (GHTC)*, San Jose, CA, USA, 2017, pp. 1-5, doi: 10.1109/GHTC.2017.8239274.

9. A. Allouch, O. Cheikhrouhou, A. Koubâa, M. Khalgui and T. Abbes, "MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems," *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Tangier, Morocco, 2019, pp. 621-628, doi: 10.1109/IWCMC.2019.8766667.

10. W. Xi, "Analysis of Huawei's International Marketing Strategy Based on the SWOT Analysis," *2021 2nd International Conference on E-Commerce and Internet Technology (ECIT)*, Hangzhou, China, 2021, pp. 151-154, doi: 10.1109/ECIT52743.2021.00041.

11. Y. Xu, G. Ren, J. Chen, L. Jia and Y. Xu, "Anti-jamming transmission in UAV communication networks: A Stackelberg game approach," *2017 IEEE/CIC International Conference on Communications in China (ICCC)*, Qingdao, China, 2017, pp. 1-6, doi: 10.1109/ICCChina.2017.8330422.

12. L. Wang, H. Wang, Z. Qin, P. Zhu, D. Wu and Y. Chen, "Research on Key Technology of UAV Communication Optical Cable Line Inspection," *2024 6th International Conference on Communications, Information System and Computer Engineering (CISCE)*, Guangzhou, China, 2024, pp. 256-262, doi: 10.1109/CISCE62493.2024.10653308.

13. Q. Zhang *et al*., "An Improved Adaptive Coding and Modulation Scheme With Hybrid Switching Standard for UAV-to-Ground Free Space Optical Communication," in *IEEE Photonics Journal*, vol. 16, no. 1, pp. 1-8, Feb. 2024, Art no. 7300108, doi: 10.1109/JPHOT.2023.3329648.

14. J. Huang *et al*., "Optical Fiber Spool with Ultralow Acceleration Sensitivity," *2019 Joint Conference of the IEEE International Frequency Control Symposium and European Frequency and Time Forum (EFTF/IFC)*, Orlando, FL, USA, 2019, pp. 1-3, doi: 10.1109/FCS.2019.8856066.

15. N. H. Motlagh, M. Bagaa and T. Taleb, "UAV-Based IoT Platform: A Crowd Surveillance Use Case," in *IEEE Communications Magazine*, vol. 55, no. 2, pp. 128-134, February 2017, doi: 10.1109/MCOM.2017.1600587CM.

16. K. Kadripathi, L. Y. Ragav, K. Shubha and P. H. Chowdary, "De-

Authentication Attacks on Rogue UAVs," *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, Thoothukudi, India, 2020, pp. 1178-1182, doi: 10.1109/ICISS49785.2020.9316032.

17. H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767-809, Secondquarter 2022, doi: 10.1109/COMST.2022.3159185.

18. Аналіз можливого бортового оснащення радіотехнічними та телевізійними системами безпілотного літального апарата / Я. М. Кожушко, О. М. Гричанюк, М. Г. Саморок, О. С. Балабуха // Збірник наукових праць Харківського національного університету Повітряних Сил / Міноборони України. - Х., 2018.\

19. M. Lichtman, J. H. Reed, T. C. Clancy and M. Norton, "Vulnerability of LTE to hostile interference," *2013 IEEE Global Conference on Signal and Information Processing*, Austin, TX, USA, 2013, pp. 285-288, doi: 10.1109/GlobalSIP.2013.6736871.

20. ADAMY, David. *EW 101: A first course in electronic warfare*. Artech house, 2001.

21. PROAKIS, John G.; SALEHI, Masoud. *Digital communications*. New York: McGraw-hill, 2001.

22. POISEL, Richard. *Modern communications jamming principles and techniques*. Artech house, 2011.

23. ROBYNS, Pieter, et al. A multi-channel software decoder for the LoRa modulation scheme.

24. NETWORK, Evolved Universal Terrestrial Radio Access. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network. 2006.

25. HAYKIN, Simon. Cognitive radio: brain-empowered wireless communications. *IEEE journal on selected areas in communications*, 2005, 23.2: 201-220.

26. TZIVARAS, Vasilis. *Raspberry Pi Zero W Wireless Projects*. Packt Publishing Ltd, 2017.

27. REMY, Jean-Gabriel; LETAMENDIA, Charlotte. *LTE standards*. John Wiley & Sons, 2014.

28. REISS, Daniel. SDN-based LoRa Mesh.

29. AGRAWAL, Govind P. *Fiber-optic communication systems*. John Wiley & Sons, 2012.

30. DE MONTMORILLON, Louis-Anne; SILLARD, Pierre. *Bending-loss insensitive single mode fibre, with a shallow trench, and corresponding optical system*. U.S. Patent No 10,962,708, 2021.

31. МОВЧАН, К. О. СИСТЕМИ КЛАСИФІКАЦІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ТА ЇХ ЗАСТОСУВАННЯ В РІЗНИХ ГАЛУЗЯХ. *ВЧЕНІ ЗАПИСКИ*, 2024, 620241.

32. КОЧЕРГА, І. О. Підвищення ефективності застосування безпілотних літальних апаратів в умовах протидії засобів радіоелектронної боротьби.

33. ГАНАБА, Світлана; ОЛІФЕРОВИЧ, Дмитро. *Ефективність безпілотних літальних апаратів у військовий та мирний час*. 2025. PhD Thesis. Авіація, промисловість, суспільство: матеріали VI Міжнародної науково-практичної конференції (м. Кременчук, 15 травня 2025 року)/Міністерство внутрішніх справ України, Харківський національний університет внутрішніх справ, Кременчуцький льотний коледж. Харків: ХНУВС, 2025. 558 с.

34. ОПІРСЬКИЙ, Іван; БИБИК, Роман. Дослідження сучасних методів РЕБ та методів і засобів її протидії. *Безпека інформації*, 2023, 29.2: 88-97.

35. SHAMANOV, D.; SOROKIN, A. Аналіз сучасних методів радіоелектронної боротьби. *Системи управління, навігації та зв'язку. Збірник наукових праць*, 2024, 1.75: 211-214.

36. ХАРЧЕНКО, В.; ПРУСОВ, Д. Аналіз застосування безпілотних авіаційних систем у цивільній сфері. *Proceedings of National Aviation University*, 2012, 50.1: 118-130.

37. QUAN, Quan. *Introduction to multicopter design and control*. Singapore: Springer, 2017.

38. HATA, Masaharu. Empirical formula for propagation loss in land mobile

radio services. *IEEE transactions on Vehicular Technology*, 2013, 29.3: 317-325.

39. NAIK, Nishith R. USB based data communication system. 2010.

40. NUMBER PACKAGE, Part. Preliminary Data Sheet. 2002.

41. BAOPING, Chen; DI, Yao; FENG, Qian. Optical fiber cables. *The Global Cable Industry: Materials, Markets, Products*, 2021, 351-388.

42. MORRELL, Benjamin, et al. An addendum to NeBula: toward extending team CoSTAR's solution to larger scale environments. *IEEE Transactions on Field Robotics*, 2024, 1: 476-526.

43. LI, Xuelong, et al. Optics-driven drone. *Science China Information Sciences*, 2024, 67.2: 124201.

44. MIROSHNICHENKO, Kateryna. Wartime Ukraine Defence Innovation Ecosystem Formation through Drone Technologies. 2025.