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

Навчально-науковий Інститут телекомунікаційних систем

Кафедра Електронних комунікацій та Інтернету речей

«До захисту допущено»
ВО завідувача кафедри
_____ Вячеслав НОСКОВ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Оптимізація системи радіозв'язку для безпілотних літальних апаратів в умовах радіоелектронної боротьби»

Виконав:
Студент IV курсу, групи ТС-11
Труш Михайло Андрійович _____

Керівник:
Доцент кафедри ЕКІР ІТС, доцент
Носков В'ячеслав Іванович _____

Рецензент:
Незалежний експерт з телекомунікацій, кандидат
технічних наук, Вахрушев Володимир Платонович _____

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

Київ - 2025 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра Електронних комунікацій та Інтернету речей

Рівень вищої освіти - перший (бакалаврський)
Спеціальність - 172 Телекомунікації та радіотехніка
Освітня програма - «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ
ВО завідувача кафедри
_____ Вячеслав НОСКОВ
«___»_____20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Трушу Михайлу Андрійовичу

1. Тема роботи «Оптимізація системи радіозв’язку для безпілотних літальних апаратів в умовах радіоелектронної боротьби», керівник роботи Носков Вячеслав Іванович, доцент, затверджені наказом по університету від 26 травня 2025 р. № 1755 - с.

2. Термін подання студентом роботи 10 червня 2025 року

3. Вихідні дані до роботи: матеріали статей та наукових видань, інформаційні ресурси мережі Інтернет, навчально-методичні матеріали. Структурований план порядку розробки матеріалів дипломної роботи.

4. Зміст роботи: Обґрунтувати актуальність теми. Розглянути та проаналізувати сучасні технології організації радіозв’язку з БПЛА. Виконати аналіз методів захисту радіоканалів від впливу навмисних перешкод та

захисту даних. Детально проаналізувати метод FHSS з інтелектуальним вибором частот. Визначити роль супутникового зв'язку для керування БПЛА та проаналізувати методи покращення його стійкості в умовах навмисних завад. Запропонувати методи оптимізації системи радіозв'язку на основі моделювання поведінки БПЛА в умовах впливу засобів РЕБ.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): 1) Тема та мета дипломної роботи; 2) Основні компоненти БПЛА; 3) Технології організації зв’язку з БПЛА; 4) Методи захисту радіоканалів від навмисних перешкод; 5) Захисні алгоритми від засобів РЕБ; 6)Моделювання стійкості зв’язку БПЛА в умовах РЕБ; 7) Висновки по роботі.

6. Дата видачі завдання 31.10.2024 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
	Огляд сучасних систем радіозв’язку для БПЛА	14.04.2025	
	Методи захисту радіозв’язку від перешкод та глушіння	22.04.2025	
	Використання супутникового Інтернету для покращення зв’язку	15.05.2025	
	Оптимізація радіосистеми для БПЛА	30.05.2025	
	Вступ, Висновки	02.06.2025	
	Чистовий варіант дипломної роботи, плакати	10.06.2025	

Студент _____ Михайло ТРУШ

Керівник роботи _____ Вячеслав НОСКОВ

РЕФЕРАТ

Текстова частина дипломної роботи: 112 с., 9 рис., 2 табл., 64 джерел.

Актуальність роботи: В умовах сучасних військових конфліктів, зокрема під час широкомасштабних бойових дій на території України, безпілотні літальні апарати (БПЛА) набули масового характеру і стали ключовим інструментом для розвідки, спостереження та коригування вогню. Водночас, одним із найпотужніших засобів протидії цим платформам є радіоелектронна боротьба (РЕБ), яка спрямована на придушення каналів зв’язку та навігації. Уразливість систем керування та передачі даних БПЛА до впливу РЕБ створює критичну загрозу для виконання бойових завдань. Тому оптимізація та захист систем радіозв'язку для забезпечення їх стабільної та надійної роботи в умовах радіоелектронного протистояння є надзвичайно актуальною задачею.

Мета роботи: Оптимізувати систему радіозв’язку для безпілотних літальних апаратів (БПЛА) для забезпечення надійної передачі даних в умовах радіоелектронної боротьби (РЕБ).

Задачі дослідження:

Проаналізувати сучасні системи радіозв'язку, що використовуються в БПЛА, та основні принципи і загрози радіоелектронної боротьби (РЕБ).

Дослідити існуючі методи захисту каналів радіозв'язку від перешкод та глушіння, зокрема шифрування, технології розширення спектру (FHSS) та програмно-визначене радіо (SDR).

Оцінити переваги та обмеження використання супутникового зв'язку як альтернативного каналу для підвищення стійкості БПЛА в умовах РЕБ.

Розробити архітектуру оптимізованої системи зв'язку та провести її симуляційне моделювання для оцінки стійкості в різних сценаріях радіоелектронного впливу.

Сформулювати практичні рекомендації щодо підвищення надійності та захищеності систем радіозв'язку для БПЛА.

Об’єкт дослідження: Система радіозв’язку та навігації для безпілотних літальних апаратів.

Предмет дослідження: Радіотехнології для захисту каналів керування та навігації від впливу систем РЕБ

Ключові слова: БПЛА, РЕБ, РАДІОЗВ’ЯЗОК, ОПТИМІЗАЦІЯ, СУПУТНИКОВИЙ ЗВ'ЯЗОК, FHSS, SDR, ГЛУШІННЯ, СПУФІНГ, ЗАХИСТ КАНАЛІВ ЗВ'ЯЗКУ.

.

ABSTRACT

The work contains 112 pages, 9 figures, 2 tables, 64 sources.

Relevance of the work: In the context of modern military conflicts, particularly during large-scale combat operations on the territory of Ukraine, unmanned aerial vehicles (UAVs) have become widespread and are a key tool for reconnaissance, surveillance, and fire correction. At the same time, one of the most powerful means of countering these platforms is electronic warfare (EW), which is aimed at suppressing communication and navigation channels. The vulnerability of UAV control and data transmission systems to EW creates a critical threat to the execution of combat missions. Therefore, the optimization and protection of radio communication systems to ensure their stable and reliable operation under conditions of electronic countermeasures is an extremely urgent task.

The purpose of the work: To optimize the radio communication system for unmanned aerial vehicles (UAVs) to ensure reliable data transmission under electronic warfare (EW) conditions.

Research tasks:

To analyze modern radio communication systems used in UAVs, and the main principles and threats of electronic warfare (EW).

To investigate existing methods for protecting radio communication channels from interference and jamming, including encryption, spread spectrum technologies (FHSS), and software-defined radio (SDR).

To evaluate the advantages and limitations of using satellite communication as an alternative channel to increase the resilience of UAVs in EW conditions.

To develop an architecture for an optimized communication system and conduct its simulation modeling to assess its stability in various electronic warfare scenarios.

To formulate practical recommendations for improving the reliability and security of radio communication systems for UAVs.

Object of research: Radio communication and navigation system for unmanned aerial vehicles.

Subject of research: Radio technologies for protecting control and navigation channels from the influence of EW systems.

Keywords: UAV, EW, RADIO COMMUNICATION, OPTIMIZATION, SATELLITE COMMUNICATION, FHSS, SDR, JAMMING, SPOOFING, COMMUNICATION CHANNEL PROTECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

АЦП/ЦАП	Аналого-цифрові/Цифро-аналогові перетворювачі
БПЛА	Безпілотний літальний апарат
ГНСС (GNSS)	Глобальна навігаційна супутникова система (Global Navigation Satellite System)
ГСУ (GCS)	Наземна станція керування (Ground Control Station)
ДПС (DGPS)	Диференціальна глобальна система позиціонування (Differential Global Positioning System)
ІНС	Інерціальна навігаційна система
КТР	Командно-телеметричний радіоканал
ППРЧ	Псевдовипадкова перебудова робочої частоти
РЕБ	Радіоелектронна боротьба
AES	Advanced Encryption Standard (Розширений стандарт шифрування)
CBC	Cipher Block Chaining (Режим зчеплення блоків шифротексту)
CFB	Cipher Feedback (Режим зворотного зв'язку по шифротексту)
CRC	Cyclic Redundancy Check (Циклічний надлишковий код)
CSS	Chirp Spread Spectrum (Модуляція з розширенням спектру)
DSSS	Direct Sequence Spread Spectrum (Пряме розширення спектру)
ECC	Elliptic Curve Cryptography (Криптографія на еліптичних кривих)
ECB	Electronic Code Book (Режим простої заміни / електронна кодова книга)

FHSS	Frequency Hopping Spread Spectrum (Розширення спектру методом псевдовипадкового перестроювання частоти)
FPGA	Field-Programmable Gate Array (Програмована логічна інтегральна схема)
FPV	First-Person View (Вид від першої особи)
GEO	Geostationary Orbit (Геостаціонарна орбіта)
GPS	Global Positioning System (Глобальна система позиціонування)
GSM	Global System for Mobile Communications (Глобальний стандарт мобільного зв'язку)
HDOP	Horizontal Dilution of Precision (Горизонтальне погіршення точності)
HF	High Frequency (Високі частоти)
IDEA	International Data Encryption Algorithm (Міжнародний алгоритм шифрування даних)
ISM	Industrial, Scientific, and Medical (Промисловий, науковий та медичний діапазон)
LEO	Low Earth Orbit (Низька навколоземна орбіта)
LoRa	Long Range (Технологія бездротового зв'язку великої дальності)
LTE	Long-Term Evolution (Довгострокова еволюція, стандарт мобільного зв'язку)
MIMO	Multiple Input Multiple Output (Множинний вхід, множинний вихід)
MVDR	Minimum Variance Distortionless Response (Відповідь з мінімальною дисперсією без спотворень)
NMEA	National Marine Electronics Association (Національна асоціація морської електроніки, протокол)
OFB	Output Feedback (Режим зворотного зв'язку по виходу)

PDOP	Position Dilution of Precision (Погіршення точності визначення місцезнаходження)
PKI	Public Key Infrastructure (Інфраструктура відкритих ключів)
QAM	Quadrature Amplitude Modulation (Квадратурна амплітудна модуляція)
QPSK	Quadrature Phase-Shift Keying (Квадратурна фазова маніпуляція)
RSA	Rivest- Shamir- Adleman (Криптографічний алгоритм)
RTCM	Radio Technical Commission for Maritime Services (Радіотехнічна комісія з морських послуг, стандарт)
RTK	Real-Time Kinematic (Кінематика в реальному часі)
SDR	Software-Defined Radio (Програмно-визначене радіо)
SNR	Signal-to-Noise Ratio (Співвідношення сигнал/шум)
UBX	Бінарний протокол компанії U-Blox
UHF	Ultra High Frequency (Ультрависокі частоти)
VDOP	Vertical Dilution of Precision (Вертикальне погіршення точності)
VHF	Very High Frequency (Дуже високі частоти)
Wi-Fi	Wireless Fidelity (Стандарт бездротових мереж)

ВСТУП

В умовах сучасних військових конфліктів безпілотні літальні апарати (БПЛА) перетворилися на ключовий елемент ведення бойових дій, забезпечуючи розвідку, цілевказання та коригування вогню в режимі реального часу. Однак ефективність їх застосування напряму залежить від стабільності каналів керування та передачі даних, які є надзвичайно вразливими до дії засобів радіоелектронної боротьби (РЕБ) противника. Придушення або перехоплення сигналів може призвести не тільки до провалу місії, але й до втрати дороговартісного апарата.

У відповідь на ці загрози виникає гостра необхідність у розробці та впровадженні передових рішень, здатних захистити радіоканали БПЛА. Сучасні технології, такі як псевдовипадкова перебудова робочої частоти (ППРЧ), програмно-визначене радіо (SDR) та супутникові системи зв'язку, відкривають нові можливості для створення гнучких, адаптивних та стійких до глушіння комунікаційних систем.

Метою цієї роботи є оптимізація системи радіозв’язку для безпілотних літальних апаратів (БПЛА) для забезпечення надійної передачі даних в умовах радіоелектронної боротьби (РЕБ). Для досягнення цієї мети поставлено такі задачі: проаналізувати сучасні системи зв'язку БПЛА та загрози з боку РЕБ, дослідити методи захисту каналів, оцінити переваги супутникового зв'язку та, на основі отриманих даних, розробити й змоделювати архітектуру оптимізованої радіосистеми.

Об’єктом дослідження є система радіозв’язку та навігації для БПЛА. Предметом дослідження виступають радіотехнології та методи, що забезпечують захист каналів керування та навігації від впливу систем РЕБ.

1 ОГЛЯД СУЧАСНИХ СИСТЕМ РАДІОЗВ’ЯЗКУ ДЛЯ БПЛА

1.1 Структура та основні компоненти безпілотних літальних апаратів

З початком широкомасштабних бойових дій на території України застосування безпілотних літальних апаратів (БПЛА) набуло масового характеру, особливо в сегменті розвідувальних платформ. У контексті сучасної війни БПЛА стали ключовим інструментом спостереження, цілевказання та коригування артилерійського вогню. За визначенням, безпілотний літальний апарат -це літальний апарат, що не має пілота на борту, здатний до польоту завдяки аеродинамічним силам та тязі двигунів, і який здійснює політ за заздалегідь запрограмованим маршрутом або в режимі дистанційного керування.

Основні цілі багатьох БПЛА:

- Розвідки та спостереження.
- Проведення фото/відео зйомки в реальному часі для виявлення цілей та коригування вогню.
- Ударні місії для знищення техніки та особового складу.

Узагальнення технічної структури безпілотних літальних апаратів (БПЛА) базується на аналізі представників даного класу систем - це Zala 421-16E, Supercam S350 та Орлан-10. Незважаючи на конструктивні та функціональні відмінності, кожен з них має набір основних функціональних підсистем, необхідних для автономного виконання польотного завдання.

1. Модуль керування

Основний обчислювальний модуль забезпечує загальну координацію роботи всіх підсистем БПЛА. У випадку з Zala 421-16E додатково використовується модуль керування виконавчими пристроями, який:

- приймає сигнали від головного модуля керування;
- формує напруги живлення для виконавчих механізмів;
- здійснює контроль струму в ланцюгах периферійного обладнання.

2. Командно-телеметричний радіоканал

Ця підсистема забезпечує двосторонній зв’язок між БПЛА та наземною станцією управління. До її складу входить радіомодем, який функціонує в певних частотних діапазонах:

- Zala 421-16E: 868-870 МГц, 902-928 МГц (антена інтегрована у кінцівки крила);
- Supercam S350: 865-1020 МГц, 840-928 МГц, 960-1020 МГц (радіомодем ISM RadioMost 19017, розташований у фюзеляжі);
- Орлан-10: 894-926 МГц, 972-1020 МГц, застосовується метод псевдовипадкової перебудови робочої частоти (ППРЧ), модем ТА1163А.

3. Система супутникової навігації

Навігаційна підсистема забезпечує визначення координат у реальному часі та підтримку курсу польоту. Всі розглянуті моделі підтримують багатостандартний супутниковий прийом:

- Zala 421-16E: модуль Ublox LEA-M8S-0-10 (GPS, Galileo, GLONASS, BeiDou);
- Supercam S350: модуль Ublox NEO-M9N-00B;
- Орлан-10: адаптивна антена “Комета-М-ВТ” з приймачем NV08CM-CSM та окремий модуль UBLOX ZED-F9P-01B-01 з керамічною патч-антеною.

4. Система передавання відео

Передавання зображення відбувається за допомогою виділеної відеопідсистеми, до складу якої входять передавач, антена, підсилювач потужності, фільтри та елементи живлення:

- Zala 421-16E: частотні діапазони - 1200-2150 МГц, 3.93-5.4 ГГц;
- Supercam S350: 1100-1480 МГц, трансивер CDR-2401BT/10 виробництва Vitec;

• Орлан-10: використовується модуль обробки відео AXIS M7011 та модуль передачі VSKS Rev4 на базі трансивера AD9361. Центральні частоти: 1105-1115 МГц, 2200-2400 МГц, 2300-2700 МГц.

5. Антенні системи

Для забезпечення надійного прийому та передавання сигналів усіх типів БПЛА оснащуються широкосмуговими або адаптивними антенами:

• В Zala 421-16E антени вмонтовані у кінцівки крила;

• В Орлан-10 використовується фазована антенна решітка адаптивного типу (“Комета-М-ВТ”).

Ілюстрація типової компонувальної схеми сучасного БПЛА на прикладі Supercam S350 подана на рис. 1.1. На ньому візуалізовано розташування ключових вузлів - антенної системи, джерел живлення, GNSS-приймача, елементів управління польотом та корисного навантаження. Це дозволяє краще зрозуміти просторову логіку розміщення радіочастотних, обчислювальних і механічних елементів на апараті.

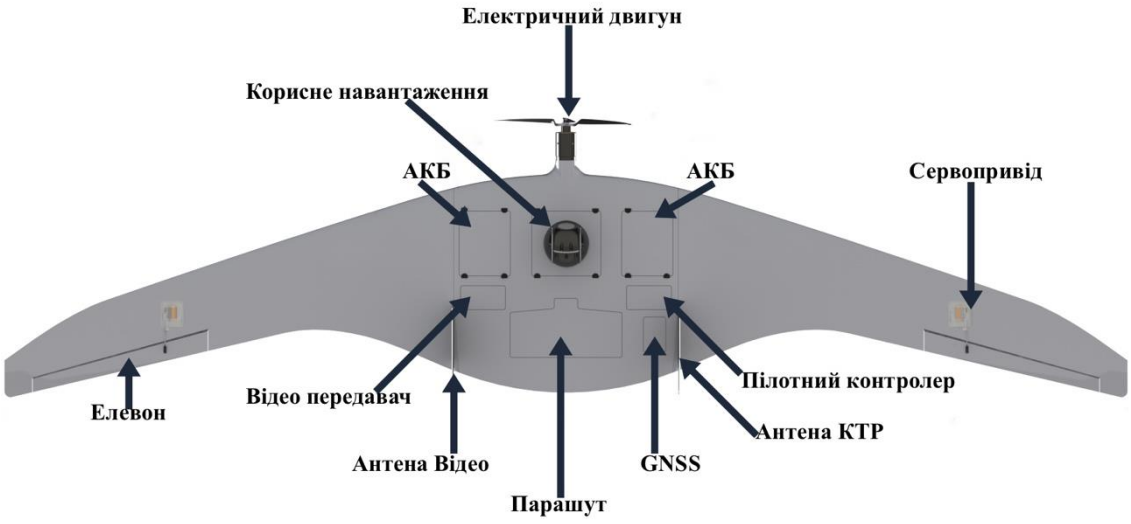

Рисунок 1.1 - Основні компоненти безпілотного літального апарата

Supercam S350 - це крилатий безпілотний літальний апарат з електричним двигуном, розроблений для виконання розвідувальних і спостережних завдань. На фото показано базові компоненти апарата:

- Електричний двигун, розташований у хвостовій частині, забезпечує тиху тягу;
- Акумуляторні батареї (АКБ), встановлені по обидва боки фюзеляжу, живлять усі електронні модулі;
- Відеопередавач та антена для трансляції зображення у реальному часі;
- GNSS-приймач і антена КТР (командно - телеметричного радіоканалу), що забезпечують навігацію та зв’язок із наземною станцією;
- Парашутна система, яка виконує функцію аварійної посадки;
- Пілотний контролер, що виконує обчислювальні функції керування;
- Сервоприводи та елевони, що відповідають за аеродинамічне керування.

Така компоновка забезпечує ефективне поєднання мінімальної ваги, функціональної гнучкості та просторової ефективності. Supercam S350 наочно демонструє типову архітектуру апаратів цього класу, де пріоритет надається модульності та легкій адаптації до різних бойових завдань.

1.2 Радіохвилі

Для розуміння ключових принципів побудови та функціонування систем зв’язку БПЛА необхідно розглянути фізичну природу радіохвиль, які є основним носієм інформації в цих системах. Їх властивості, поширення в різних середовищах, здатність до дифракції, поглинання чи відбиття мають безпосередній вплив на якість і стійкість зв’язку в умовах реального середовища, особливо в бойовій обстановці. Тому доцільно перейти до розгляду фундаментальних характеристик радіохвиль, що використовуються в системах зв’язку безпілотних літальних апаратів.

Радіохвилі як форма електромагнітного випромінювання займає центральне місце у забезпеченні бездротового зв’язку, зокрема між наземними станціями керування та безпілотними літальними апаратами. Це змінне електромагнітне поле, яке поширюється в просторі зі сталою швидкістю - приблизно 300 000 км/с у вакуумі. У класичній теорії поля електромагнітна хвиля розглядається як система взаємозв’язаних векторних полів - електричного та магнітного - які коливаються у взаємно перпендикулярних площинах і формують фронт хвилі, що рухається перпендикулярно до обох складових.

Електромагнітне поле не потребує матеріального середовища для свого поширення: його формування зумовлене змінами електричного та магнітного полів у часі. Ця здатність забезпечує можливість передачі сигналів крізь атмосферу, вакуум, а також через діелектричні або провідникові середовища. Електромагнітні хвилі у вигляді радіохвиль можуть мати різну довжину та частоту, що визначає їх проникну здатність, дальність поширення, ступінь поглинання, а також можливість використання у тих чи інших умовах.

Визначається як:

$$\lambda = \frac{c}{f}$$

с - швидкість поширення хвилі.

Частота (f) - кількість повних коливань електромагнітного поля за одиницю часу. Вимірюється в герцах (Гц). Зростання частоти веде до зменшення довжини хвилі.

Довжина хвилі (λ) - просторовий інтервал між двома точками хвилі, які перебувають в однаковій фазі. [1]

Потужність - кількість енергії, що переноситься хвилею за одиницю часу. Визначає інтенсивність сигналу та впливає на дальність дії системи зв’язку.

Фаза та поляризація - визначають конфігурацію хвилі в просторі та впливають на приймання сигналу в антенних системах.

Особливістю радіохвиль є їх здатність до відбиття, заломлення, дифракції та інтерференції, що значною мірою ускладнює їх передбачуване поширення в реальному середовищі. Так, наприклад, у міських умовах сигнали часто зазнають багатопроменевого поширення, коли хвиля досягає приймача декількома маршрутами, спричиняючи фазові зсуви та ефект затухання. У свою чергу, в умовах відкритої місцевості або на висоті, сигнал здатен поширюватися на великі відстані без значних втрат.

Для ефективної передачі даних у радіоканалах зв’язку використовуються радіохвилі з різним частотним діапазоном - від десятків кілогерців до десятків гігагерців. Зокрема, у системах зв’язку з БПЛА переважно застосовуються частоти в діапазонах 900 МГц, 2,4 ГГц, 5,8 ГГц, залежно від потрібної дальності, пропускної здатності та стійкості до завад. Чим вища частота, тим більша пропускна здатність, але й тим більша чутливість до фізичних перешкод і атмосферних явищ.

Розуміння фізичних властивостей радіохвиль є ключовим при проектуванні бездротових систем зв’язку, антенних конфігурацій та систем протидії завадам. В умовах активного застосування радіоелектронної боротьби знання про характеристики поширення та спотворення хвиль набуває особливої актуальності для забезпечення надійності та стійкості зв’язку з безпілотними платформами.

1.3 Вплив середовища та місцевості на ефективність радіозв’язку

Отже, радіохвилі як носії інформації мають низку фундаментальних фізичних властивостей, зокрема довжину, частоту, поляризацію, напрямок поширення, здатність до відбиття, заломлення й затухання. Усі ці характеристики впливають на параметри та надійність передавання сигналу в радіоканалі.

Однак на практиці ефективність радіозв’язку визначається не лише внутрішніми параметрами хвильового сигналу, а й зовнішніми умовами його поширення. На шляху від передавача до приймача сигнал неминуче взаємодіє з фізичним середовищем, у якому поширюється: повітрям, рельєфом місцевості, будівлями, рослинністю, атмосферними явищами тощо.

Саме тому важливим етапом аналізу є вивчення впливу середовища та географічних особливостей місцевості на характеристики радіохвильового розповсюдження, зокрема в контексті побудови стійких каналів зв’язку для безпілотних літальних апаратів у складних або бойових умовах. Під час застосуваннь БПЛА, коли стабільний зв’язок є критично важливим, ці фактори відіграють ключову роль у проектуванні та реалізації радіомереж.

На характер поширення радіосигналу впливає безліч чинників:

• Дифракція - здатність радіохвиль огинати перешкоди. Хвилі з більшою довжиною огинають перешкоди краще, але мають більш громіздкі антени.

• Одним із критично важливих чинників, що впливають на надійність функціонування систем зв’язку безпілотних літальних апаратів (БпЛА), є інтерференція - взаємне накладення двох або більше радіосигналів у межах одного або суміжних частотних діапазонів. Наслідком цього процесу може бути суттєве зниження якості прийому сигналу, його повна втрата або спотворення, що унеможливлює стабільне керування апаратом у реальному часі. «Інтерференція виникає, коли кілька БпЛА використовують один і той самий частотний канал для передачі даних, від інших бездротових мереж та пристроїв, що працюють на сусідніх каналах зв’язку, від фазового зсуву і зміни амплітуди при відбиванні одного і того ж сигналу від різних поверхонь, від впливу засобів радіоелектронної боротьби (РЕБ) противника, внаслідок атмосферних явищ» [2, с. 348]. Іншими словами, джерелами інтерференції можуть бути як зовнішні - інші дрони, ворожі засоби РЕБ, цивільні пристрої (Wi-Fi, відеопередавачі), так і внутрішні чинники - зокрема багатопроменеве поширення сигналу від об’єктів рельєфу або інфраструктури. У разі

виникнення фазових зсувів між основним і відбитим сигналом можлива поява деструктивної інтерференції, що призводить до завмирання сигналу. Це, в свою чергу, може спричинити втрату каналу керування, зупинку передачі відеопотоку або навіть падіння апарата.

• Радіохвилі не проходять, тобто поглинаються через землю, залізобетонні та цегляні будівлі, а також конструкції з металу або з металевим покриттям. Дерев'яні споруди та лісові масиви пропускають радіохвилі краще, але викликають їхнє загасання.

• Погодні умови - дощ і сильний туман можуть погіршити якість зв'язку, особливо на великих відстанях.

• Дощ: Краплі води поглинають та розсіюють радіохвилі, що призводить до затухання сигналу. Це особливо помітно на частотах вище 10 ГГц (наприклад, у діапазоні міліметрових хвиль, які використовуються в технологіях 5G).

• Сніг та град: Сніжинки та градини також можуть викликати затухання сигналу, хоча їх вплив зазвичай менший, ніж у дощу. Однак при сильних снігопадах або граді вплив може бути значним.

• Туман складається з дрібних крапель води, які можуть поглинати радіохвилі, особливо на високих частотах. Це призводить до зниження інтенсивності сигналу.

• Хмари також можуть впливати на сигнал, хоча їх вплив зазвичай менший, ніж у туману або дощу.

• Висока вологість може призводити до поглинання радіохвиль молекулами води, що особливо помітно на частотах вище 20 ГГц.

• Температурні інверсії, які виникають у разі, коли теплі шари повітря розташовуються над холоднішими, здатні значно змінювати умови поширення радіохвиль. У таких умовах спостерігається явище заломлення радіохвиль, при якому їхній напрямок викривлюється вниз, ближче до земної поверхні. Це

може призводити до непередбачуваних втрат або спотворень на звичних ділянках зв’язку. [3]

- На відкритій місцевості зв’язок стабільніший і має більшу дальність, ніж у лісі чи місті. Цей фактор слід враховувати при налаштуванні зв’язку.
- Гори та пагорби: Вони можуть блокувати або відбивати сигнал, що призводить до мертвих зон, де зв’язок відсутній.
- Рівнини та відкриті простори: На таких ділянках сигнал поширюється краще, оскільки менше перешкод.
- Ліси та рослинність: дерева та інша рослинність можуть поглинати та розсіювати радіохвилі, особливо на високих частотах. Це призводить до затухання сигналу. Вологий ліс (наприклад, під час дощу) має більший вплив на сигнал, ніж сухий.
- Антени слід захищати від опадів та не розміщувати під схилами дахів або на відкритому повітрі без захисту від вологи.
- Одним із важливих чинників, що визначають ефективність радіозв’язку, є висота встановлення антени над рівнем землі. Чим вище розміщена антена, тим більшу зону прямої видимості вона охоплює, що, у свою чергу, забезпечує стабільніший канал зв’язку та збільшує максимальну дальність передачі даних. Це особливо важливо для безпілотних платформ, які працюють на значній відстані від наземної станції керування.
- При розміщенні антен особливу увагу слід приділяти навколишнім об’єктам: уникати встановлення поблизу матеріалів або конструкцій, які можуть поглинати або екранувати радіохвилі, наприклад, залізобетон, металеві покритт, а також не розташовувати антени поруч з іншими джерелами електромагнітного випромінювання чи поблизу ліній електропередач. У тактичних умовах важливо забезпечити мінімізацію вірогідності виявлення джерела випромінювання противником. З цією метою доцільно встановлювати антену за фізичною перешкодою в напрямку від противника, щоб ускладнити технічну пеленгацію. Для стаціонарних або

тилових передавачів доцільно використовувати спрямовані антени, які концентрують потужність сигналу в бік приймача і, водночас, знижують рівень випромінювання у протилежному напрямку. У прифронтовій зоні рекомендовано застосовувати слабші передавачі з вузьким спрямуванням для мінімізації радіовипромінювання та зниження ймовірності виявлення. У разі нанесення камуфляжного покриття слід враховувати, що деякі види фарб можуть містити металеві частинки, які частково або повністю екранують електромагнітне випромінювання. Найпростіший спосіб перевірити сумісність фарби з радіочастотними застосуваннями - помістити невелику кількість фарби в скляну або картонну ємність та розмістити її на кілька хвилин у мікрохвильову піч. Якщо фарба залишається холодною - вона не взаємодіє з мікрохвильовим випромінюванням і може бути використана. Якщо ж нагрівається - така фарба містить домішки, які можуть негативно вплинути на параметри випромінювання антени, і тому є непридатною для застосування в системах зв’язку.

Таким чином, ефективність радіозв’язку визначається не лише характеристиками самого сигналу, а й численними зовнішніми чинниками, серед яких провідну роль відіграють рельєф місцевості, погодні умови, вологість, перешкоди в середовищі та фізичний стан радіоапаратури.

Одним із ключових компонентів, який безпосередньо взаємодіє з усіма цими чинниками, є антена. Саме антенні системи визначають, наскільки ефективно сигнал випромінюється, поширюється та приймається в конкретних умовах. У зв’язку з цим далі детальніше буде детальніше розгялнуто конструктивні та функціональні особливості антен, які застосовуються в сучасних системах зв’язку БпЛА.

1.4 Антени

Антена є невід’ємним елементом будь-якої радіосистеми, оскільки вона виконує функцію перетворення електричних коливань у електромагнітні хвилі під час передавання та зворотне перетворення при прийомі сигналу. У системах зв’язку з безпілотними літальними апаратами (БпЛА) антена визначає дальність зв’язку, стабільність каналу, стійкість до перешкод і навіть рівень виявлення станції противником.

Типи антен

Антени класифікують за функціональним призначенням на три основні типи:

- Передавальні антени - перетворюють електричні сигнали з передавача в електромагнітні хвилі, які поширюються в просторі.
- Приймальні антени - виконують зворотний процес: вловлюють радіохвилі з навколишнього середовища та перетворюють їх у електричні сигнали для приймача.
- Приймально-передавальні - універсальні, вони можуть працювати одночасно або почергово у режимах прийому та передавання.

Конструктивні особливості антен

Фізичні параметри антени мають вирішальний вплив на її резонансні властивості, ефективність та стабільність роботи. Антени зазвичай виготовляють із високопровідних матеріалів, таких як мідь, алюміній або бронза. Ці метали забезпечують низький опір і добрі характеристики електромагнітного випромінювання.

Розміри антени, зокрема її довжина, безпосередньо залежать від робочої частоти сигналу. Наприклад, для хвилі довжиною 1 м оптимальна антена повинна мати розмір, близький до половини або чверті цієї довжини. Це обумовлено резонансними умовами, за яких відбувається найбільш ефективне

перетворення енергії. Резонансна довжина антени дозволяє знизити коефіцієнт відбиття та втрати у каналі. [4,5]

Також одним із параметрів антени є діаграма спрямованості - графік, що ілюструє розподіл енергії випромінювання або прийому в просторі. Вона показує, у яких напрямках антена працює найбільш ефективно.

Антени можуть мати всеспрямовану діаграму, наприклад, класичні штирьові антени, яка дозволяє покривати простір рівномірно у горизонтальній площині. Такий тип зручний для мобільних об’єктів, що рухаються у випадкових напрямках. Водночас спрямовані антени концентрують енергію в певному напрямку, забезпечуючи підвищену дальність та стійкість зв’язку. У тактичних умовах спрямованість дозволяє не лише покращити якість зв’язку, а й знизити рівень побічного випромінювання, що ускладнює пеленгацію з боку противника.

Частота сигналу безпосередньо впливає на фізичні розміри антени. На високих частотах, де довжина хвилі менша можливо використовувати компактні антени, що зручно для авіаційних або переносних засобів зв’язку. Проте високочастотні антени більш чутливі до поглинання вологи, дощу, туману та лісової рослинності. Тому під час вибору частотного діапазону завжди слід враховувати особливості середовища, в якому працюватиме система зв’язку.

Отже, антенна система є не просто технічним елементом БПЛА, а складною підсистемою, що формує якість, надійність і стійкість радіоканалу. Тип, діаграма спрямованості, робоча частота та умови експлуатації - усі ці параметри визначають здатність дрона ефективно приймати команди та передавати дані. У воєнних умовах, де сигнал може зазнавати значного спотворення або приглушення, роль антени стає ще важливішою, зокрема у контексті захисту від зовнішніх електромагнітних впливів.

1.5 Радіоелектронна боротьба

Зі зростанням інтенсивності застосування безпілотних літальних апаратів у зоні бойових дій, радіоелектронна боротьба стала одним із найпотужніших засобів протидії цим платформам. РЕБ охоплює комплекс технічних та тактичних заходів, спрямованих на виявлення, придушення або обман радіоелектронних систем противника. Особливо уразливими до впливу РЕБ є саме канали зв’язку, навігації та телеметрії БПЛА, які працюють у відкритому середовищі.

В умовах сучасних військових конфліктів бойові дії дедалі активніше ведуться не лише на фізичному полі бою, а й в інформаційному середовищі, яке значною мірою формується за рахунок електромагнітного спектра. Частина цього спектра, яка використовується для передавання, прийому та обробки інформації, визначається як електромагнітне середовище. Доступ до цього середовища та можливість його безперешкодного використання стають критичними для збройних сил, адже з одного боку відкривають нові оперативні можливості, а з іншого створюють вразливості. У такому контексті електромагнітна або електронна війна виступає інструментом впливу, що здійснювює контроль над спектром, атакувати противника через електромагнітні засоби або перешкоджати його діям.

Метою електромагнітної війни є позбавлення ворога переваг у спектрі та забезпечення власним силам надійного й захищеного доступу до нього. Електронна боротьба може здійснюватися з повітря, суші, моря або космосу, з використанням як пілотованих, так і безпілотних систем. Основними об’єктами впливу стають засоби зв’язку, радіолокаційні системи, навігаційне та управлінське обладнання як військового, так і цивільного призначення.

Радіоелектронна боротьба (РЕБ) - це різновид збройної боротьби, котрий здійснює радіоперешкоди для радіоелектронних засобів розвідки, систем зв’язку та керування ворога для ускладнення його роботи і передачі даних.

Основними завданнями РЕБ є зрив роботи засобів спостереження противника, а також радіоелектронне подавлення ліній радіозв’язку, що забезпечує перевагу на полі бою шляхом порушення інформаційного обміну ворога.

1.5.1 Класифікація РЕБ

Системи радіоелектронної боротьби класифікуються за базуванням:

- Наземні системи РЕБ: Встановлюються на стаціонарних або мобільних платформах, таких як автомобілі чи бронетехніка. Вони забезпечують захист стратегічно важливих об’єктів та інфраструктури від радіоелектронних загроз.
- Повітряні системи РЕБ: Розміщуються на літаках, вертольотах або безпілотниках. Їх основна функція -забезпечення електромагнітного захисту повітряного простору та підтримка операцій авіації.
- Морські системи РЕБ: Інтегруються на кораблях та підводних човнах для захисту морських сил від радіоелектронних загроз, таких як протикорабельні ракети чи ворожі радари.
- Портативні системи РЕБ: Компактні пристрої, які можуть переноситися піхотою або встановлюватися на малих платформах. Вони забезпечують захист на тактичному рівні, зокрема від безпілотних літальних апаратів та інших локальних загроз.

Кожен тип системи РЕБ має свої особливості та призначення, що дозволяє ефективно використовувати їх у різних умовах бойових дій та забезпечувати комплексний захист від радіоелектронних загроз.

Окрім класифікації за типом базування, системи радіоелектронної боротьби також поділяють за функціональним призначенням. Такий підхід дозволяє краще зрозуміти спеціалізацію кожного комплексу РЕБ у межах конкретної операції та його вплив на електромагнітне середовище.

Рисунок 1.2 - Поділ засобів РЕБ за функціональним рівнем: стратегічно-оперативний, тактичний, окопний [63]

Опис типів засобів РЕБ:

• Стратегічно-оперативні системи (зображені ліворуч і праворуч на рисунку) - це потужні комплекси, здатні впливати на широкі ділянки спектру в межах десятків кілометрів. Вони зазвичай розміщуються на стаціонарних вежах або мобільних платформах, таких як багатовісні вантажівки. Основне призначення - придушення систем зв’язку, навігації (GNSS), супутникового передавання даних, радіолокаційних систем противника.

• Тактичні системи - середнього радіусу дії, призначені для підтримки конкретних бойових підрозділів у зоні активних бойових дій. Вони можуть використовуватися для глушіння командних радіоканалів БПЛА, придушення Wi-Fi або мобільного зв’язку. Тактичні РЕБ часто розміщуються на щоглах, переносних мачтах або легких автомобілях.

• Окопні (або піхотні) засоби РЕБ - це портативні або напівпортативні пристрої, призначені для локального придушення дронів, GPS або радіоканалів у межах 0.5-2 км. Вони працюють від акумуляторів або портативних джерел живлення. До цього класу належать системи типу «Антидрон», EDM4S, KVS ANTIDRONE, які активно використовуються в Україні.

1.5.2 Основні напрями функціонального застосування систем РЕБ

1. Для придушення засобів радіозв’язку

Основна мета таких систем -створення завад у діапазонах, що використовуються для голосового та цифрового обміну інформацією. Це дозволяє порушити зв’язок між підрозділами противника, ускладнити командування та управління, знизити бойову ефективність. Такі системи часто використовують широкосмугові генератори шуму або спрямовані імпульсні перешкоди.

2. Для придушення сигналів управління БПЛА

Спеціалізовані комплекси призначені для виявлення та блокування каналів керування дронами (часто це частоти 2.4 ГГц, 5.8 ГГц або L-діапазон). Їх застосування дозволяє припинити польотну місію БПЛА або перехопити контроль над апаратом. Деякі системи забезпечують не лише глушіння, а й впровадження хибних команд у лінію керування.

3. Для виявлення та нейтралізації радарів

Цей клас РЕБ-комплексів призначений для пасивного виявлення радіолокаційного випромінювання противника з подальшим активним придушенням чи обманом. Найбільш ефективними є комплекси з адаптивними алгоритмами, що змінюють частоту, фазу або модуляцію завад у режимі реального часу. У сучасних умовах системи позиціонування і супутникового зв’язку відіграють важливу роль у навігації та бойовому управлінні.

4. Для виявлення та нейтралізації сигналів віддаленого управління

Дані засоби РЕБ застосовуються для захисту особового складу від саморобних вибухових пристроїв, які активуються через бездротові канали (мобільний зв’язок, радіостанції, Wi-Fi). Принцип дії полягає у створенні постійного захисного електромагнітного купола, що перекриває сигнали активації в критичних частотних діапазонах.

5. Для захисту техніки та особового складу від керованих боєприпасів

Зокрема, йдеться про системи активного РЕБ, які можуть виявляти наведення високоточного озброєння (лазерне, ІЧ, радіочастотне) та створювати перешкоди у відповідному спектрі. Прикладом є комплекси, що глушать канали наведення протитанкових ракет або блокують приймання координат із зовнішніх джерел.

6. Змішаного використання (мультифункціональні комплекси)

Сучасні РЕБ-системи дедалі частіше створюються як багатофункціональні, здатні одночасно працювати в кількох режимах. Вони поєднують придушення зв’язку, нейтралізацію дронів, GPS, радарів і засобів управління озброєнням. Прикладом таких систем є вітчизняні комплекси «Нота» та «Полонез», які демонструють високу ефективність проти широкого спектра загроз.

Важливою складовою РЕБ є створення радіоперешкод. Існують різні типи таких перешкод:

- Точкова перешкода фокусується на конкретному каналі або частоті, подаючи концентровану потужність з метою блокування зв’язку. Вона складна для виявлення, але малоефективна проти сигналів із псевдовипадковою перестройкою частоти. Прикладом може бути аналогова або цифрова радіостанція, підключена до підсилювача і спрямована на ворожу антену.
- Плаваюча перешкода змінює частоту з часом, пробігаючи короткими імпульсами по певній частині спектра. До цієї категорії належать усі сигнали на базі генератора, керованого напругою, що може мати модуляцію у вигляді пили або синусоїди і керується напругою, яка подається на нього. Це простий і дешевий спосіб створення перешкоди, але має недоліки. Завада йде швидкими імпульсами через проміжок часу, тому сигнал псевдовипадкової частоти може пролізти через сітку імпульсів.
- Суцільна перешкода передбачає блокування багатьох частот одночасно. Така завада ефективніша за плаваючу або точкову, проте використовує багато ресурсів і потужності, тому ефект може бути обмеженим. Один із методів

створення такої перешкоди є DDS - Direct Digital Sinthesis (прямий цифровий синтез). Він є ефективним методом, адже дає більш щільну перешкоду через яку майже неможливо прорватися псевдовипадковому сигналу.

- Найскладнішим і найнебезпечнішим видом є розумна перешкода. Вона базується на аналізі сигналу противника та генерації потужного фальшивого сигналу, що його підміняє. Так працюють, зокрема, спуфери - системи підміни GPS, які змінюють координати навігаційних систем, вводячи техніку або боєприпаси в оману. Така перешкода також здатна маскувати об’єкти на радарах, збивати системи наведення та виводити з ладу комунікації. Виявити її важко, а наслідки можуть залишатися непоміченими на початковому етапі, що робить її особливо загрозливою в умовах сучасної війни. [6]

1.6 Огляд сучасних систем радіозв’язку для БПЛА

Ефективність БПЛА залежить від стабільного, надійного та захищеного радіозв’язку, який забезпечує передачу телеметричних даних, команд керування та навігаційної інформації.

Існує багато протоколів, які забезпечують різні аспекти зв’язку між БПЛА та наземною станцією. У цьому огляді розглянуто чотири ключові системи передачі даних, що активно використовуються в безпілотних платформах:

- NMEA - текстовий протокол для передачі навігаційних даних;
- UBX Binary - бінарний протокол компанії U-Blox із розширеними можливостями;
- RTCM - стандарт для високоточних поправок у системах позиціонування;
- LoRa - технологія далекого зв’язку з низьким енергоспоживанням.

Метою цього огляду є порівняльний аналіз зазначених систем за критеріями точності, завадостійкості, швидкості обміну даними та

енергоспоживання, з урахуванням особливостей використання в умовах бойових дій та РЕБ.

1.6.1 NMEA (National Marine Electronics Association)

NMEA - текстовий протокол для передачі навігаційних даних, який є стандартом для систем GNSS. Модуль GPS надсилає інформацію у форматі NMEA. Інформація у форматі NMEA - це набір речень. Речення - це набір слів, розділених символом «,». Значення кожного слова залежить від типу даних.

Структура повідомлення

- Починається зі спеціального символу $ або !, який позначає початок повідомлення і закінчується символом '(переведення рядка (\r\n))'.
- Містить ідентифікатор типу повідомлення, наприклад, $(GPGGA, GPRMC, GPVTG) (дані про місцезнаходження).
- Поля даних розділені комами, а наприкінці додається контрольна сума

Приклад - $GPGGA,123456.78,4916.45,N,12311.12,W,1,08,1.0,0.0,M,0.0,M,,47

Типи повідомлень:

- GGA (Global Positioning System Fix Data) - Містить ключові координати місцезнаходження, висоту над рівнем моря, кількість супутників, які використовуються для фіксації, HDOP (горизонтальна точність), тощо.
- RMC (Recommended Minimum Specific GNSS Data) - Надає мінімально необхідні навігаційні дані: координати, дата, час, швидкість, напрямок руху.
- GSA (GNSS DOP and Active Satellites) - Вказує, які супутники використовуються в обчисленнях, а також значення PDOP, HDOP та VDOP (точності положення).
- GSV (GNSS Satellites in View) - Дає інформацію про всі супутники в полі зору: номер супутника, азимут, кут підйому, рівень сигналу.

• VTG (Track Made Good and Ground Speed) - Повідомляє курс (у градусах) та швидкість відносно поверхні землі у вузлах (knots) та км/год.

Приклад повідомлення
$GPRMC,085120.307,A,3541.1493,N,13945.3994,E,000.0,240.3,181211,,,A6A

Розбір повідомлення:

GPRMC - тип повідомлення (навігаційні дані).

085120.307 - UTC-час: 08:51:20.307.

A - статус: A = активний (valid), V = невалідний (warning).

3541.1493,N - широта: 35°41.1493' пн.ш.

13945.3994,E - довгота: 139°45.3994' сх.д.

000.0 - Швидкість руху на поверхні землі. Від 000,0 до 999,9 у вузлах.

240.3 -Напрямок руху на поверхні Землі. Від 000,0 до 359,9 градусів.

181211 - Дата в всесвітньому координованому часі - 18 грудня 2011 року.

,,,A - Режим: Автономний метод. Режим, N = Немає даних, A = Автономний (Автономний Метод), D = Диференціальний (Метод Позиціонування Перешкод), E = Розрахунковий (Орієнтовний).

6A - Значення контрольної суми.

Переваги:

• Підтримується більшістю GNSS-приймачів.

• Простота інтеграції завдяки текстовому формату.

Недоліки:

• Високе навантаження на канал через великий об’єм текстових даних.

Обмежена функціональність порівняно з бінарними протоколами. [7]

1.6.2 UBX Binary

Протокол UBX - це протокол, створений U-Blox, який передає дані, отримані GPS, у двійковий тип даних, на відміну від стандарту NMEA-0183. Модуль GPS U-Bolx може одночасно виводити протоколи NMEA та UBX. Ви

можете вибрати вихід протоколу NMEA та протоколу UBX за допомогою програми U-Center, наданої U-Blox. У випадку протоколу NMEA потрібен окремий буфер, оскільки він поставляється у форматі ASCII, а після зберігання ASC у буфері дані символьного типу повинні бути перетворені в дані цілого або плаваючого типу. У випадку протоколу UBX з половиною імені дані надходять зі значенням Binary(HEX), тобто попередній байт синхронізації.

Повідомлення UBX має фіксовану структуру:

- Sync Char - Синхронізуючі байти завжди: 0xB5, 0x62.
- Class - Категорія повідомлення (напр. навігація, конфігурація, моніторинг)
- ID - Тип повідомлення у класі
- Length - Довжина даних (Payload) у байтах
- Payload - Основне повідомлення з корисною інформацією
- Checksum - Контрольна сума (2 байти, обчислюється за алгоритмом RFC)

Типи повідомлень:

- NAV-POSLLH - передача широти, довготи та висоти.
- NAV-VELNED - швидкість, напрямок руху.
- CFG-MSG - налаштування параметрів передачі повідомлень.

Переваги:

- Висока ефективність передачі даних завдяки компактності.
- Можливість гнучкого налаштування параметрів GNSS-приймача.

Недоліки:

- Вимагає спеціального програмного забезпечення для обробки та аналізу даних.
- UBX складніший для читання людиною, оскільки є бінарним. [8]

1.6.3 RTCM (Radio Technical Commission for Maritime Services)

RTCM - це загальноприйнятий формат передачі даних, який надається Міжнародною комісією з морських радіотехнологій. Члени запропонували йому сформулювати стандарти для диференційованих глобальних систем навігації та позиціонування та динамічних операцій у режимі реального часу.

- RTCM 2.x: старий стандарт, використовуваний для базових поправок.
- RTCM 3.x: сучасний стандарт із покращеною компактністю та підтримкою багатосмугових GNSS-систем.

Призначення:

- Передача поправок для систем DGPS (диференціального GPS) і RTK (кінематичне позиціонування в реальному часі).

Структура повідомлення:

- Початок кадру: завжди починається з D3 (у двійковому - 11010011) - це преамбула.
- За преамбулою йде довжина повідомлення (10 біт).
- Далі - ID типу повідомлення (12 біт) і самі дані (залежно від типу).
- Кожне повідомлення завершується CRC-24Q для перевірки цілісності.

Типи повідомлень:

- 1005 (Reference Station ARP) - Передає положення базової станції у вигляді геоцентричних координат X, Y, Z у системі WGS-84. Ці координати використовуються рухомим приймачем для обчислення відносної позиції. Повідомлення не містить інформації про висоту антени.
- 1006 (Reference Station ARP + Height) - Варіант повідомлення 1005, доповнений додатковим полем - висотою антени над референтною точкою. Це дозволяє підвищити точність вертикального позиціювання.
- 1019 (GPS Ephemeris Data) - Містить ефемериди супутників GPS. Ці орбітальні параметри дозволяють приймачу розрахувати точне положення

супутника у конкретний момент часу, що критично важливо для високоточних навігаційних розрахунків.

• 1020 (GLONASS Ephemeris Data) - Аналог повідомлення 1019 для супутників GLONASS. Формат трохи відрізняється через специфіку системи GLONASS (наприклад, різна структура частот та координатні системи).

• 1033 (Antenna Descriptor) - Містить опис обладнання базової станції: тип антени, серійний номер, тип GNSS-приймача. Ці дані важливі для ідентифікації джерела поправок у мережах RTK.

• 1074 (MSM4 - GPS Multiple Signal Messages) - Одне з найбільш використовуваних повідомлень нового покоління. Передає багатосигнальні дані з супутників GPS: псевдовідстані, фазові вимірювання, час захоплення сигналу, CNR (рівень сигналу/шуму). Забезпечує високу точність позиціювання.

• 1084 (MSM4 - GLONASS Multiple Signal Messages) - Аналог 1074 для GLONASS. Забезпечує обробку багатьох супутників і частот одночасно, що особливо корисно у міських умовах або для мультисистемних приймачів.

• 1094 (MSM4 - Galileo Multiple Signal Messages) - Містить багаточастотні дані від супутників Galileo. Підтримує точне позиціювання у глобальних та регіональних системах навігації.

• 1114 (MSM4 - QZSS Multiple Signal Messages) - Використовується для обміну високоточними даними від супутників QZSS (японська регіональна навігаційна система).

• 1124 (MSM4 - BeiDou Multiple Signal Messages) - Забезпечує передачу багаточастотних даних від супутників китайської системи BeiDou. Забезпечує повноцінну підтримку глобального GNSS-розрахунку.

Переваги:

• Висока точність позиціонування (до сантиметрів у режимі RTK).

Недоліки:

- Залежність від стабільного каналу передачі даних для підтримки зв’язку в реальному часі. [9]

1.6.4 LoRa (Long Range)

LoRa, абревіатура від Long Range - це технологія бездротового зв'язку великої дальності з низьким енергоспоживанням. У 2009 році французька компанія Cycleo розробила алгоритм для широкосмугового зв'язку, котрий потім був придбаний американською компанією Semtech, що випустила чіп LoRa у 2013 року.

Основні характеристики:

- Дальність передачі: до 15 км у відкритому просторі
- Швидкість передачі: 300 біт/с - 37.5 кбіт/с
- Споживання енергії: дуже низьке (ідеально для пристроїв на батарейках)
- Частотні діапазони: ISM (безкоштовні) частоти - 433 МГц, 868 МГц (Європа), 915 МГц (США)
- Тип модуляції: CSS (Chirp Spread Spectrum) - дозволяє сигналу залишатися розпізнаваним навіть за низького рівня SNR (співвідношення сигнал/шум).
- Енергоспоживання: Надзвичайно низьке, що дозволяє пристроям працювати на батареях роками.
- Безпека: Шифрування AES-128 для захисту даних.

Мережа на базі LoRa зазвичай складається з:

- LoRa-терміналів (сенсори, пристрої)
- LoRa-шлюзів (gateway), які передають дані в інтернет
- Серверів (мережевий, додатків, контролю доступу, тощо)

На основі LoRa працює вищий протокол - LoRaWAN, який визначає архітектуру мережі та методи доступу до середовища.

Переваги:

• Хороша завадостійкість - завдяки спектрально-розширеній модуляції (CSS) має високий рівень стійкості до завад.

Недоліки:

• Обмежена кількість одночасних підключень у щільних мережах - при великій кількості пристроїв можливі колізії.

• Відносно висока вартість обладнання - особливо це стосується шлюзів промислового рівня. [10]

Таблиця 1.1 - Порівняння протоколів зв’язку та навігаційних даних, що використовуються в БПЛА

	NMEA	UBX	RTCM	LoRa
Тип протоколу	Текстовий, ASCII	Бінарний, двійковий	Бінарний, стандартний	Радіопротокол (MAC + PHY)
Призначення	Навігаційні дані від GNSS-приймача	Повна конфігурація та отримання даних з GNSS-чипа	Передача поправок у режимі реального часу (RTK, DGPS)	Дальній бездротовий зв’язок для сенсорних/телеметричних даних
Структура повідомлень	$ID,дані,…*контрольна_сума	Sync(0xB5, 0x62) + Class + ID + Length + Payload + Checksum	D3 (преамбула) + Довжина + ID + Дані + CRC-24Q	Payload + CRC + Frame Info
Формат	Людинозрозумілий, текстовий	Компактний, для комп’ютерної обробки	Компактний, для високоточної навігації	Широкоспектральна модуляція (CSS), пакети малого об’єму
Типові повідомлення	GGA, RMC, VTG, GSV, GSA	NAV-POSLLH, NAV-VELNED, CFG-MSG	1005, 1019, 1033, 1074, 1094, 1124 тощо	Визначається LoRaWAN або власним протоколом

Продовження таблиці 1.1

	NMEA	UBX	RTCM	LoRa
Обсяг даних	Великий - 60-100 байт/повідомлення	Малий - 20-60 байт/повідомлення	Середній - залежно від типу повідомлення	Дуже малий - 11-51 байт/пакет
Пропускна здатність	~4800-9600 бод	Висока (до 115200 бод)	Середня (високоточні RTK системи - до 9600 бод)	Низька (0.3-50 кбіт/с)
Затримка	Мінімальна	Мінімальна	Мінімальна (при стабільному каналі)	Залежить від конфігурації та навантаження
Стійкість до завад	Низька	Вища (за рахунок компактності)	Середня	Висока (спектральне розширення
Вимоги до обробки	Простий розбір (парсинг), великі об’єми	Необхідне спец. ПЗ (u-center), складність для людини	Специфічне ПЗ або ГНСС-бібліотеки (RTKLIB, Trimble, Septentrio)	Потребує LoRaWAN- або власного контролера
Сумісність	Стандартизований, підтримується більшістю модулів	Можлива на рівні застосунку	Залежить від ГНСС-приймача та ПЗ	Відкрита, з LoRaWAN підтримкою
Основні переваги	Простота, стандартизація	Ефективність, багатофункціональність	Висока точність позиціювання (до сантиметрів)	Велика дальність, низьке споживання
Основні недоліки	Великі об’єми, низька ефективність	Складність у налаштуванні	Залежність від каналу передачі, складність у реалізації	Обмеження на трафік і кількість пристроїв

Як видно з порівняльної таблиці, кожен із розглянутих протоколів має свої особливості та обмеження. Текстовий протокол NMEA залишається поширеним завдяки простоті інтеграції, проте поступається в ефективності бінарному UBX. Протокол RTCM є критично важливим для реалізації високоточного позиціонування в режимі RTK, особливо у бойових умовах. У той час як LoRa вирізняється великою дальністю та низьким енергоспоживанням, що робить його привабливим для створення мережевого зв'язку з великою автономністю. Вибір конкретного протоколу повинен залежати від вимог до точності, захищеності, затримки, енергоефективності та складності реалізації у системах зв'язку БПЛА.

Використання сучасних протоколів зв'язку, таких як NMEA, UBX, RTCM та LoRa, забезпечує ефективну передачу телеметричної інформації, координат, керуючих команд і службових повідомлень між наземними станціями та безпілотними літальними апаратами. Проте ефективність роботи зазначених протоколів значною мірою залежить від радіочастотного середовища, у якому здійснюється передача сигналів, особливо в умовах активної радіоелектронної боротьби.

1.7 Роль частотних діапазонів

Одним із ключових аспектів ефективної роботи БПЛА є стабільний і захищений радіозв'язок, що здійснюється в частотних діапазонах. Саме вибір та використання частотного діапазону визначає якість зв'язку між оператором та безпілотником, стійкість до перешкод, дальність керування. У бойових умовах, де інтенсивно використовуються засоби глушіння та перехоплення сигналу, правильне використання частот стає важливим аспектом для результативності дрона.

У бойових умовах використовуються різні частотні діапазони, включаючи HF (3-30 МГц), VHF (30-300 МГц) та UHF (300-3000 МГц). Для боротьби з

дронами можуть одночасно або незалежно подавлятися загальні діапазони частот, такі як 900 МГц, 1,5 ГГц, 5,8 ГГц. Системи протидії БПЛА можуть працювати в діапазонах 400-470 МГц, 850-930 МГц, 1550-1620 МГц, 2400-2480 МГц, 5725-5850 МГц.

Частотні діапазони мають прямий вплив на стійкість зв'язку з БПЛА в умовах бойових дій. Вибір певного діапазону визначає:

• Дальність зв'язку: Різні частоти мають різну здатність до поширення та проникнення через перешкоди. Наприклад, нижчі частоти можуть краще огинати перешкоди, але можуть бути більш схильними до певних видів природних та індустріальних перешкод. Вищі частоти можуть забезпечувати більшу пропускну здатність для передачі даних (наприклад, відео високої роздільної здатності), але їх поширення більше залежить від прямої видимості та вони сильніше поглинаються атмосферою та перешкодами.

• Стійкість до перешкод: Противник активно використовує РЕБ для створення навмисних перешкод у частотних діапазонах, які використовуються для управління БПЛА. Ефективність подавлення залежить від потужності завади, відстані до джерела сигналу БПЛА та використовуваного частотного діапазону. Деякі частоти можуть бути більш завантаженими через використання іншими системами зв'язку, що робить їх більш вразливими до ненавмисних та навмисних перешкод.

• Пропускна здатність: Ширина виділеного частотного діапазону впливає на обсяг інформації, який можна передати за одиницю часу. Для передачі відеопотоку в реальному часі потрібна більша пропускна здатність, яку зазвичай забезпечують вищі частотні діапазони.

Оптимізація частотних діапазонів для кращої роботи в умовах РЕБ є критично важливим завданням. Існує кілька стратегій для підвищення стійкості зв'язку:

• Використання кількох частотних діапазонів: БПЛА та системи управління можуть бути розроблені з можливістю швидкого переходу між

різними робочими частотами або використання декількох частот одночасно. При виявленні перешкод на одній частоті, система може автоматично або за командою оператора переключитися на резервну частоту, менш схильну до впливу РЕБ. Пристрій може мати кілька вбудованих модульних діапазонів частот, що забезпечує незалежне управління та налагодження модулів у різних діапазонах.

• Псевдовипадкова перебудова робочої частоти (ППРЧ): Ця технологія передбачає швидку та псевдовипадкову зміну робочої частоти за заздалегідь визначеним алгоритмом. Це значно ускладнює противнику ефективне подавлення сигналу, оскільки завада постійно втрачає ціль.

• Використання нестандартних частот: Застосування частотних діапазонів, які рідше використовуються або не входять до стандартних наборів частот засобів РЕБ противника, може ускладнити їх подавлення.

• Направлені антени: Використання направлених антен як на стороні оператора, так і на БПЛА дозволяє концентрувати енергію сигналу в вузькому промені в напрямку один одного. Це зменшує ймовірність перехоплення та подавлення сигналу з інших напрямків.

• Оптимізація протоколів зв'язку: Використання стійких до перешкод методів модуляції та кодування сигналу може підвищити надійність передачі даних навіть в умовах дії завад. Аналоговий зв'язок може частково відновлюватися при якісній фільтрації шуму, на відміну від цифрового, де втрата пакетів може призвести до неможливості декодування. Для відеозв'язку з FPV дронами відсутність необхідності кодування-декодування робить його швидшим і стійкішим до РЕБ.

• Моніторинг спектра: Постійний моніторинг радіоефіру за допомогою портативних аналізаторів спектра дозволяє виявляти джерела перешкод та аналізувати їх характеристики, що дає змогу оперативно змінювати робочі частоти або застосовувати відповідні контрзаходи.

Таким чином, ефективне використання частотних діапазонів для управління БПЛА в умовах бойових дій вимагає комплексного підходу, що включає вибір оптимальних частот, застосування технологій захисту від РЕБ та постійний моніторинг електромагнітної обстановки. Гнучкість у виборі частот та здатність швидко адаптуватися до змін у радіоефірі є ключовими факторами забезпечення стійкого зв'язку та ефективного застосування БПЛА.

1.8 Висновки до розділу 1

У першому розділі було здійснено аналіз структурної організації безпілотних літальних апаратів (БПЛА) та особливостей їх функціонування з точки зору радіозв’язку. Було окреслено основні компоненти сучасного БПЛА, що включають систему управління, навігаційний модуль, радіомодуль, антенні пристрої та засоби телеметрії, які утворюють єдину інформаційно-керуючу систему.

Розгляд фізичних властивостей радіохвиль дозволив з’ясувати ключові закономірності їх розповсюдження, такі як відбиття, дифракція, заломлення та затухання сигналів. Окремо було проаналізовано вплив різних типів місцевості (лісистої, міської, відкритої) та погодних умов (дощ, туман, іоносферні збурення) на якість та стабільність радіозв’язку.

У підрозділі, присвяченому антенам, охарактеризовано типи антен, які використовуються в БПЛА, а також їх вплив на діаграму направленості, коефіцієнт підсилення та ширину променя, що критично важливо для забезпечення цілеспрямованої передачі сигналів у бойових умовах.

Особливу увагу приділено темі радіоелектронної боротьби (РЕБ). Розкрито класифікацію засобів РЕБ, основні напрями їхнього функціонального застосування, зокрема створення активних і пасивних перешкод, перехоплення сигналів управління та подавлення каналів зв’язку.

Проаналізовано типові форми ведення РЕБ у контексті сучасних військових конфліктів, що дозволяє краще розуміти загрози для систем управління БПЛА.

Важливим аспектом став огляд сучасних протоколів зв’язку, що використовуються для передачі навігаційної та службової інформації, зокрема NMEA, UBX Binary, RTCM та LoRa. Наведено їхні функціональні особливості, переваги та недоліки з огляду на вимоги до захищеності, надійності та енергоефективності.

Завершальний підрозділ було присвячено ролі частотних діапазонів, що використовуються для управління БПЛА в умовах бойових дій. З’ясовано, що вибір частоти значною мірою визначає стійкість до перешкод, дальність зв’язку та ймовірність виявлення, що, своєю чергою, формує технічні вимоги до адаптивних систем зв’язку в умовах радіоелектронного протистояння.

Отримані результати та узагальнення створюють основу для подальшого дослідження методів захисту радіоканалів, аналізу алгоритмів стійкої модуляції, частотного перестроювання у наступних розділах.

2 МЕТОДИ ЗАХИСТУ РАДІОЗВ’ЯЗКУ ВІД ПЕРЕШКОД І ГЛУШІННЯ

З огляду на результати, отримані в попередньому розділі, можна зробити висновок, що ефективність функціонування систем управління безпілотними літальними апаратами (БПЛА) значною мірою залежить від надійності радіоканалів у складному та змінному радіочастотному середовищі. В умовах бойових дій особливої актуальності набуває проблема впливу навмисних перешкод, які створюються засобами радіоелектронної боротьби для придушення або спотворення сигналів управління і телеметрії.

Цей розділ присвячено аналізу сучасних методів захисту радіозв’язку від перешкод і глушіння. Розглянуто як класичні технічні рішення, зокрема частотне перестроювання, поширення спектра, адаптивне управління модуляцією, так і інноваційні підходи на основі штучного інтелекту та програмно-визначених радіосистем. Особливу увагу приділено їхній доцільності для використання в системах зв’язку БПЛА з урахуванням загроз з боку РЕБ.

У сучасних бойових умовах, через постійне використання засобів радіоелектронної боротьби, захист системи радіозв’язку безпілотних літальних апаратів набуває критичного значення. Противник активно використовує різні типи перешкод - від точкових до високотехнологічних засобів глушіння сигналу.

У відповідь на ці загрози необхідно впроваджувати багаторівневі методи захисту, які включають як технічні рішення, так і програмні алгоритми.

У цьому розділі розглядаються ключові підходи до забезпечення стійкості зв’язку БПЛА, від використання сучасних методів шифрування, котрі захищають дані від несанкціонованого доступу, до впровадження динамічного управління частотами, що дозволяє зменшити ефективність ворожих завад.

Мета цього розділу - проаналізувати наявні технології та принципи, які підвищують захищеність каналів зв’язку дронів, і визначити їхню ефективність в умовах дії потужних радіоелектронних впливів.

2.1 Шифрування і захист сигналу

Шифрування один із способів захисту інформації в системах радіозв’язку БПЛА. Воно забезпечує конфіденційність, цілісність і автентичність даних, що передаються між безпілотником та наземною станцією, адже зв'язок між БПЛА та наземною станцією керування може бути вразливим до атак типу "людина посередині", де зловмисник може перехопити та дізнатися про передані дані. Для вирішення цих проблем необхідно впроваджувати ефективні механізми шифрування та захисту сигналу в системах зв'язку БПЛА. Існуючі підходи включають використання різних криптографічних алгоритмів та протоколів безпеки.

Надійний захист радіозв'язку є критично важливим, особливо для безпілотних літальних апаратів, які можуть передавати чутливі дані або виконувати завдання в умовах потенційного перехоплення чи глушіння. Шифрування та методи захисту сигналу відіграють ключову роль у забезпеченні конфіденційності, цілісності та доступності зв’язку.

Методи шифрування даних поділяються на два основні типи: симетричне та асиметричне шифрування.

2.1.1 Симетричні алгоритми

Симетричні алгоритми використовують один ключ для шифрування та розшифрування. Хоча раніше застосовувався алгоритм IDEA [11], сьогодні він вважається застарілим.

Ключовим сучасним стандартом є AES (Advanced Encryption Standard), що підтримує ключі довжиною 128, 192 та 256 біт [12]. Його робота базується на виконанні послідовних раундів перетворень над блоками даних [13].

Проте, реалізація AES у найпростішому режимі ECB (Electronic Code Book) є вразливою. Оскільки однакові блоки відкритого тексту шифруються в однакові блоки шифротексту, це дозволяє зловмиснику аналізувати трафік [14]. Наприклад, у російському БПЛА «Орлан-10» апаратне шифрування реалізовано саме за допомогою AES-128 у режимі ECB [15, 16]. Аналогічні вразливості існують і в апаратних модулях мікроконтролерів, що знижує стійкість системи до перехоплення.

2.1.2 Асиметричні алгоритми

Асиметричні алгоритми використовують пару ключів (відкритий та приватний), що усуває проблему безпечного обміну секретним ключем.

RSA. Цей алгоритм, що базується на складності факторизації великих чисел [17], зазвичай застосовується для безпечного обміну симетричними ключами. Його недоліком є потреба у ключах великої довжини (2048 біт і більше), що вимагає значних обчислювальних ресурсів.

Криптографія на еліптичних кривих (ECC). Є більш ефективною альтернативою, яка забезпечує аналогічний рівень безпеки при значно меншій довжині ключа. Наприклад, 256-бітний ключ ECC еквівалентний за надійністю 3072-бітному ключу RSA [18, 19]. Завдяки компактності та високій продуктивності, ECC є перспективним стандартом для пристроїв з обмеженими ресурсами, як-от БПЛА [20]. Однак, ECC є вразливою до атак побічними каналами (side-channel attacks) у разі некоректної програмної реалізації [21].

На практиці асиметричні алгоритми (RSA або ECC) часто комбінують із симетричними (AES) у гібридних схемах: асиметричний алгоритм

використовується для встановлення захищеного з'єднання та обміну ключами, а симетричний - для швидкого шифрування основного потоку даних [22].

2.2 Методи захисту радіозв'язку від перешкод і глушіння

Один із найефективніших способів захисту радіозв’язку від перешкод - це використання технології розширення спектру з перестрибуванням частот (Frequency Hopping Spread Spectrum, FHSS). Цей метод був уперше запропонований ще під час Другої світової війни актрисою Геді Ламарр і композитором Джорджем Антейлом для забезпечення захищеного керування торпедами [23]. Із того часу технологія зазнала суттєвої еволюції й нині є невіддільною складовою багатьох сучасних систем зв’язку, зокрема у військових радіостанціях, Bluetooth та Wi-Fi.

Суть роботи FHSS полягає у динамічній зміні частоти передачі сигналу відповідно до заздалегідь узгодженого алгоритму. Спершу визначається широка смуга частот (наприклад, 2,4 ГГц для Bluetooth), яка ділиться на окремі канали. Передавач і приймач синхронізовано перестрибують між цими каналами за псевдовипадковою послідовністю, відомою лише обом сторонам зв’язку. Такий підхід значно ускладнює виявлення та глушіння сигналу. У сучасних системах, як-от Bluetooth 5.0, частота перестрибування може сягати до 1600 разів на секунду [24], що забезпечує високий рівень захисту й стійкості до радіоелектронних перешкод.

2.2.1 Реалізація FHSS у безпілотних літальних апаратах

У сфері безпілотних літальних апаратів (БПЛА) технологія FHSS широко використовується для забезпечення надійного зв’язку між дроном і оператором, особливо в умовах дії засобів радіоелектронної боротьби (РЕБ). Перед початком польоту здійснюється синхронізація між БПЛА та наземною

станцією: обмінюються ключі перестрибування, визначається початкова частота та часові параметри. У процесі польоту відбувається постійне перемикання каналів зв’язку відповідно до узгодженого алгоритму, а у випадку виявлення глушіння система автоматично переходить на резервні частоти. Передача коротких пакетів даних дозволяє зменшити втрати інформації під час частотних перестрибувань. Наприклад дрон DJI Matrice 300 впроваджує подвійну систему FHSS, поєднуючи частоти 2.4 ГГц і 900 МГц, що підвищує загальну надійність зв’язку [25].

Ефективність використання FHSS у безпілотних літальних апаратах значною мірою залежить від правильного вибору та конфігурації параметрів системи зв’язку. У загальному випадку оператор БпЛА повинен обрати оптимальний частотний діапазон (наприклад, 2,4 ГГц, 5,8 ГГц або 900 МГц), визначити кількість каналів, які будуть використані для перестрибування, а також задати тип алгоритму перестрибування. Найпростішим є послідовний алгоритм (Sequential Hopping), однак у системах, що працюють в умовах інтенсивного радіоелектронного протидії, більш доцільним є застосування псевдовипадкового перестрибування (Pseudorandom Hopping), що забезпечує вищу завадостійкість та зменшує ймовірність прогнозування частот противником.

У сучасних безпілотних системах конфігурація FHSS включає також попереднє сканування радіоефіру для виявлення зашумлених або зайнятих каналів, після чого формується таблиця допустимих частот. Перед польотом здійснюється тестування зв’язку в режимі реального часу з метою перевірки стабільності комунікаційного каналу.

Наприклад розглянемо систему FHSS, яка реалізована в військовому безпілотному літальному апараті «Мерлин-ВР». Згідно з даними, ця система використовує високошвидкісне частотне перестрибування зі швидкістю 50 стрибків на секунду, що забезпечує високу завадостійкість та знижує ймовірність перехоплення сигналу. Кожна посилка передається протягом 7,77

мс, після чого відбувається пауза тривалістю 12,23 мс. Завдяки цьому формується динамічний, нестабільний для ворожих засобів РЕБ радіосигнал.

Миттєва ширина спектра сигналу складає приблизно 730 кГц, а крок сітки частот - 500 кГц, що дозволяє уникати накладення частот при щільному плануванні каналу. У накопиченому спектрі передбачено 10 номіналів частот у діапазоні приблизно 914,95-919,45 МГц, зокрема 914,95 МГц; 915,45 МГц; 915,95 МГц; ... до 919,45 МГц. Таким чином, загальна ширина накопиченого спектра складає близько 5,23 МГц, що відповідає нормам частотного планування у військових мережах тактичного рівня.

Реалізація FHSS із такими характеристиками дозволяє системі зв’язку «Мерлин-ВР» протистояти як активному глушінню, так і спробам радіотехнічного розвіддання. Динамічність спектру, швидкість стрибків і обмежена тривалість передачі кожної посилки формують комунікаційне середовище з високим ступенем еластичності, що є надзвичайно важливим у бойових умовах.

Разом з тим, незважаючи на свої переваги, технологія FHSS (Frequency Hopping Spread Spectrum) має певні обмеження. Однією з основних проблем є затримка сигналу, що виникає внаслідок постійного перемикання частот. У системах реального часу, зокрема під час польоту та маневрування БПЛА, це може призвести до зменшення точності або затримок в управлінні. Одним з можливих рішень є реалізація пріоритетного обслуговування критичних пакетів, таких як команди управління або телеметричні дані, з використанням окремих, слабо завантажених каналів.

2.3 Інтелектуальне управління частотами

Новітнім напрямом у захисті радіозв’язку є використання штучного інтелекту для автоматичної зміни частот. Алгоритми підсиленого навчання (Reinforcement Learning) здатні аналізувати поточний рівень перешкод і

динамічно визначати найменш зашумлені канали. Один із прикладів реалізації - система Cognitive Radio, розроблена компанією Lockheed Martin, яка застосовує ШІ для запобігання глушінню у режимі реального часу [26]. Такий підхід суттєво підвищує адаптивність та ефективність зв'язку в складних умовах.

Окрім FHSS, існують й інші підходи до захисту сигналів від перешкод. Одним з них є метод прямого розширення спектру (Direct Sequence Spread Spectrum, DSSS), який застосовується, зокрема, у системах GPS та деяких військових засобах зв'язку. Сигнал у DSSS розширюється шляхом накладання шумоподібного коду (наприклад, коду Баркера), що ускладнює його виявлення та глушіння. Оскільки перешкоджувальні сигнали зазвичай не мають доступу до коду розширення, DSSS забезпечує високу завадостійкість. Яскравим прикладом є система Link 16, яка широко використовується у Збройних силах НАТО [27].

Одним із важливих засобів підвищення ефективності зв'язку в безпілотних літальних апаратах є адаптивна модуляція та кодування (Adaptive Modulation and Coding,). Ця технологія забезпечує динамічне підлаштування параметрів модуляції та кодування залежно від поточних умов радіоканалу. У сприятливих умовах - при високому співвідношенні сигнал/шум (SNR), система може застосовувати високоефективні схеми, такі як 64-QAM або 256-QAM, що дозволяють досягати великих швидкостей передачі даних. Однак у разі появи завад або погіршення якості каналу, зв'язок автоматично перемикається на менш складні, але більш стійкі схеми, наприклад QPSK або BPSK. Це забезпечує безперервність та надійність зв'язку навіть у складних умовах [28].

Технологія AMC широко застосовується у сучасних комерційних та професійних БПЛА. Зокрема, у дронах серії DJI Matrice 300 RTK реалізовано автоматичне перемикання модуляційних схем, що дозволяє підтримувати

стабільну трансляцію відеопотоку на відстані до 15 км навіть за наявності перешкод у середовищі [29].

2.4 Програмно-визначене радіо

Програмно-визначене радіо (SDR, Software Defined Radio) є ключовою технологією сучасних бездротових систем зв’язку, що переносить більшість апаратних функцій (модуляція, демодуляція, фільтрація, спектральний аналіз) у програмне забезпечення. Це дозволяє створювати гнучкі, швидко оновлювані системи, здатні адаптуватися до змінних радіочастотних умов, особливо в умовах радіоелектронної боротьби [30; 31].

Фізично SDR складається з радіофронтенду - антени, підсилювачів, фільтрів, аналого-цифрових перетворювачів - та цифрової платформи, яка виконує обробку сигналів у реальному часі за допомогою процесорів, FPGA або DSP [32]. Така архітектура дозволяє підтримувати різні стандарти зв’язку і швидко змінювати параметри залежно від обстановки.

Для безпілотних літальних апаратів важливою перевагою SDR є здатність динамічно адаптуватися до перешкод і глушіння, змінюючи частоту, тип модуляції, потужність передавання або алгоритми кодування. Це робить системи більш стійкими до РЕБ і підвищує надійність зв’язку в бойових умовах [33]. Крім того, програмна природа системи дозволяє оновлювати протоколи зв’язку і безпеки дистанційно, що особливо актуально для масштабного розгортання БПЛА.

Практична реалізація SDR у дронах передбачає використання MIMO-конфігурацій, супутникової навігації та криптозахисту. Типові частотні діапазони - 900 МГц, 2,4 ГГц, 5,8 ГГц - із підтримкою таких протоколів як FHSS, OFDM, QPSK. SDR-системи можуть в реальному часі оцінювати зайнятість спектра, формувати спектральні карти, здійснювати частотне перестрибування і шифрувати передачі з мінімальними затримками [34; 35].

Прикладом є модулі Harris RF-7850A, які встановлюються на тактичні БПЛА типу RQ-21 Blackjack і забезпечують захищений зв’язок із застосуванням адаптивного кодування, криптографії та інтелектуального управління ресурсами спектра [36]. В Україні розробки на базі GNU Radio демонструють підтримку стрибкоподібної зміни частоти, спектрального аналізу FFT та інтеграцію з наземними SDR-приймачами, такими як HackRF і Ettus USRP [37].

Таким чином, SDR є критично важливою складовою сучасних систем зв’язку для БПЛА, що підвищує їх живучість, гнучкість і здатність адаптуватися до складних умов радіочастотного середовища, особливо під час радіоелектронної боротьби.

2.5 Висновки до розділу 2

У другому розділі проведено комплексний аналіз методів забезпечення стійкого та захищеного радіозв’язку для безпілотних літальних апаратів в умовах активного радіочастотного протистояння. Особлива увага приділена технологіям, здатним протидіяти впливу як природних, так і штучних (ворожих) перешкод, зокрема тим, що створюються в результаті роботи засобів радіоелектронної боротьби.

Перш за все, розглянуто криптографічні методи захисту інформації, що передається. Симетричні алгоритми (наприклад, AES) забезпечують високошвидкісне шифрування даних при наявності спільного ключа, але потребують ефективної системи керування ключами. Асиметричні методи (RSA, ECC) дозволяють вирішити цю проблему завдяки використанню відкритих і закритих ключів, однак вимагають більше обчислювальних ресурсів. Важливим є те, що застосування криптографії гарантує збереження цілісності, автентичності й конфіденційності управлінських і телеметричних повідомлень БПЛА.

У межах фізичного рівня комунікації досліджено ефективність застосування технології FHSS (Frequency Hopping Spread Spectrum), яка забезпечує частотну псевдовипадкову зміну несучої частоти сигналу. Це ускладнює завдання глушіння або перехоплення сигналу противником, оскільки необхідно знати алгоритм стрибків і їхню синхронізацію. Описано теоретичні основи та принципи реалізації FHSS, а також можливість її конфігурації оператором відповідно до умов місії та рівня загрози.

Крім того, розглянуто перспективи інтелектуального управління частотами, які базуються на алгоритмах машинного навчання. Такі алгоритми дозволяють системам БПЛА в реальному часі оцінювати радіочастотне середовище, прогнозувати дії противника та обирати оптимальні параметри зв’язку, що значно підвищує виживаність апарата в складних умовах.

Також було досліджено програмно-визначене радіо (SDR) як ключовій технології для реалізації адаптивних систем зв’язку. SDR забезпечує гнучке перепрограмування характеристик радіопередавача без фізичного втручання, що дозволяє оперативно змінювати тип модуляції, ширину каналу, частоту та інші параметри відповідно до зовнішніх умов і загроз. Поєднання SDR із технологіями розширеного спектра та інтелектуального управління частотами дозволяє досягти високого рівня захищеності зв’язку та його безперервності в складних електромагнітних умовах.

Таким чином, у результаті аналізу встановлено, що ефективний захист зв’язку БПЛА в умовах радіоелектронної боротьби досягається за рахунок комплексного застосування криптографічних протоколів, технологій динамічного перестроювання частот, інтелектуальних алгоритмів адаптації та гнучких SDR-рішень.

3 ВИКОРИСТАННЯ СУПУТНИКОВОГО ІНТЕРНЕТУ ДЛЯ ПОКРАЩЕННЯ ЗВ'ЯЗКУ

3.1 Аналіз супутникових систем зв'язку

Потреба в ефективному каналі зв'язку для безпілотних літальних апаратів є критично важливою, особливо в умовах сучасного ведення бойових дій, де широко застосовуються засоби радіоелектронної боротьби. Наземні канали зв'язку, зокрема радіорелейні, Wi-Fi та LTE-з'єднання, швидко стають неефективними у випадку активного подавлення сигналу або фізичного знищення мережевої інфраструктури. У зв'язку з цим супутникові технології дедалі більше розглядаються як ключовий інструмент забезпечення надійного управління та передачі даних для БПЛА в зоні бойових дій.

Світовий досвід, зокрема країн НАТО, свідчить про системне впровадження супутникового зв'язку у військові комунікаційні платформи. Наприклад, США експлуатують одразу кілька супутникових систем - AEHF (Advanced Extremely High Frequency), MUOS (Mobile User Objective System) та WGS (Wideband Global SATCOM). Система AEHF забезпечує багатоканальний захищений зв'язок, призначений для стратегічного управління, з використанням Q-діапазону (44/20 ГГц), що має високу стійкість до завад і можливість передачі даних із високим ступенем шифрування [38]. MUOS, яка функціонує в UHF-діапазоні, орієнтована на мобільні користувачі, зокрема платформи типу БПЛА, і підтримує сучасні стандарти адаптивного зв'язку, сумісні з технологіями 3G [39].

У європейському просторі подібні системи також активно застосовуються. Наприклад, Велика Британія експлуатує систему Skynet 5, яка розгорнута на геостаціонарній орбіті та інтегрована у спільну інфраструктуру НАТО. Система здатна забезпечувати мобільний зв'язок з високою пропускною здатністю навіть у зоні активних бойових дій [40]. Франція розгорнула супутники Syracuse III, які забезпечують захищений канал зв'язку

в X- і Ka-діапазонах, адаптований для платформ, що діють у складному електромагнітному середовищі. Німеччина, у свою чергу, впровадила систему SATCOMBw, яка, крім стратегічного використання, має можливість інтеграції з мобільними бойовими платформами, включаючи безпілотні літальні апарати [41].

Особливої уваги заслуговує поява комерційних супутникових систем, таких як Starlink (SpaceX), які довели свою ефективність у реальних бойових умовах. Після початку повномасштабного вторгнення РФ в Україну у 2022 році, система Starlink стала критичним елементом забезпечення зв'язку для Збройних Сил України, особливо у районах, де традиційна інфраструктура була знищена або перебувала під впливом РЕБ. Система використовує низькоорбітальні супутники (LEO) на висоті близько 550 км, забезпечуючи низьку затримку (30-60 мс) і високошвидкісну передачу даних, що дає змогу ефективно передавати телеметрію, координати цілей, відеопотоки з камер БПЛА в реальному часі тощо.

Starlink підтримує технологію beamforming - формування вузьконаправленого променя сигналу, що дозволяє суттєво зменшити площу можливого подавлення сигналу. Крім того, у систему інтегровано frequency hopping - частотне псевдовипадкове перестроювання, яке ускладнює роботу засобів РЕБ противника. За даними Державної служби спеціального зв'язку та захисту інформації України, Starlink використовується не лише для передачі команд і координат, а й для підтримки обміну в тактичних мережах - між командирами на полі бою та центрами управління [42].

Варто зазначити, що не лише Starlink, але й інші системи - такі як Iridium, OneWeb або Globalstar - поступово впроваджуються у військові програми. Наприклад, Iridium, попри свою низьку пропускну здатність (до 128 кбіт/с), відзначається дуже високою живучістю, стійкістю до глушіння та здатністю функціонувати навіть за наявності інтенсивного радіоелектронного впливу. Це

робить її доцільною для резервного зв’язку або передавання службової інформації в екстремальних умовах [43].

Застосування комерційних систем у військових цілях має як переваги, так і обмеження. До переваг належать швидкість розгортання, мобільність терміналів, доступність обладнання та висока якість зв’язку. До недоліків - потенційна вразливість до централізованого управління доступом (наприклад, вимкнення покриття з боку постачальника), обмежена захищеність цивільних каналів і політичні ризики. Прецеденти, пов’язані з тимчасовим обмеженням покриття Starlink на певних територіях, вже викликали занепокоєння серед військових аналітиків [42].

У військовому плануванні дедалі частіше реалізується концепція гібридного супутникового зв’язку, яка передбачає одночасне використання як державних військових систем, так і комерційних платформ. Такий підхід забезпечує багаторівневу надлишковість, адаптивність і стійкість до багатьох типів загроз. Зокрема, БПЛА можуть бути оснащені мультипротокольними терміналами, що автоматично перемикаються між каналами в залежності від наявності сигналу, рівня шуму або активності засобів РЕБ.

3.2 Оцінка переваг супутникового зв’язку для передачі даних на великі відстані

Традиційні засоби радіозв’язку обмежені лінією прямої видимості, потужністю передавача, значним затуханням сигналу на великих відстанях, а також високою вразливістю до радіоелектронного придушення (РЕБ). У порівнянні з цим, супутниковий зв’язок надає можливість глобального покриття з мінімальною залежністю від наземної інфраструктури, що особливо важливо в умовах зруйнованої або відсутньої інфраструктури, типових для зон бойових дій [44].

Супутникові системи базуються на двох основних орбітальних групах: геостаціонарні супутники (GEO), які забезпечують стабільне покриття фіксованих регіонів, та супутники низької навколоземної орбіти (LEO), що швидко рухаються над поверхнею Землі, забезпечуючи більшу масштабованість і гнучкість. Системи на базі LEO, такі як Starlink, складаються з тисяч супутників, які створюють мережу з широким і стійким покриттям навіть у віддалених та прифронтових районах, де наземні мережі відсутні або зруйновані [44].

Особливою перевагою супутникового зв'язку є його стійкість до традиційних засобів РЕБ. Сигнали супутникових систем приходять під кутом, а не горизонтально, що ускладнює їхнє ефективне придушення за допомогою наземних засобів глушіння, які орієнтовані саме на горизонтальне подавлення радіосигналів [45]. Крім того, використання спрямованих антен і динамічне частотне перестроювання в LEO-системах дозволяє мінімізувати вплив активного радіоперешкоджання [46].

Швидкість передачі даних у сучасних супутникових системах Starlink, OneWeb сягає 100- 300 Мбіт/с, що дозволяє безперервно передавати відео високої чіткості, телеметрію та командні сигнали керування БПЛА. Навіть менш потужні системи, такі як Iridium, ефективні для передачі координат, текстових повідомлень і навігаційних сигналів, що важливо для підтримки зв'язку в умовах обмежених ресурсів [47]. Крім того, затримка сигналу у LEO-супутниках складає 30- 60 мс, що є критично низьким показником для задач оперативного управління і контролю безпілотників, на відміну від GEO-супутників із затримкою до 600 мс, що є занадто великим для реактивного керування [47].

Досвід Збройних Сил України підтвердив практичну ефективність супутникового зв'язку у бойових умовах. За даними Міноборони України та численних звітів волонтерських груп, система Starlink активно застосовувалась для підтримки командного зв'язку, а також безпосередньо для

забезпечення зв’язку з БПЛА. Вона забезпечувала передачу відео у режимі реального часу, що суттєво підвищувало ефективність коригування артилерійського вогню та виявлення цілей на великих дистанціях. В умовах активного глушіння або фізичного знищення наземної інфраструктури супутникові термінали залишалися єдиним стабільним каналом зв’язку [42]

Ще одним важливим аспектом є висока адаптивність супутникових мереж. Системи LEO можуть динамічно перенаправляти трафік між супутниками, забезпечуючи балансування навантаження і стійкість роботи мережі навіть при локальних перевантаженнях. Це робить супутниковий зв’язок масштабованим і гнучким інструментом для забезпечення комунікації великої кількості користувачів на значній території [48].

Наукові дослідження підтверджують, що супутникові системи LEO мають вищу стійкість до глушіння завдяки спрямованому передаванню сигналу та можливості частотного перестроювання. Це дозволяє зберігати зв’язок у середовищі активного застосування засобів РЕБ, де традиційні VHF/UHF-канали втрачають ефективність [46]. Крім того, одночасна робота кількох БПЛА через супутник підвищує секретність каналу, забезпечуючи динамічний розподіл ресурсів і адаптивну маршрутизацію інформації, що ускладнює перехоплення чи глушіння [49].

Таким чином, супутниковий зв’язок поєднує в собі ключові переваги: глобальне покриття, незалежність від наземної інфраструктури, високу швидкість і низьку затримку передачі даних, масштабованість, а також стійкість до впливу РЕБ. Ці характеристики роблять його незамінним у сучасних військових операціях і забезпечують ефективне функціонування систем безпілотних літальних апаратів у складних бойових умовах.

3.3 Інтеграція супутникового зв’язку в апаратне забезпечення БПЛА

Інтеграція супутникового зв’язку в БПЛА передбачає встановлення на борт наступних компонентів:

- Мініатюрного супутникового терміналу (наприклад, RockBLOCK для Iridium або Mini Starlink Kit);
- Направленої антени з автоматичним позиціюванням на супутник;
- Інтерфейсу зв’язку з бортовим комп’ютером (через Ethernet, UART або USB);
- Програмного забезпечення, що підтримує алгоритми динамічного перемикання каналів (failover), шифрування, а також зв’язок із наземною станцією.

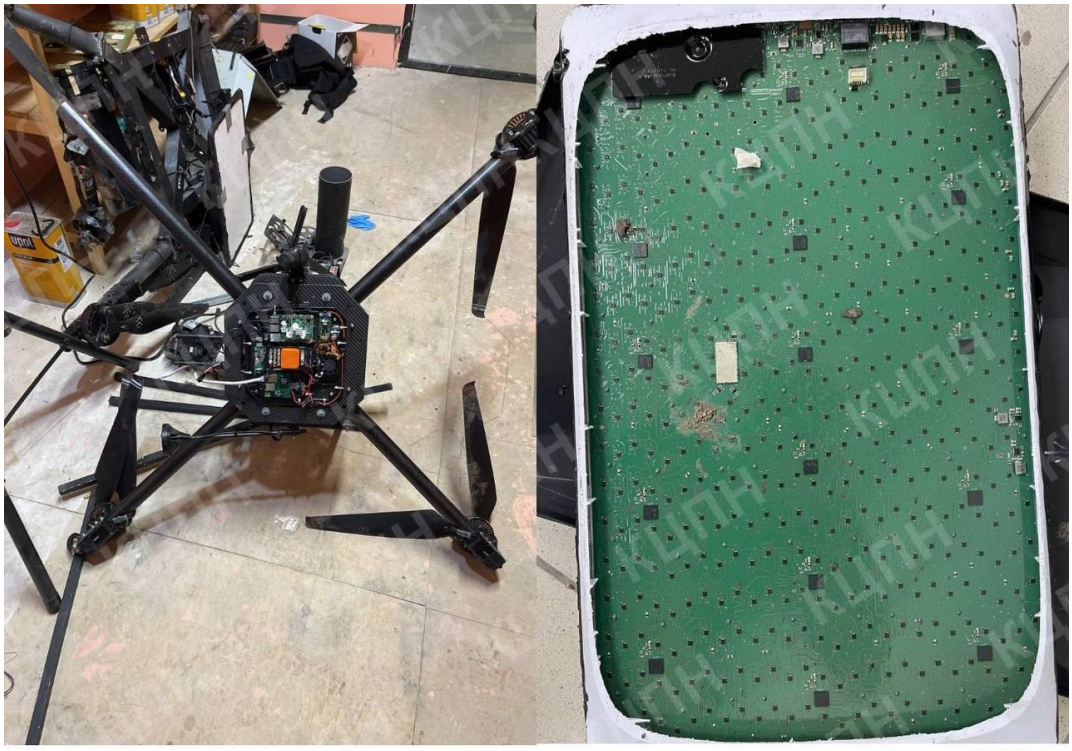

Рисунок 3.1 - Збитий дрон зі встановленою антеною Starlink, січень 2023 року [64]

У системах типу LEO (Starlink, OneWeb), супутники автоматично переміщаються над дронами і ретранслюють сигнал на найближчий наземний шлюз або безпосередньо до іншого терміналу. Дослідження Європейського оборонного агентства (EDA, 2022) показало, що подібні системи підтримують динамічну маршрутизацію між супутниками (inter-satellite links), що підвищує стійкість і дозволяє уникати перевантажених або зашумлених ділянок спектра [48].

3.4 Захисні алгоритми від РЕБ

Для забезпечення стійкості зв’язку БПЛА в умовах РЕБ застосовуються такі основні технології:

Beamforming - технологія формування вузьконаправленого променя сигналу, спрямованого безпосередньо на приймач (наприклад, супутник). Завдяки концентрації енергії в обмеженому кутовому секторі знижується ймовірність глушіння чи перехоплення сигналу. У системах Starlink beamforming реалізується за допомогою фазованих антенних решіток, які автоматично відстежують рух об’єкта та спрямовують сигнал у його бік [50].

FHSS (Frequency Hopping Spread Spectrum) - метод перестроювання частоти передачі у псевдовипадковому порядку, що значно ускладнює глушіння сигналу.

Шифрування AES-256 та вище забезпечує конфіденційність передачі, унеможливлюючи дешифрування перехоплених даних.

Аналітика загроз (Threat-Aware Routing) - адаптивне управління мережею, що автоматично перенаправляє трафік при виявленні завад чи атак. Алгоритми аналізують параметри каналу (SNR, затримки, втрати пакетів) і динамічно змінюють маршрут, наприклад, переключаючись на інший супутник або наземний шлюз. Особливо ефективно у супутникових системах

з міжсупутниковими лінками, які забезпечують багатоваріантне маршрутизування без залежності від наземної інфраструктури [50].

Алгоритм MVDR (Minimum Variance Distortionless Response) застосовується для подавлення джерел перешкод у багатоканальних приймачах, зокрема фазованих антенах. Він формує просторовий фільтр, який мінімізує потужність сигналів із небажаних напрямків, зберігаючи при цьому неспотворену форму цільового сигналу. MVDR автоматично адаптується до змін середовища, що робить його ефективним для рухомих платформ, зокрема БПЛА [50].

3.5 Практичні приклади

Інтеграція супутникового інтернету значно підвищує стійкість систем зв’язку БПЛА в умовах РЕБ. Завдяки низькій затримці, глобальному покриттю, завадостійким алгоритмам та можливості автономної маршрутизації даних, супутникові технології стають не просто альтернативою, а необхідністю у сучасному військовому середовищі.

Американська компанія Maxar у 2025 році представила систему RAPTOR, яка дозволяє БПЛА працювати без GPS, використовуючи лише супутниковий зв’язок, візуальні сенсори та 3D-карти місцевості [51]. Це рішення забезпечує збереження навігаційної функції навіть у повністю заглушеному середовищі. Аналогічно, українська компанія Sine.Engineering розробляє прототипи дронів, здатних до роботи без GPS- і GSM-зв’язку, лише з використанням супутникового каналу та оптичного корегування, що забезпечує надвисоку живучість в умовах інтенсивної радіоелектронної боротьби [52].

Також практичне підтвердження ефективності подібних рішень спостерігається під час операцій Збройних Сил України на південному напрямку. Одним із найбільш показових прикладів стало бойове застосування

модернізованих баражуючих боєприпасів, керованих виключно через супутниковий канал зв’язку. Ці апарати, побудовані на базі БПЛА «Рубака» [53], були адаптовані для умов подавлення традиційних каналів навігації та зв’язку. Завдяки оригінальній конструкції корпусу, в який вбудовано антену Starlink, дрони отримали можливість стабільного управління навіть у глибокому тилу противника.

Перевагою такого підходу стала не лише завадостійкість, а й здатність зберігати низький профіль - як фізичний, так і радіолокаційний. Навіть із мінімальною бойовою частиною ці апарати виявилися здатними критично пошкоджувати високовартісні об’єкти, такі як радіолокаційні станції, зенітно-ракетні комплекси або ворожі катери. Зазначені приклади доводять, що супутниковий інтернет не лише компенсує втрату традиційних каналів у зоні дії РЕБ, а й створює передумови для розвитку нової концепції бойового застосування БПЛА - автономних, захищених від глушіння та придатних до керування в реальному часі на будь-якій відстані.

Водночас розвиток супутникового зв’язку в сучасному конфлікті супроводжується низкою викликів. Дедалі частіше супутниковий інтернет використовується обома сторонами протистояння. Зафіксовані випадки встановлення терміналів Starlink на безпілотниках типу «Shahed-136», що свідчить про спроби Російської Федерації використовувати ті самі технології для створення віддалено керованих платформ із можливістю передачі відеопотоку або телеметрії в реальному часі [54]. Існує підозра, що такі термінали надходять до РФ через треті країни. Факт серійної інтеграції супутникових систем у російські БПЛА викликав занепокоєння на міжнародному рівні, зокрема в самій компанії SpaceX.

Показово, що противник адаптується до умов насиченого РЕБ, поступово відмовляючись від вразливих до глушіння GPS-модулів і GSM-каналів на користь нової архітектури зв’язку. За даними аналітичного звіту The Economist, останні модифікації іранських дронів Shahed, які Росія активно

використовує, здатні функціонувати без доступу до GPS, завдяки алгоритмам штучного інтелекту та вбудованим системам супутникового зв’язку:

«The newest models… are unfazed by Ukraine’s electronic warfare. This is because they no longer rely on jammable GPS, are driven by artificial intelligence, and piggy-back on Ukraine’s own internet and mobile networks» (The Economist, 2024).

(Найновіші моделі... не бояться української радіоелектронної боротьби. Це тому, що вони більше не покладаються на GPS, який можна заглушити, керуються штучним інтелектом і використовують власний інтернет і мобільні мережі України)

Цей приклад демонструє, що ефективна реалізація супутникового інтернету у ворожих БПЛА створює якісно новий рівень загрози. Вони отримують можливість проникати глибоко в тил, уникати перешкод і передавати телеметрію або відео без використання традиційних каналів, які легко подавити. У відповідь на це Збройні Сили України мають розвивати власну суверенну інфраструктуру супутникового зв’язку, орієнтовану на створення адаптивних, захищених та автономних каналів керування. Практичний досвід показує, що саме мультиканальна архітектура з автоматичним перемиканням між супутниковим та наземним зв’язком дає змогу зберігати управління БПЛА навіть в умовах повного глушіння радіоефіру. Такий підхід забезпечує не лише живучість платформи, а й оперативну перевагу на полі бою. [55]

Рисунок 3.2 - Збитий над Україною російський безпілотник «Герань-2» (Shahed), у якому був встановлений термінал Starlink. Вересень 2024 [56]

Попри очевидну загрозу, пов’язану з можливістю використання супутникового інтернету противником, деякі аналітики висловлюють сумніви щодо масштабності чи регулярності таких випадків. Зокрема, фахівці припускають, що йдеться не про масову інтеграцію Starlink у бойові платформи РФ, а радше про експериментальні або демонстраційні зразки. Один із авторів публікації, в якій було оприлюднено фото збитого дрона з терміналом Starlink, зауважив:

«Дуже дивне і сумнівне рішення, як на мене, і поки більше схоже на утилізацію трофейних українських або не працюючих на території РФ терміналів» [56].

Така оцінка підкреслює, що навіть у випадку фіксації наявності обладнання Starlink на ворожих БПЛА, це ще не обов’язково свідчить про системну модернізацію арсеналу противника. Водночас навіть поодинокі приклади успішного використання таких рішень потребують уважного аналізу та негайної реакції з боку системи оборонного планування. Українські підрозділи мають бути готовими як до реальної загрози втрати переваги в завадостійкості, так і до маніпуляцій інформаційного характеру.

За деякими даними, передача супутникових сигналів може бути перевантажена через одночасне використання мережі Starlink з обох сторін фронту, що вже фіксувалося українськими військовими. У відповідь на ці виклики в Україні розпочато створення «білого списку» авторизованих терміналів, які мають право на підключення до мережі, тоді як компанія SpaceX веде консультації з урядом США щодо централізованого блокування терміналів у разі виявлення їхнього несанкціонованого використання [57].

Таким чином, хоч супутниковий інтернет демонструє значний потенціал як засіб забезпечення стійкого каналу зв’язку для БПЛА в умовах РЕБ, його масове впровадження супроводжується як технологічними, так і безпековими загрозами. Вони вимагають не лише вдосконалення засобів шифрування та автентифікації, а й комплексного підходу до управління доступом, у тому числі на державному рівні.

3.6 Моделювання критичних сценаріїв

Моделювання критичних ситуацій включає комплексний аналіз роботи системи в умовах часткового пошкодження супутникової інфраструктури. Згідно з даними SpaceX, навіть при доступності лише 20-30% супутників, система зберігає працездатність із незначним збільшенням затримки сигналу від 45мс до 55мс, та зниженням пропускної здатності до 60-70%. Ці показники підтверджують життєздатність супутникового зв'язку як резервного каналу в екстремальних умовах.

Для проведення точного моделювання використовуються спеціалізовані програмні комплекси, такі як OPNET та NS-3, які дозволяють враховувати всі ключові параметри роботи системи. Згідно з міжнародними стандартами [58] та військовими специфікаціями [59], моделювання включає аналіз максимальної відстані зв'язку (1000-1500 км), швидкості переміщення БПЛА (100-300 м/с) та рівня перешкод (80-140 dBм).

На основі аналізу сучасних підходів сформовано практичні рекомендації щодо підвищення стійкості зв’язку в системах безпілотних літальних апаратів. Доцільно є впровадження гібридних рішень, які поєднують супутникові канали зв’язку з традиційними радіоканалами. Такий підхід дозволяє забезпечити резервування каналу в разі перешкод або втрати прямої видимості. Крім того, перспективним напрямом є використання алгоритмів машинного навчання для прогнозування втрат зв’язку та динамічного налаштування параметрів передачі. У передових військових системах БПЛА супутниковий зв’язок вже виконує роль ключового елементу інфраструктури управління, забезпечуючи стійкість комунікацій навіть в умовах активного радіоелектронного впливу.

3.7 Обмеження використання супутникового зв’язку в системах управління БПЛА

Незважаючи на очевидні переваги супутникового зв’язку, застосування цих каналів у системах БПЛА супроводжується низкою технічних, експлуатаційних та організаційних обмежень. Ці фактори обов’язково мають враховуватись під час розробки, планування й використання безпілотних апаратів, які покладаються на супутниковий інтернет як основний або резервний канал зв’язку.

Одним із найважливіших параметрів, що обмежує ефективність супутникових систем, є затримка сигналу. У системах, що використовують геостаціонарні супутники (на висоті близько 36 000 км), середня затримка однієї транзакції (RTT - round-trip time) становить 500-600 мс. Це робить управління в реальному часі майже неможливим. Хоча сучасні системи на низькій навколоземній орбіті (LEO), зокрема Starlink, OneWeb та Iridium NEXT, демонструють значно меншу затримку - у межах 30-60 мс, - цього може бути недостатньо для виконання задач із високими вимогами до швидкодії,

зокрема маневрування на низькій висоті, перехоплення цілей, або управління FPV-дронами. У подібних сценаріях навіть короткочасне збільшення затримки може спричинити втрату керованості або погіршення ситуаційної обізнаності оператора.

Ще одним важливим обмеженням є залежність якості супутникового каналу від метеорологічних умов. У системах, що використовують Ka- і Ku-діапазони, які є типовими для Starlink, OneWeb, значна втрата сигналу спостерігається під час сильного дощу, снігопаду або щільної хмарності. Це явище називається атмосферне затухання, та може призвести до тимчасового падіння швидкості передачі даних або повної втрати з’єднання. У високодинамічному середовищі бойових дій така ситуація є критичною, особливо якщо зв’язок з БПЛА здійснюється виключно через супутник і не дублюється наземними каналами.

Також необхідно враховувати енергетичні обмеження на борту БПЛА, особливо малого і середнього класу. Супутникові термінали, як правило, потребують суттєво більше енергії для стабільної роботи порівняно зі звичайними радіомодулями. Наприклад, термінал Starlink High Performance може споживати до 100 Вт у активному режимі, що вимагає додаткових джерел живлення або суттєвого скорочення тривалості польоту через підвищене енергоспоживання. Для FPV-дронів або інших малогабаритних платформ це обмеження є особливо критичним, адже енергетичний баланс системи прямо впливає на дальність та час роботи.

Крім технічних обмежень, існує низка організаційних і політичних ризиків, пов’язаних із використанням комерційних супутникових сервісів у військових цілях. У випадку із системою Starlink, яка належить приватній компанії SpaceX, можливість централізованого обмеження доступу до покриття або функціональності залишається прерогативою постачальника. У 2023 році вже мав місце інцидент, коли компанія частково заблокувала використання Starlink для керування БПЛА за межами лінії фронту через

побоювання ескалації конфлікту. Такі випадки підкреслюють, що у відсутність повного контролю над інфраструктурою зв’язку з боку держави, навіть найкраща технологія може бути раптово недоступною з політичних або етичних причин.

Окрім цього, слід згадати технічну вразливість до кіберзагроз. Незважаючи на високий рівень шифрування, супутникові термінали є потенційною мішенню для атак типу Man-in-the-Middle (MITM), спуфінгу або DDoS через наземні шлюзи. Злам наземного терміналу або втручання в маршрутизацію можуть призвести до втрати або перехоплення критично важливої інформації. Певні дослідження вказують також на можливість симуляції сигналу супутника, що у випадку недостатньої аутентифікації може дезорієнтувати приймач або перенаправити його до фальшивого джерела даних.

Ще одним фактором є маса та габарити супутникових антен і терміналів, які часто є надто великими для інтеграції у компактні платформи. Хоча сучасні розробки (Starlink Mini) вже дозволяють значно зменшити розміри обладнання, все ще залишаються виклики щодо аеродинаміки, масо-габаритних характеристик і розміщення на борту дрона без шкоди для його основних функцій.

Таким чином, попри численні переваги, супутниковий зв’язок не є універсальним рішенням. Для досягнення максимальної ефективності необхідно впроваджувати гібридні системи, які поєднують супутникові, наземні та автономні канали зв’язку. У поєднанні з адекватними алгоритмами шифрування, резервуванням енергії та автономністю навігації, супутниковий зв’язок може виконувати роль стратегічного каналу в критичних умовах, але не повинен розглядатись як єдине джерело зв’язку без альтернатив.

3.8 Висновки до розділу 3

У третьому розділі було проведено комплексний аналіз використання супутникового зв'язку як засобу для покращення стійкості та розширення можливостей безпілотних літальних апаратів в умовах радіоелектронної боротьби. На основі дослідження можна зробити наступні висновки.

Супутниковий зв'язок є ефективним рішенням для обходу наземних засобів РЕБ. Традиційні наземні канали зв'язку є вразливими до глушіння, оскільки працюють у зоні прямої дії ворожих систем. Супутникові канали, отримуючи сигнал з високого кута, дозволяють обходити зони локального подавлення, що робить їх надійним альтернативним або резервним каналом.

Низькоорбітальні (LEO) системи, зокрема Starlink, є найбільш придатними для керування БПЛА. На відміну від геостаціонарних супутників з великою затримкою сигналу (до 600 мс), LEO-системи забезпечують затримку на рівні 30-60 мс, що є прийнятним для управління апаратом у режимі реального часу. Висока пропускна здатність таких систем дозволяє передавати якісний відеопотік та великі обсяги телеметричних даних.

Сучасні супутникові системи мають вбудовані механізми захисту. Такі технології, як формування вузьконаправленого променя (Beamforming) та псевдовипадкова перебудова робочої частоти (FHSS), які реалізовані в системах типу Starlink, додатково підвищують стійкість до спроб глушіння та перехоплення.

Практичний досвід бойових дій підтвердив високу ефективність супутникового зв'язку. Термінали Starlink активно використовуються Збройними Силами України для забезпечення зв'язку з БПЛА, коригування артилерійського вогню та управління ударними дронами на великих відстанях, де інші канали недоступні.

Незважаючи на переваги, супутниковий зв'язок має суттєві обмеження. До них належать:

Вразливість до погодних умов: сильний дощ або сніг можуть викликати значне затухання сигналу в Ka- та Ku-діапазонах.

Високе енергоспоживання терміналів: це є критичним обмеженням для БПЛА малого класу з обмеженою ємністю акумуляторів.

Залежність від комерційного провайдера: можливість централізованого обмеження доступу до сервісу з боку компанії-власника створює операційні та політичні ризики.

Вразливість до специфічних атак: супутникові канали залишаються вразливими до цілеспрямованого потужного глушіння та атак типу GPS-спуфінг, що підтверджено в ході подальшого моделювання.

Таким чином, супутниковий інтернет є не універсальною панацеєю, а стратегічно важливим компонентом гібридної, багаторівневої системи зв'язку. Його доцільно використовувати як основний канал для далекобійних місій або як надійний резервний канал, що активується при подавленні наземних ліній зв'язку. Розуміння як сильних сторін, так і обмежень супутникового зв'язку є критично важливим для проєктування комплексної та по-справжньому стійкої архітектури, що розглядається в наступному розділі.

4 ОПТИМІЗАЦІЯ РАДІОСИСТЕМИ ДЛЯ БПЛА

У цьому розділі буде розроблено архітектуру системи зв’язку для безпілотного літального апарата з урахуванням особливостей бойового середовища та загроз, пов’язаних з використанням засобів радіоелектронної боротьби. В основі проектування покладено принципи стійкості до глушіння, гнучкого використання частотного ресурсу, а також можливість інтеграції технологій - FHSS, SDR та супутникового зв’язку. Проведено аналіз реальних випадків втрати управління над БПЛА внаслідок дії РЕБ та надано рекомендації щодо оптимального частотного планування. Завершальним етапом стала реалізація симуляційної моделі, яка дозволяє змоделювати поведінку БПЛА в різних сценаріях: з традиційним каналом зв’язку, із захистом FHSS, із використанням супутникового каналу, а також у незахищеному режимі. Результати симуляції дозволили порівняти ефективність кожного з підходів та сформувати висновки щодо доцільності їх застосування в умовах ведення бойових дій.

4.1 Проектування системи зв’язку

Проєктування сучасної системи радіозв’язку для БПЛА, що функціонує в умовах активної радіоелектронної боротьби, вимагає інтеграції засобів, здатних забезпечити стабільний та захищений канал керування й передачі даних. В умовах, коли противник застосовує засоби РЕБ, необхідно розробити архітектуру зв’язку, що поєднує гнучкість програмно-визначеного радіо , завадостійкість методів спектрального розширення, зокрема FHSS, резервні канали супутникового зв’язку та алгоритми динамічного реагування на перешкоди.

У загальному вигляді система зв’язку БПЛА повинна складатися з трьох функціональних підсистем:

- Передавально-приймальний комплекс на борту БПЛА;
- Наземна станція керування (GCS - Ground Control Station);
- Резервний або супутниковий канал зв’язку.

Кожна з цих підсистем повинна підтримувати такі ключові характеристики: динамічне частотне перестроювання, криптографічний захист, резервування каналів, захист від виявлення та перехоплення сигналу. На рисунку 4.1 подано принципову структурну схему проєктованої системи зв’язку.

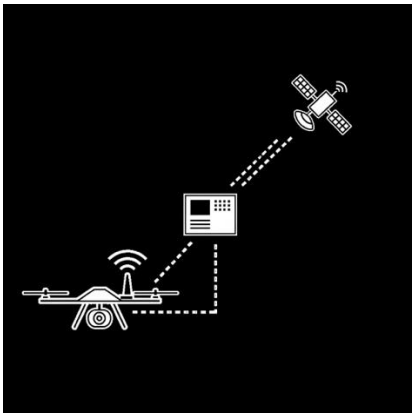

Рисунок 4.1 - Архітектура системи зв’язку

Основною вимогою до проєктованої архітектури є забезпечення функціональної живучості зв’язку при втраті основного каналу. Для цього у системі реалізовано три рівні стійкості:

Базова завадостійкість реалізована за допомогою технології FHSS, яка забезпечує частотне перестроювання сигналу з високою швидкістю та у довільному порядку, що ускладнює роботу РЕБ засобів противника.

SDR-платформа дозволяє адаптувати параметри модуляції, ширину каналу та навіть протокол роботи у реальному часі, виходячи з умов середовища. Це дає змогу, наприклад, автоматично переходити з QPSK на BPSK або зі стандартного каналу на агрегований при погіршенні умов прийому.

У разі повного подавлення FHSS-каналу в системі реалізовано автоматичне перемикання на супутниковий канал зв’язку (Starlink, Iridium або інші LEO-системи), що забезпечує глобальне покриття та високу пропускну здатність.

На борту БПЛА SDR-модуль виконує роль керованого трансивера, який взаємодіє з блоком частотного планування та криптографічного захисту. Передача керуючих команд відбувається з використанням симетричного шифрування AES-256, а розповсюдження ключів - через асиметричні алгоритми (RSA або ECC). Таким чином, забезпечується як автентифікація, так і конфіденційність управління.

Значну роль у системі відіграє модуль оцінки спектральної обстановки (Spectrum Awareness Module), розташований на стороні наземної станції. Він здійснює постійне сканування спектру на наявність активних перешкод, аналізує інтенсивність та тип завад і формує рекомендації для SDR-модуля БПЛА щодо зміни робочої частоти або перемикання на резервний канал. При цьому рішення ухвалюються з урахуванням статистичних моделей поведінки РЕБ.

Особливу увагу приділено антенному комплексу. Застосування всеспрямованої антени з широким діапазоном частот або фазованої антенної решітки дозволяє підвищити енергоозброєність каналу та зменшити ймовірність втрати зв’язку при зміні орієнтації БПЛА. Водночас вектор керування променем (beamforming) дозволяє зменшити витік сигналу та ускладнити його виявлення.

Щодо передачі телеметричних даних, система використовує окремий логічний канал, пріоритезований за критичністю. При перевантаженні каналу або спробі перехоплення відбувається зменшення частоти передачі даних, їх ущільнення та адаптація формату передачі.

У контексті архітектури також передбачено реалізацію симулятора, який дозволить моделювати роботу системи у таких сценаріях:

- нормальні умови з FHSS;
- спроба подавлення РЕБ засобами широкого діапазону;
- автоматичне перемикання на супутниковий канал при виявленні глушіння;
- вплив місцевості (ліс, місто, поле) на стабільність сигналу;
- затримка, втрати пакетів та вплив погодних умов.

Таким чином, проєктована система зв’язку забезпечує багаторівневий захист, адаптивність до умов РЕБ, гнучке управління спектром та резервування каналів, що критично важливо для застосування БПЛА в умовах сучасної війни.

Адаптація системи зв’язку до змінних умов: частотне перестроювання, навігація в спектрі та виявлення РЕБ-атак

Ефективне функціонування БПЛА в умовах активного радіоелектронного протиборства вимагає від системи зв’язку не лише стійкості до перешкод, а й здатності до адаптації в реальному часі. У цьому контексті ключовими є такі компоненти: динамічне частотне перестроювання, навігація у спектрі (spectrum navigation), розпізнавання атак радіоелектронної боротьби РЕБ та відповідне перемикання каналів передачі даних і управління.

Одним із механізмів адаптації є частотне перестроювання (frequency agility), що реалізується завдяки технології FHSS (Frequency Hopping Spread Spectrum), яка дозволяє радіомодулю швидко змінювати робочу частоту в межах заздалегідь визначеного діапазону. Змінюючи частоту з високою швидкістю та псевдовипадковим чином, система мінімізує ризик тривалого впливу завад у певному піддіапазоні. Типовими параметрами для військового застосування є швидкість перестроювання на рівні ≥ 1000 перестроювань/с з шириною смуги до 20 МГц. При цьому використовується синхронізація з наземною станцією через захищений канал із наперед погодженим псевдовипадковим кодом перестроювання (PN-генератором).

Сучасні засоби РЕБ, здатні сканувати широкий спектр частот та автоматично реагувати на активні передачі. Тож доцільно забезпечити функцію навігації у спектрі (spectrum navigation), яка передбачає постійний моніторинг спектральної обстановки, виявлення «чистих» вікон для передачі та уникнення зон активного глушіння. Реалізація цієї функції можлива за рахунок інтеграції модуля спектрального аналізу, здатного виконувати сканування з дискретністю до 1 МГц і відображати спектральну карту у реальному часі.

Розроблена система зв’язку БПЛА включає алгоритм виявлення РЕБ-атак на основі аналізу наступних ознак:

- Раптове зростання рівня фонових шумів у певному діапазоні (signal-to-noise degradation);
- Втрата синхронізації між передавачем і приймачем;
- Зменшення ймовірності правильної декодування пакетів (packet error rate > threshold);
- Наявність сигналів із нетиповими параметрами (наприклад, широкосмугове шумоподібне випромінювання).

У разі виявлення таких ознак активується адаптивний механізм ухилення від перешкод (jam avoidance), який виконує такі дії:

1. Здійснює повторне сканування спектру для виявлення вільних піддіапазонів.
2. Перебудовує частоту SDR-модуля на нове значення з урахуванням карти завад.
3. У разі повного подавлення у всьому робочому діапазоні - автоматично перемикається на резервний канал зв’язку (супутниковий або вузькосмуговий цифровий канал нижчої частоти, наприклад 433 МГц).

Важливим елементом архітектури є система оцінювання достовірності РЕБ-атаки. Зокрема, при фіксації перешкоди сигнал класифікується як:

- тимчасова перешкода

- цілеспрямоване
- активне сканування (частотна зміна за визначеним алгоритмом).

Ключовим інструментом, який дозволяє реалізувати всі зазначені функції, є програмно-визначене радіо (SDR). На відміну від традиційних систем, SDR забезпечує гнучке перебудування параметрів модуляції, частотного діапазону, протоколу, ширини смуги пропускання, рівня потужності передавання тощо - відповідно до команд вбудованого адаптивного модуля. На практиці це дозволяє, наприклад, у відповідь на РЕБ-атаку перейти з QAM64 на BPSK, знизити швидкість передачі, зменшити спектральну помітність сигналу, або активувати супутникову резервну систему.

Реалізація динамічної адаптації до умов радіоелектронного протиборства дозволяє суттєво підвищити живучість каналу зв’язку, зменшити ймовірність втрати управління над БПЛА та забезпечити доставку телеметричних даних у найскладніших умовах електромагнітного середовища.

4.2 Оцінка можливих вразливостей

Надійність систем зв’язку безпілотних літальних апаратів залежить не тільки від якості каналів передавання, а також від здатності протистояти спробам перехоплення, глушіння, підміни сигналів або навігаційного обману. В умовах бойового застосування, особливо в середовищі насиченому засобами радіоелектронної боротьби , система зв’язку БПЛА виявляється вразливою до низки цілеспрямованих атак.

По-перше, основною вразливістю є використання фіксованих частот передачі даних, особливо у випадку аналогових або простих цифрових систем управління. У таких системах радіомодем працює в межах сталого діапазону (наприклад, 868-928 МГц або 2.4 ГГц), що дає можливість РЕБ-комплексам

виявити, проаналізувати та з високою точністю придушити сигнал. У випадках, коли частотне перестроювання (FHSS) не реалізоване або не адаптоване під конкретні умови середовища, система втрачає живучість. Особливо небезпечно це в умовах активного сканування спектру противником.

Другою критичною вразливістю є передача незашифрованих або слабо захищених телеметричних даних. У багатьох випадках, особливо в недорогих або комерційно модифікованих БПЛА, передача GPS-координат, статусу систем та команд управління здійснюється у відкритому вигляді. Це дає можливість противнику здійснювати перехоплення каналів зв’язку, аналізувати логіку польоту та навіть виводити апарат із ладу шляхом надсилання шкідливих команд (takeover attack). Використання простих протоколів по-типу MAVLink без шифрування AES-256 підвищує ризики.

Окрему групу вразливостей становлять навігаційні канали. У більшості БПЛА орієнтація в просторі здійснюється за допомогою сигналів GPS, GLONASS або Galileo. Проте сигнали супутникової навігації є слабкими та можуть бути приглушені або підмінені (спуфінг). Такі атаки дозволяють противнику «переконати» БПЛА, що він знаходиться в іншому місці, змінити його маршру.

Ще одним вектором вразливості є архітектура системи зв’язку. Якщо БПЛА використовує лише один канал управління (наприклад, традиційний радіоканал), втрата цього каналу призводить до негайного втрачання контролю. У таких умовах надзвичайно важливою стає наявність резервних каналів - супутникових, 3G/4G, або попередньо запрограмованих автономних сценаріїв (failsafe).

До технічних вразливостей також належать:

- Відсутність адаптивного регулювання потужності передавача: чим сильніший сигнал - тим легше його виявити.

- Використання стандартних або незахищених протоколів передачі відео (наприклад, аналоговий FPV або Wi-Fi).
- Прямолінійна структура польоту, яка дозволяє прогнозувати траєкторію руху апарата.

Таким чином, оцінка вразливостей систем зв’язку БПЛА демонструє необхідність створення багаторівнево захищеної архітектури управління - з використанням криптографічних протоколів, адаптивного перестроювання частот, резервних каналів і вбудованої логіки автономного ухилення від РЕБ. Виявлення слабких місць на етапі проектування є критичним кроком у забезпеченні живучості та ефективності безпілотних платформ в умовах сучасного поля бою.

4.2.1 Аналіз реальних бойових випадків перехоплення

В умовах сучасної війни в системи радіоелектронної боротьби стали важливим елементом протидії безпілотним літальним апаратам, зокрема дронам-камікадзе типу «Shahed-136», він же «Герань-2», які активно використовує Російська Федерація. В останні роки було зафіксовано безліч вдалих випадків нейтралізації дронів без застосування кінетичних засобів ураження, шляхом використання технологій радіопридушення та навігаційного спуфінгу.

Одним із найбільш показових прикладів стало використання національної системи спуфінгу під назвою «Покрова». За даними американського видання Forbes, ця система є високотехнологічним інструментом, здатним створювати фальшиві сигнали GPS і GLONASS, збиваючи з пантелику навігаційні системи ворожих дронів. Її ефективність особливо проявилася проти баражуючих боєприпасів Shahed, навіть у версіях, що оснащені навігаційним блоком «Комета-М» з підвищеною стійкістю до перешкод. Як зазначає експерт британського аналітичного центру RUSI Томас

Вітінгтон: «Спуфінг може бути способом обійти контрзаходи, як-от стійкі до перешкод приймачі» [60].

Підтвердження ефективності цієї тактики міститься у публікації журналу Newsweek, в якій з посиланням на французьке видання Le Monde повідомляється, що українські сили здатні змінювати координати дронів типу Shahed, змушуючи їх розвертатися в бік Росії або Білорусі. Зокрема, в ніч на 9 квітня 2024 року Повітряні сили ЗСУ заявили, що з 188 дронів понад 90 були збиті з курсу електронною боротьбою, а 5 з них перетнули білоруський повітряний простір [61].

Попри високу технологічність дронів, оснащених резервною інерціальною навігацією, українські інженери виявили вразливості в їхніх навігаційних системах, що дозволило ефективно застосовувати спуфінг. Про це офіційно заявляв Іван Павленко, начальник Головного управління РЕБ та кібербезпеки Генерального штабу ЗСУ [61].

Ще один реальний наслідок широкомасштабного застосування спуфінгу - побічний вплив на цивільну інфраструктуру. Під час масованих атак дронів у жовтні 2023 року жителі Києва почали скаржитись на некоректну роботу GPS-навігації на смартфонах: деякі пристрої показували місцезнаходження у Брянську, Курську або Москві. За роз’ясненням Генерального штабу ЗСУ, такі збої є результатом роботи РЕБ-систем, які створюють фальшиві супутникові сигнали [62].

Журналісти видання The Record повідомляють про безліч випадків, коли українці запізнювались на роботу, пропускали зустрічі або виявляли зміну часового поясу на телефонах. Один із користувачів соцмереж написав: «Друзі, якщо не хочете так облажатись, як я, - вимикайте автоматичну зміну часу. Бо ви можете проспати, думаючи, що запізнились, хоча насправді ваш телефон на курському часі, блін» [62].

Таким чином, реальні бойові події підтверджують, що:

- РЕБ-системи ефективно нейтралізують високотехнологічні БПЛА шляхом спуфінгу
- Системи дозволяють не тільки виводити дрони з ладу, а й спрямовувати їх назад до противника
- Спуфінг має побічні ефекти для цивільного населення, що потребує обережного й контрольованого застосування.

4.2.2 Вразливості командно-телеметричних каналів

Сучасні БПЛА малого та середнього класу демонструють високу вразливість до засобів РЕБ через використання незахищених ISM-діапазонів, слабке або відсутнє шифрування та фіксовані частоти зв’язку. Протокол MAVLink, що широко застосовується у цивільних дронах, не підтримує шифрування, що дозволяє перехоплювати телеметрію та реалізовувати атаки типу takeover. Використання фіксованих частот без адаптації сигналу дає змогу легко виявити та приглушити канал зв’язку. Додатковою загрозою є атаки типу spoofing на GPS, що особливо ефективні через відсутність інерціальної навігації у більшості моделей. Типові навігаційні модулі (наприклад, u-blox) не мають механізмів перевірки координат, що робить апарат вразливим до фальсифікації даних.

Більшість БПЛА покладаються на єдиний канал зв’язку, і його втрата через РЕБ призводить до втрати управління. Резервні канали, зокрема на базі LTE або супутникових мереж, зазвичай відсутні. Аналогові FPV-системи легко перехоплюються, а цифрові на Wi-Fi або LoRa - уразливі через слабке шифрування та передбачувану структуру пакетів. У серійних платформах рідко застосовуються технології FHSS, DSSS, SDR або агрегація каналів, що суттєво знижує їхню стійкість до РЕБ.

Аналіз трофейних дронів, зокрема «Shahed-136», показує їхню чутливість до GPS-spoofing навіть при наявності інерціальної навігації. Багато

платформ передають координати у відкритому вигляді, що спрощує їх виявлення та перехоплення. Тому забезпечення стійкості до РЕБ потребує комплексного підходу: впровадження сучасної криптографії, динамічного частотного перестроювання, SDR, резервної навігації та мультиканальної передачі даних.

Таблиця 4.1 - Типові вразливості систем зв’язку та навігації БПЛА

Компонент системи	Тип вразливості	Причина вразливості	Потенційні наслідки
Командно-телеметричний канал	Відсутність шифрування, передача відкритим текстом	Використання MAVLink без захисту, LoRa без AES	Перехоплення управління, перехоплення телеметрії
Частотна схема	Робота на фіксованій частоті	Відсутність FHSS / DSSS	Легке виявлення й подавлення
GNSS-приймач	Уразливість до спуфінгу та джамінгу	Відсутність перевірки достовірності координат	Втрата маршруту, дезорієнтація апарату
Відеопередача	Відкритий аналоговий сигнал або незахищений Wi-Fi	Відсутність шифрування або захисту доступу	Перехоплення відео, виявлення місця оператора
Апаратна архітектура	Один канал управління без резерву	Відсутність супутникового або LTE-резервного каналу	Повна втрата керування при глушінні
Навігаційна система	Відсутність інерціального дублювання	Орієнтація лише на GNSS	Втрата координат у зоні РЕБ
Антенна система	Ненаправлені антени або без адаптації	Нестійкість до спрямованих перешкод	Локальне подавлення сигналу
Протоколи обміну	Відсутність автентифікації пакетів	Спрощена реалізація протоколів	Можливість введення хибних команд, takeover

Як видно з Таблиці, більшість вразливостей пов’язана не стільки з наявністю ворожих засобів РЕБ, скільки з відсутністю сучасної архітектури захисту в самих БПЛА. Це підтверджує потребу в проектуванні гнучких, адаптивних і захищених систем зв’язку з використанням SDR, динамічного частотного планування та криптографічного захисту.

4.3 Моделювання стійкості зв’язку БПЛА в умовах РЕБ

Мета даного дослідження полягає у перевірці ефективності розробленої архітектури зв’язку безпілотного літального апарата (БПЛА) в умовах радіоелектронної протидії. Зокрема, аналізується здатність системи підтримувати стабільний канал керування та передачі даних у разі впливу активних засобів радіоелектронної боротьби (РЕБ). Оцінка стійкості здійснюється шляхом комп’ютерного моделювання сценаріїв польоту дрона із застосуванням різних підходів до захисту каналу зв’язку.

Інструментарій моделювання. Для реалізації моделювання було використано спеціалізоване програмне середовище Python із бібліотеками matplotlib, numpy, random і sciру, а також віртуальний простір для імітації сценаріїв польоту, розроблений автором. У моделі реалізовано два головні суб’єкти: БПЛА та система РЕБ, що динамічно реагує на виявлення сигналів управління. Параметри симуляції налаштовано для відображення реалістичних умов електромагнітного середовища: затухання сигналу, розсіювання, багатопроменеве поширення та вплив рельєфу.

Для відображення впливу середовища враховано три типи місцевості:

- відкрите поле, яке характеризується найменшими втратами сигналу;
- лісова ділянка, де спостерігається поглинання та розсіювання радіохвиль;
- міська забудова, яка спричиняє багатопроменеве поширення та перешкоди через відбиття.

Модель РЕБ-системи передбачає:

• широкий діапазон сканування від 0 до 6000 МГц з частотою дискретизації 1 МГц;

• здатність фокусуватися на ±50 МГц навколо активної частоти дрона після виявлення;

• реалізацію двох режимів впливу: спрямоване глушіння (на конкретну частоту) та широкосмугове подавлення (у межах широкого діапазону).

Сценарій 1. БПЛА з незахищеним каналом зв’язку

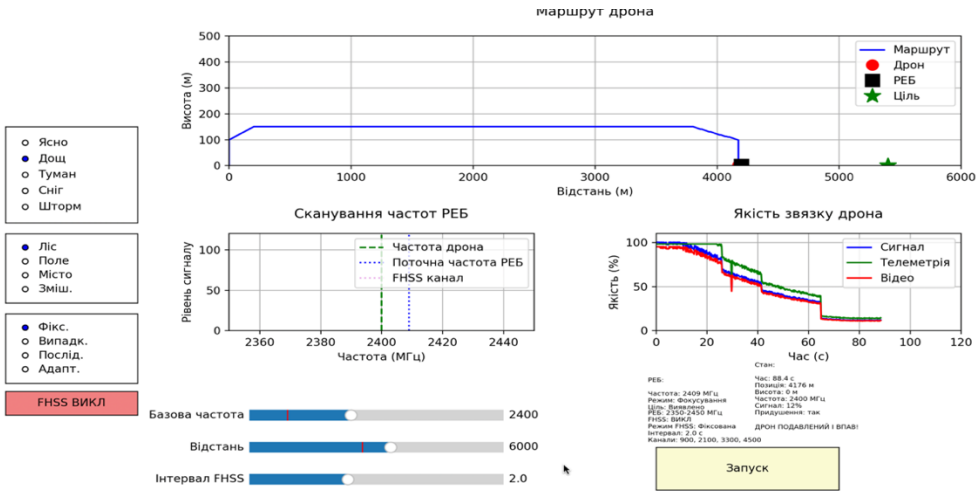

Рисунок 4.2 - Симуляція польоту БПЛА в умовах радіоелектронної боротьби (ППРЧ вимкнено)

Для симуляції польоту БПЛА з незахищеним каналом були задані наступні умови: дрон стартував до цілі на відстані 5400 метрів, а ворожа система РЕБ знаходилася на землі на позначці 4200 метрів. Зв'язок відбувався на одній фіксованій частоті 2400 МГц без використання технології перестрибування частот (FHSS). Для чистоти експерименту були обрані сприятливі умови: ясна погода та відкрита місцевість ("Поле").

Хід симуляції розгортався наступним чином:

1. Початковий етап: БПЛА успішно злетів, набрав висоту близько 150 метрів і попрямував до цілі. На цьому етапі якість сигналу, телеметрії та відео трималася на рівні, близькому до 100%.
2. Зближення та погіршення зв'язку: Приблизно на 20-30 секунді польоту, на відстані 1000-1500 метрів, якість зв'язку почала поступово знижуватися. Це було пов'язано як зі збільшенням відстані до станції керування, так і з початком аналізу спектра системою РЕБ.
3. Активна протидія РЕБ: Система РЕБ успішно виявила робочу частоту дрона (2400 МГц) і сфокусувала на ній своє подавлення.
4. Критична втрата зв'язку та падіння: Коли БПЛА наблизився до позначки 4000 метрів (на 60-70 секунді польоту), він увійшов у зону ефективного ураження РЕБ. Це спричинило різке, майже вертикальне падіння якості всіх каналів зв'язку до значень 0-10%.

Результат та висновки:

Внаслідок ефективного подавлення незахищеного каналу, БПЛА повністю втратив керування і впав, не досягнувши цілі, що було підтверджено даними симуляції: "Стан: ДРОН ПОДАВЛЕНИЙ І ВПАВ!".

Цей сценарій наочно продемонстрував, що канал зв'язку на одній фіксованій частоті є надзвичайно вразливим. Система РЕБ змогла легко виявити та подавити сигнал, що призвело до провалу місії, навіть попри ідеальні погодні умови.

Сценарій 2. БПЛА з FHSS (Frequency Hopping Spread Spectrum)

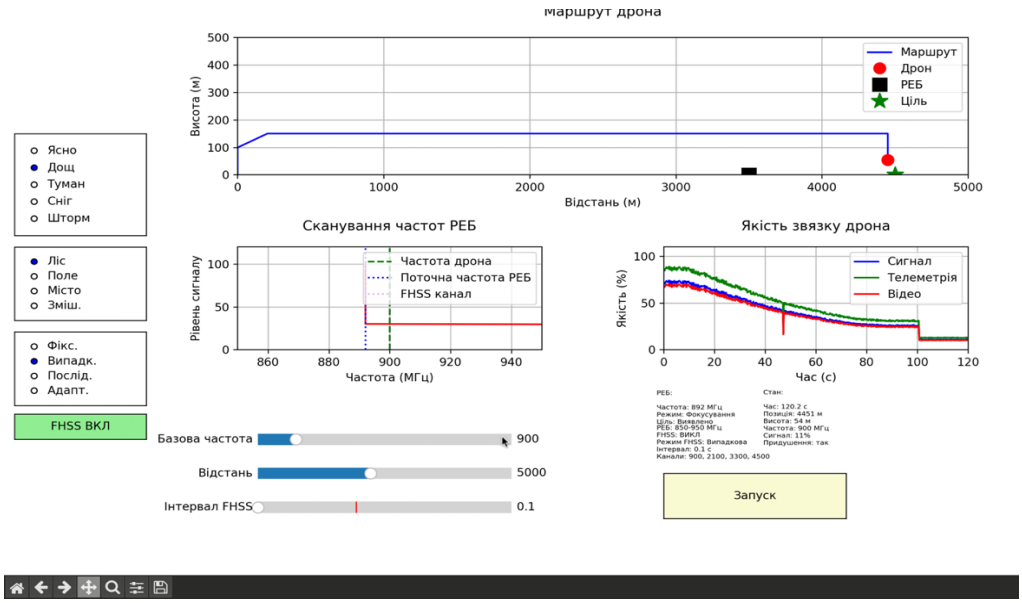

Рисунок 4.3 - Результати симуляції протидії РЕБ БПЛА з увімкненою технологією ППРЧ (FHSS)

Для симуляції польоту БПЛА з використанням технології перестрибування частот (ППРЧ) були задані наступні умови: канал зв’язку працював у режимі FHSS з активованою функцією “FHSS ВКЛ” та випадковим вибором частот (режим «Випадк.»). Стрибки відбувалися з високою частотою - кожні 0.1 секунди, що забезпечувало динамічну зміну каналів між 900, 2100, 3300 та 4500 МГц. Водночас маршрут польоту передбачав досягнення цілі на відстані 4500 метрів, а ворожа система РЕБ була розміщена на позначці 3500 метрів. Умови були навмисно ускладнені: тип місцевості - «Ліс», а погодні умови - «Дощ», що мало додатковий вплив на поширення сигналу.

Хід симуляції розгортався наступним чином:

1. Початковий етап: БПЛА успішно злетів, набрав висоту близько 150 метрів і почав рух до цілі. Незважаючи на несприятливі умови середовища, якість сигналу на перших етапах залишалась на високому

рівні, хоча поступово знижувалась через погіршене радіохвильове поширення у дощовому лісі.

2. Аналіз та реакція РЕБ: Система радіоелектронної боротьби виявила активність БПЛА, незважаючи на швидке перемикання частот. Аналіз графіку «Сканування частот РЕБ» засвідчив, що РЕБ сфокусувалася на діапазоні 850-950 МГц, виявивши один із використовуваних каналів - 900 МГц. На частоті 892 МГц було активовано інтенсивне подавлення, що призвело до істотного зниження якості зв’язку.
3. Погіршення зв’язку та спроби адаптації: Приблизно на 100-120 секунді польоту спостерігалося критичне зниження якості зв’язку - сигнали телеметрії та відео впали до рівня 10-20%. Хоча ППРЧ мала забезпечити перехід на інші частоти (2100, 3300, 4500 МГц), вони, ймовірно, мали ще гірші умови передачі через ослаблення сигналу на великій відстані та у складному середовищі. Існує також ймовірність того, що РЕБ розширила діапазон сканування для охоплення інших частот.
4. Критична фаза та аварія: На позначці 4450 метрів (майже досягнута ціль), БПЛА раптово зупинився - його швидкість знизилась до нуля, висота впала, а зв’язок остаточно зник. Статус системи зафіксував: «ДРОН ПОДАВЛЕНИЙ І ВПАВ!». Це свідчить про повну втрату керування попри активну технологію ППРЧ.

Результати та висновки: Проведена симуляція показала, що навіть за наявності потужного засобу захисту - ППРЧ з високою частотою перестрибування - дрон залишається вразливим у складних середовищах та при наявності адаптивної системи РЕБ. Особливо уразливими є ті канали, які використовуються частіше через кращі характеристики поширення (наприклад, 900 МГц), що автоматично робить їх пріоритетною мішенню для засобів подавлення.

Аналіз обмежень: Обрані частоти ППРЧ були надто широко рознесені по спектру. Це могло призвести до значного зниження ефективності зв’язку на

високочастотних каналах через більші втрати при поширенні та нестабільну роботу радіообладнання на таких частотах. Внаслідок цього система частіше використовувала нижчі частоти, що спростило роботу РЕБ.

Рекомендації: Для підвищення стійкості до РЕБ доцільно використовувати тісніше згруповані частоти у межах одного ефективного діапазону, вдосконалені алгоритми перестрибування (наприклад, на основі псевдовипадкових послідовностей або адаптивного вибору частот), а також додаткові заходи - контроль потужності передавача, спрямовані антени та модулі ШІ для оцінки якості каналів у реальному часі.

Вплив глушіння супутникового зв'язку на БПЛА

Використання супутникових каналів зв’язку (SatCom) для керування безпілотними літальними апаратами (БПЛА) суттєво розширює їхню зону дії, знімаючи обмеження, пов’язані з прямою видимістю до наземної станції управління. Це особливо актуально для розвідувальних і ударних платформ, що діють на стратегічних відстанях. Проте в умовах сучасного електронного протиборства супутникові канали залишаються вразливими до навмисного перешкодження, зокрема до активного глушіння та спуфінгу сигналів супутникової навігації (GPS). У даному підрозділі розглянуто результати моделювання таких атак за допомогою програмної симуляції.

Сценарій 3.1: Вплив активного глушіння супутникового каналу зв’язку на функціонування БПЛА

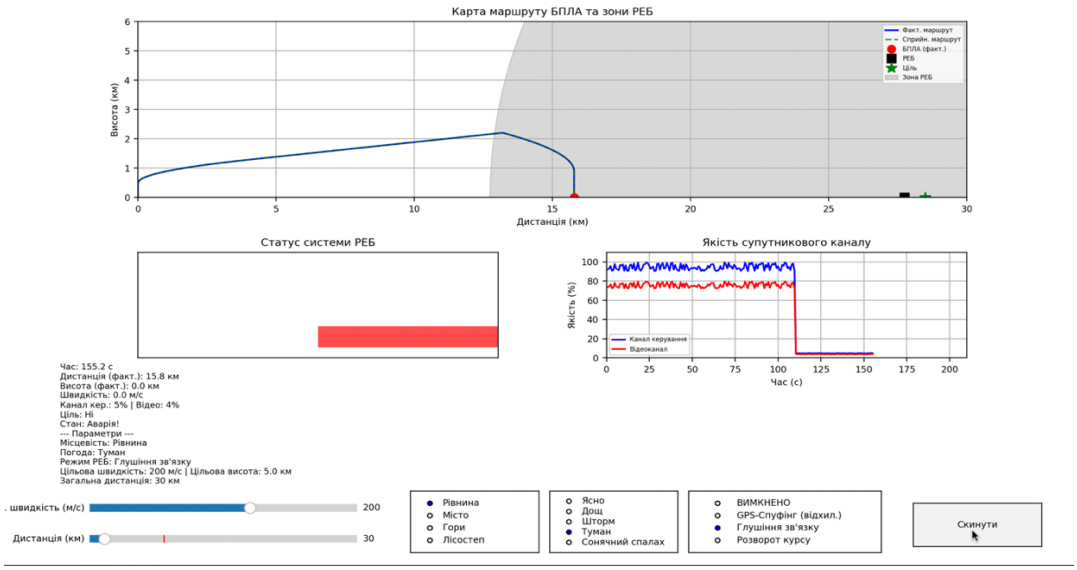

Рисунок 4.4 — Результати симуляції глушіння супутникового каналу зв’язку БПЛА системою РЕБ

- Тип каналу зв’язку БПЛА: супутниковий (SatCom).
- Тип місцевості: рівнина; погодні умови: туман.
- Маршрут БПЛА: політ до заданої цілі на відстані 27 км.
- Параметри польоту: швидкість - 200 м/с, висота - 5,0 км.
- Розміщення системи РЕБ: на відстані 26 км від точки старту БПЛА.
- Режим РЕБ: активне глушіння супутникового зв’язку.

Етапи розвитку подій у симуляції:

1. Початковий етап польоту.

БПЛА здійснює штатний зліт, набір висоти та переходить до горизонтального польоту з заданою швидкістю у напрямку цілі. Протягом перших 100 секунд спостерігається стабільна якість як каналу керування, так і відеопотоку через супутниковий зв’язок. На графіках видно високу інтенсивність сигналу в обох каналах.

2. Входження в зону дії засобів РЕБ.

Починаючи з 100-110 секунди (на дистанції 13-15 км від старту), БПЛА входить у зону ефективного покриття активної системи радіоелектронної боротьби, що веде цілеспрямоване глушіння супутникових частот. Зона дії РЕБ охоплює висотний діапазон до 7 км.

3. Критична втрата зв’язку.

На графіку “Якість супутникового каналу” фіксується різке зниження сигналу до нульових значень як у каналі керування, так і у відеопотоці. У цей самий момент на індикаторі “Активність РЕБ” видно інтенсивну смугу червоного кольору, що свідчить про максимальну потужність випромінювання перешкод.

4. Втрата керування та аварійне завершення польоту.

Через повну втрату зв’язку із наземним пунктом управління система автономного стабілізування не здатна відновити траєкторію. Відповідно до даних симуляції, БПЛА стрімко знижується. Траєкторія обривається на відмітці 155,2 секунди польоту при висоті 0 км. Фінальна координата апарата - 15,8 км від точки старту. Статус місії визначено як “Аварія!”.

Результати симуляції демонструють високу ефективність активного глушіння супутникових каналів управління БПЛА. Навіть у випадку польоту на значній висоті (5 км) з використанням SatCom, потужне вузькоспрямоване перешкодження може призвести до повної втрати контролю над апаратом. Виявлено, що ключовими факторами успішної атаки є потужність випромінювання, ширина смуги подавлення та точність спрямування антени РЕБ. Таким чином, для забезпечення надійності SatCom-каналів у військових БПЛА доцільно впроваджувати адаптивні протидії, зокрема перехід на резервні частоти, автоматичне перемикання на альтернативні канали, шифрування протоколів та використання інерційних систем навігації, здатних продовжити політ у разі втрати зовнішнього керування.

Сценарій 3.1: Вплив GPS-спуфінгу на БПЛА з супутниковим каналом зв’язку

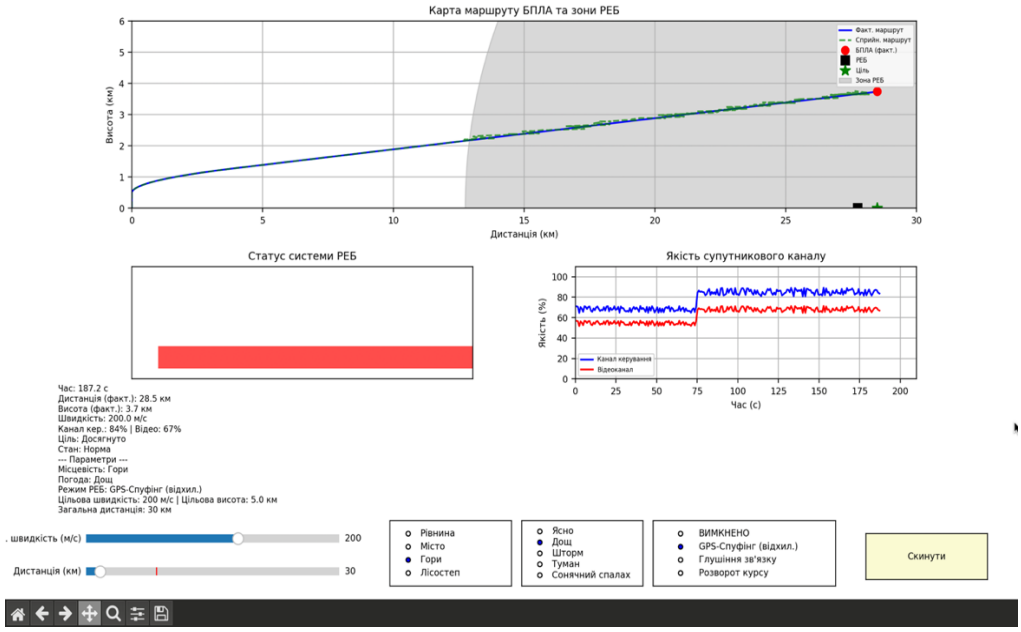

Рисунок 4.5 — Результати симуляції впливу GPS-спуфінгу на навігацію БПЛА із супутниковим каналом

Умови симуляції

- Маршрут БПЛА: Ціль розташована на відстані 28 км. Система РЕБ активується на 27 км.
- Тип зв’язку: Супутниковий канал керування та передачі відео.
- Середовище: Гірська місцевість, погодні умови - дощ. Це зумовлює потенційне зниження якості сигналу через мультипутінг та ослаблення сигналу внаслідок атмосферного поглинання.
- Система РЕБ: Активний режим «GPS-спуфінг (відхиляючий тип)».
- Параметри польоту: Швидкість - 200 м/с, висота - 5,0 км.

Динаміка впливу засобів РЕБ та аналіз результатів симуляції

1. Початковий етап польоту:

БПЛА стартує, виконує набір висоти та прямує до цілі за заданим маршрутом. Незважаючи на несприятливі умови (гори та опади), якість

супутникового зв’язку залишається у межах 60-80% - допустимий рівень для стабільного керування та телеметрії.

2. Активація спуфінгу при входженні в зону РЕБ:

При наближенні БПЛА до 27 км система РЕБ активує спуфінг. На карті маршруту відображено фактичну (синя лінія) та сприйняту (зелена пунктирна) траєкторії. Під впливом спуфінгу дрон починає зміщувати курс, орієнтуючись на фальсифіковані координати GPS.

3. Аналіз впливу на зв’язок:

На відміну від глушіння, GPS-спуфінг не впливає безпосередньо на рівень сигналу або якість супутникового зв’язку. Графік «Якість супутникового каналу» демонструє лише незначні флуктуації, зумовлені географічними та погодними факторами, а не самим спуфінгом. У той же час, графік «Статус системи РЕБ» відображає помірну активність, характерну для менш енергомісткого режиму GPS-атаки.

4. Поведінка БПЛА та результат місії:

Унаслідок навмисного спотворення навігаційних даних БПЛА відхиляється від реального маршруту. Оскільки навігаційна підсистема апарата повністю покладається на GPS, апарат не здатен виявити спотворення координат. У фінальній точці симуляції дрон «вважає», що прибув у точку призначення, хоча фактичне розташування від неї суттєво відрізняється.

Висновки

GPS-спуфінг є прикладом асиметричної електронної атаки, що не потребує потужного сигналу, але здатна критично дезорієнтувати БПЛА. На відміну від традиційного глушіння, спуфінг не викликає безпосередньої втрати зв’язку або аварії, але чинить прихований вплив, змушуючи систему навігації дрона приймати хибні координати як достовірні.

Таким чином, навіть при наявності надійного супутникового каналу зв’язку, відсутність альтернативної або резервної навігації призводить до критичних помилок виконання місій. Це підкреслює необхідність інтеграції

засобів виявлення та протидії спуфінгу в сучасні платформи БПЛА, зокрема для бойових дронів, що діють у складних умовах електронної протидії.

4.4 Висновки до розділу 4

У четвертому розділі було розроблено та проаналізовано оптимізовану архітектуру системи радіозв'язку для БПЛА, призначену для функціонування в умовах інтенсивної радіоелектронної боротьби. На основі проведеного проектування, аналізу вразливостей та комп'ютерного моделювання сформульовано наступні висновки.

Розроблено гібридну архітектуру системи зв'язку. Запропонована система базується на трьох рівнях стійкості: базовий захист за допомогою технології псевдовипадкової перебудови робочої частоти (ППРЧ), адаптивне управління параметрами каналу на основі програмно-визначеного радіо (SDR) та використання резервного супутникового каналу зв'язку для випадків повного подавлення наземних радіоканалів. Ця багаторівнева структура забезпечує функціональну живучість системи при різних сценаріях впливу засобів РЕБ.

Результати моделювання підтвердили ефективність запропонованих рішень та виявили їхні обмеження.

1. Сценарій з незахищеним каналом продемонстрував, що БПЛА на фіксованій частоті зазнає гарантованого подавлення та втрати керування ще на підльоті до зони дії РЕБ, навіть за ідеальних умов.
2. Сценарій з використанням ППРЧ (FHSS) значно підвищив стійкість БПЛА, дозволивши йому наблизитися до цілі. Однак моделювання також показало, що за умов складного рельєфу («Ліс») та адаптивної роботи РЕБ, яка фокусується на найбільш ефективних частотах діапазону, канал все одно може бути подавлений.
3. Моделювання атак на супутниковий канал виявило два ключові аспекти: по-перше, потужне спрямоване глушіння здатне повністю розірвати

зв'язок і призвести до аварії апарата. По-друге, GPS-спуфінг є «тихою» атакою, яка не впливає на якість каналу зв'язку, але призводить до повного провалу місії через дезорієнтацію апарата, який вважає, що досяг цілі, хоча насправді знаходиться далеко від неї.

Обґрунтовано необхідність комплексного підходу до захисту. Жодна окрема технологія не є панацеєю. Ефективний захист БПЛА досягається лише за умови інтеграції кількох механізмів: криптографічного захисту, динамічного частотного перестроювання, використання резервних каналів зв'язку (зокрема супутникових) та наявності альтернативних систем навігації (наприклад, інерціальних), здатних протистояти спуфінгу. Симуляційне моделювання підтвердило, що саме такий гібридний підхід дозволяє протидіяти різним типам загроз РЕБ та забезпечувати максимальну живучість БПЛА на сучасному полі бою

ВИСНОВКИ

У даній дипломній роботі було проведено комплексне дослідження систем радіозв’язку для безпілотних літальних апаратів (БПЛА) з метою їх оптимізації для забезпечення надійної передачі даних в умовах активної радіоелектронної боротьби (РЕБ). На основі аналізу теоретичних засад, сучасних технологій та результатів симуляційного моделювання сформульовано наступні висновки.

Основні результати дослідження:

Проаналізовано ключові компоненти та вразливості систем радіозв’язку БПЛА. Детально розглянуто структуру БПЛА, фізичні властивості радіохвиль та їх поширення, вплив середовища та місцевості, а також роль антенних систем. Виявлено, що незахищені канали зв'язку, особливо ті, що працюють на фіксованих частотах, є надзвичайно вразливими до виявлення та подавлення засобами РЕБ. Навіть за сприятливих умов поширення сигналу, РЕБ здатна ефективно нейтралізувати такі БПЛА.

Досліджено сучасні методи захисту радіозв’язку БПЛА. Проаналізовано криптографічні методи (симетричні, як AES, та асиметричні, як RSA та ECC) для забезпечення конфіденційності, цілісності та автентичності даних. Розглянуто ефективність технології розширення спектру з перестрибуванням частот (FHSS) як засобу протидії глушінню, а також перспективи інтелектуального управління частотами та програмно-визначеного радіо (SDR) для динамічної адаптації до умов РЕБ.

Проведено симуляційне моделювання впливу РЕБ на БПЛА з різними типами каналів зв’язку.

Визначено ключові фактори, що впливають на стійкість зв’язку БПЛА: До них належать тип каналу зв'язку (фіксована частота, ППРЧ, супутниковий), наявність та ефективність криптографічного захисту, адаптивність системи до змін радіоелектронної обстановки, характеристики

засобів РЕБ противника, а також умови навколишнього середовища (рельєф, погода).

Практичні рекомендації:

На основі проведеного дослідження сформульовано наступні практичні рекомендації для підвищення стійкості систем радіозв’язку БПЛА в умовах РЕБ:

Комплексний підхід до захисту: Необхідно впроваджувати багаторівневу систему захисту, що поєднує криптографічні методи (AES-256 для шифрування даних та ECC для обміну ключами), технології розширення спектру (FHSS, DSSS), адаптивне управління частотами та потужністю сигналу.

Оптимізація параметрів ППРЧ: При використанні FHSS слід обирати достатню кількість каналів в оптимальному робочому діапазоні, використовувати непередбачувані алгоритми стрибків та адаптувати інтервал стрибків до поточної радіоелектронної обстановки. Уникати використання дуже широко рознесених каналів, які можуть мати суттєво різні характеристики поширення.

Впровадження програмно-визначеного радіо (SDR): Технології SDR дозволяють створювати гнучкі та адаптивні системи зв’язку, здатні динамічно змінювати свої параметри (частоту, модуляцію, протокол) у відповідь на виявлені загрози РЕБ.

Використання резервних каналів зв’язку: Інтеграція супутникових каналів (наприклад, Starlink, Iridium) як резервних або навіть основних для операцій на великих відстанях може значно підвищити живучість БПЛА в умовах подавлення традиційних радіоканалів. Необхідно враховувати обмеження супутникового зв'язку, такі як затримка сигналу, енергоспоживання та залежність від метеоумов.

Застосування спрямованих антен та технології Beamforming: Це дозволяє концентрувати енергію сигналу, збільшуючи дальність та якість

зв'язку, а також зменшуючи ймовірність перехоплення та подавлення сигналу з боку противника.

Інтеграція інерціальних навігаційних систем (ІНС): Для протидії GPS-спуфінгу та тимчасовій втраті GNSS-сигналу необхідно використовувати ІНС з корекцією за іншими даними (наприклад, оптичною або радіолокаційною одометрією) для забезпечення автономної навігації.

Моніторинг радіоелектронної обстановки: Оснащення наземних станцій керування та, можливо, самих БПЛА засобами спектрального аналізу для виявлення активності РЕБ, ідентифікації типів завад та автоматичної адаптації параметрів зв’язку.

Напрями подальших досліджень:

Незважаючи на значний обсяг проведеної роботи, існує низка перспективних напрямків для подальших досліджень у сфері оптимізації систем радіозв’язку БПЛА:

Розробка та дослідження адаптивних алгоритмів ППРЧ та SDR на основі штучного інтелекту (ШІ):Моделювання та практична реалізація систем, здатних в реальному часі аналізувати радіоелектронну обстановку, прогнозувати дії РЕБ та самостійно обирати оптимальні параметри зв’язку (частоту, модуляцію, потужність, канали ППРЧ) для максимізації стійкості.

Дослідження ефективності мультисенсорної навігації для протидії комплексному впливу РЕБ: Аналіз можливостей поєднання даних від GNSS, ІНС, візуальних датчиків, лідарів та інших сенсорів для забезпечення точної та надійної навігації БПЛА в умовах повного подавлення або спуфінгу супутникових сигналів.

Аналіз вразливостей та розробка методів захисту супутникових каналів зв’язку БПЛА від новітніх загроз РЕБ: Враховуючи зростаючу роль супутникового зв'язку, необхідні дослідження специфічних методів його подавлення та розробка контрзаходів, включаючи аналіз стійкості комерційних систем типу Starlink до цілеспрямованих атак.

Розробка методів мінімізації електромагнітного сліду БПЛА: Дослідження конструктивних та програмних рішень для зменшення ймовірності виявлення БПЛА засобами радіотехнічної розвідки противника, включаючи адаптивне керування потужністю випромінювання та використання пасивних режимів роботи.

Подальший розвиток цих напрямків дозволить суттєво підвищити ефективність, надійність та безпеку застосування безпілотних літальних апаратів у складних умовах сучасних збройних конфліктів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Струць Є.М., Тарарака С.М., Коваленко О.О., Кравченко О.І. ПІДГОТОВКА СПЕЦІАЛІСТІВ РАДІОЗВ'ЯЗКУ : посібник / за заг. ред. Є.М. Струця. Полтава : військова частина А3990, 2015. URL: https://sprotyvg7.com.ua/wp-content/uploads/2022/04/Посібник-РАДІОЗВЯЗОК-HARRIS.pdf

2. ОСОБЛИВОСТІ ТЕХНОЛОГІЇ MAN-IA ДЛЯ УНИКНЕННЯ НТЕРФЕРЕНЦІЇ СПЕКТРУ В СИСТЕМАХ ЗВ'ЯЗКУ З БпЛА. Випробування і сертифікація озброєння та військової техніки. URL: https://dndivsovt.com/article/download

3. Pryor D. Temperature inversion interferes with signal. KGOU. 19.05.2023. URL: https://www.kgou.org/show/managers-minute/2023-05-19/temperature-inversion-interferes-with-signal

4. Ільїнов М.Д., Гурський Т.Г., Борисов І.В., Гриценок К.М. ЛІНІЇ РАДІОЗВ'ЯЗКУ ТА АНТЕННІ ПРИСТРОЇ: навчальний посібник. Київ : Військовий інститут телекомунікацій та інформатизації, 2018. URL: https://sprotyvg7.com.ua/wp-content/uploads/2023/05/антеніілінії.pdf

5. Збільшення радіусу дії рації: наука про узгодження антен. Herda Radio. 02.04.2023. URL: https://herdaradio.com/uk/blog/radioknowledge/antenna-matching/

6. ЗАХИСТ КАНАЛІВ ЗВ'ЯЗКУ ВІД ВПЛИВУ РЕБ. Для підрозділів зв'язку та БПЛА. Київ : Рота зв'язку В/Ч А4076, 2024. URL: https://sprotyvg7.com.ua/wp-content/uploads/2024/02/ЗАХИСТ_КАНАЛІВ_ЗВЯЗКУ_ВІД_ВПЛИВУ_РЕБ.pdf

7. GPSのNMEAフォーマット. hiramine.com. URL: https://www.hiramine.com/physicalcomputing/general/gps_nmeaformat.htm

8. NMEA & UBX Protocol(2). https://www.google.com/search?q=soaring-dylan.tistory.com. URL: https://soaring-dylan.tistory.com/45

9. meishujian (username). RTCM3.2协议格式说明. CSDN blog. URL: https://blog.csdn.net/meishujian/article/details/133642359

10. What is LoRaWAN?. The Things Network. URL: https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/

11. Callas J., Donnerhacke L., Finney H., Thayer R. OpenPGP Message Format. Network Working Group, RFC 4880. 2007. URL: https://tools.ietf.org/html/rfc4880

12. Advanced Encryption Standard (AES). FIPS PUB 197. National Institute of Standards and Technology, 2001 (updated 2023). URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.ipd.pdf

13. Daemen J., Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag Berlin Heidelberg New York, 2002. URL: https://cs.ru.nl/~joan/papers/JDA_VRI_Rijndael_2002.pdf

14. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Wiley Publishing, Inc., 2010. URL: https://www.schneier.com/wp-content/uploads/2015/12/fortuna.pdf

15. Реєстр компонентів. War & Sanctions. URL: https://war-sanctions.gur.gov.ua/components/5239

16. SX1233 DATASHEET. Semtech. URL: https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/44000000MDhJ/uoZxVBBi45_s8hUeWxMuVb.XHyW7EZsn_Gb0YdRrmVk

17. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978. Vol. 21, No. 2. P. 120-126. DOI: 10.1145/359340.359342. URL: https://dl.acm.org/doi/pdf/10.1145/359340.359342

18. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer Science+Business Media, Inc., 2004. URL: http://tomlr.free.fr/Math%E9matiques/Math%20Complete/Cryptography/Gu

ide%20to%20Elliptic%20Curve%20Cryptography%20-%20D.%20Hankerson,%20A.%20Menezes,%20S.%20Vanstone.pdf

19. Barker E., Roginsky A. Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST Special Publication 800-131A Revision 2. National Institute of Standards and Technology, 2019. DOI: 10.6028/NIST.SP.800-131Ar2. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

20. López J., Dahab R. An Overview of Elliptic Curve Cryptography. Technical Report IC-00-10. Institute of Computing, UNICAMP, Brazil, 2000. URL: https://www.ic.unicamp.br/~reltech/2000/00-10.pdf

21. Kocher P., Jaffe J., Jun B. Differential Power Analysis. Advances in Cryptology - CRYPTO' 99. Lecture Notes in Computer Science, vol 1666. Springer, Berlin, Heidelberg, 1999. P. 388-397. DOI: 10.1007/3-540-48405-1_25. URL: https://link.springer.com/chapter/10.1007/3-540-44448-3_38

22. Stallings W. Cryptography and Network Security: Principles and Practice. 5th ed. Prentice Hall, 2011. URL: https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Cryptography_and_Network_Security.pdf

23. Rhodes R. Hedy's folly : the life and breakthrough inventions of Hedy Lamarr, the most beautiful woman in the world. Doubleday, 2011. URL: https://archive.org/details/hedysfollylifea00rhod/page/n7/mode/2up

24. Woolley M. Bluetooth® Core 5.2 Feature Overview. Version 1.0.2. Bluetooth SIG. 13.01.2025. URL: https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf

25. MATRICE 300 RTK User Manual v3.0. DJI. 2021.11. URL: https://dl.djicdn.com/downloads/matrice-300/20211125UM/M300_RTK_User_Manual_EN_v3.0.pdf

26. Lockheed Martin demonstrates adaptive communications jamming. Intelligence Community News.

URL: https://intelligencecommunitynews.com/lockheed-martin-demonstrates-adaptive-communications-jamming/

27. Link 16. Wikipedia. URL: https://en.wikipedia.org/wiki/Link_16

28. Holma H., Toskala A., Nakamura T. (eds.). 5G Technology: 3GPP Evolution to 5G-Advanced. 2nd ed. Wiley, 2023. URL: https://dokumen.pub/5g-technology-3gpp-evolution-to-5g-advanced-9781119816034.html

29. M300 RTK Release Notes. DJI. 16.04.2025. URL: https://dl.djicdn.com/downloads/matrice-300/20250416RN/M300_RTK_Release_Notes_en.pdf

30. Kaur H.J., Singh M.L. Modelling and Reporting Parameters of Optical OFDM System Using Different Modulation Techniques. Circuits and Systems. 2012. Vol. 3, No. 3. P. 257-264. DOI: 10.4236/cs.2012.33036. URL: https://www.scirp.org/journal/paperinformation?paperid=32869

31. Dillinger M., Madani K., Alonistioti N. (eds.). Software Defined Radio: Architectures, Systems and Functions. Wiley, 2003. URL: https://content.e-bookshelf.de/media/reading/L-580205-4b85c2135a.pdf

32. Software-Defined Radios (SDRs): A Key Enabling Technology for Modern Military Applications. Saab. 11.03.2025. URL: https://saabrds.com/software-defined-radios-sdrs-a-key-enabling-technology-for-modern-military-applications/ (Примітка: Дата 11.03.2025 вказана як дата публікації та є майбутньою відносно дати звернення).

33. Software Defined Radio. Annap Micro. URL: https://www.annapmicro.com/solutions/sw-defined-radio/

34. Le Roy F., Roland C., Le Jeune D., Diguet J-P. Risk assessment of SDR-based attacks with UAVs. 2019 16th International Symposium on Wireless Communication Systems (ISWCS). Oulu, Finland, 2019. P. 566-570. DOI: 10.1109/ISWCS.2019.8877144.
URL: https://www.researchgate.net/publication/336728079_Risk_assessment_of_SDR-based_attacks_with_UAVs

35. Michailidis E.T., Maliatsos K. Software-Defined Radio Deployments in UAV-Driven Applications: A Comprehensive Review. TechRxiv. Preprint posted online 29.08.2024. DOI: 10.36227/techrxiv.171778948.88990152/v1. URL: https://www.researchgate.net/publication/381259303_Software-Defined_Radio_Deployments_in_UAV-Driven_Applications_A_Comprehensive_Review#pf7

36. Airborne and Ground Antennas and RF Systems. L3Harris Technologies. 2021. URL: https://www.l3harris.com/sites/default/files/2021-07/cs-tcom-airborne-portfolio-sell-sheet.pdf (Примітка: Назва з метаданих PDF).

37. Polikarovskykh O., Hula I. Implementing the Search Algorithm of the Correlation Interferometer Direction Finder through the GNU Radio Software Platform. Security of Infocommunication Systems and Internet of Things. 2023. Vol. 1, No. 2. P. 02006(1)-02006(7). DOI: 10.31861/sisiot2023.2.02006. URL: https://journals.chnu.edu.ua/article/download/299045/293368

38. Advanced Extremely High Frequency. Wikipedia. URL: https://en.wikipedia.org/wiki/Advanced_Extremely_High_Frequency

39. Mobile User Objective System (MUOS). General Dynamics Mission Systems. URL: https://gdmissionsystems.com/satellite-ground-systems/mobile-user-objective-system

40. SKYNET Integrated Enterprise Solution (SKIES) programme. GOV.UK. URL: https://www.gov.uk/guidance/skynet-integrated-enterprise-solution-skies-programme

41. Syracuse IV. Airbus. URL: https://www.airbus.com/en/products-services/defence/military-space/syracuse-iv

42. Дудко В., Наконечна А., Мельник Т. SpaceX обмежила використання Starlink на українському фронті. Звинувачує дрони. Що це означає для ЗСУ. Forbes.ua. 09.02.2023. URL: https://forbes.ua/innovations/spacex-obmezhila-vikoristannya-starlink-na-ukrainskomu-fronti-zvinuvachue-droni-shcho-tse-oznachae-dlya-zsu-09022023-11632

43. Satellite phones obsolete; DISA looking for a new, secure capability. Defense Systems Staff. Defense One. 08.05.2013. URL: https://www.defenseone.com/defense-systems/2013/05/satellite-phones-obsolete-disa-looking-for-a-new-secure-capability/190042/

44. Satellite Technology. Starlink. URL: https://www.starlink.com/technology

45. Основи радіоелектронної боротьби: теорія та застосування. Lander.kiev.ua. 10.06.2024. URL: https://lander.kiev.ua/osnovy-radioelektronnoi-borotby-teoriia-ta-zastosuvannia/?srsltid=AfmBOoq_2FbOF-sDw4jj35z_1iowuLny1EucUryELS-RpBV0LQljuRs4

46. Yao L., Qin H., Gu B. et al. A Study on Anti-Jamming Algorithms in Low-Earth-Orbit Satellite Signal-of-Opportunity Positioning Systems for Unmanned Aerial Vehicles. Drones. 2024. Vol. 8(4), 164. DOI: 10.3390/drones8040164. URL: https://www.mdpi.com/2504-446X/8/4/164

47. IMPROVING STARLINK'S LATENCY. Starlink. URL: https://www.starlink.com/public-files/StarlinkLatency.pdf

48. The 2023 EU Capability Development Priorities. European Defence Agency, 2023. URL: https://eda.europa.eu/docs/default-source/brochures/qu-03-23-421-en-n-web.pdf

49. Cheng G., Huang Q., Xing R., Lin M., Upadhyay P.K. On the secrecy performance of integrated satellite-aerial-terrestrial networks. International Journal of Satellite Communications and Networking. 2021. Vol. 39, No. 5. P. 535-546. DOI: 10.1002/sat.1334. URL: https://dl.acm.org/doi/10.1002/sat.1334 (Примітка: Посилання dl.acm.org, але DOI вказує на Wiley).

50. Xi Y., Liu J., Zhao W. SATCOM Earth Station Arrays Anti-Jamming Based on MVDR Algorithm. Applied Sciences. 2023. Vol. 13(14), 8337. DOI: 10.3390/app13148337. URL: https://www.mdpi.com/2076-3417/13/14/8337

51. Panella C. Here's how a top satellite imagery company plans to fly drones through intense GPS jamming. Business Insider. March 2025.

URL: https://www.businessinsider.com/new-software-to-fly-drones-through-toughest-gps-jamming-2025-3

52. Panella C. This Ukrainian tech company is working to beat Russia's electronic warfare without hard-wiring drones to an operator. Business Insider. February 2025. URL: https://www.businessinsider.com/ukrainian-company-could-have-new-answer-to-russias-drone-jamming-2025-2

53. Какими беспилотниками мы атакуем цели противника в Крыму? ВРБ | Новини ↑ аналітикаканалу. Telegram. URL: https://t.me/c/1795199366/56602

54. Війська РФ використовують термінали Starlink переважно на окупованих територіях - експерт. Укрінформ. 12.02.2024. URL: https://www.ukrinform.ua/rubric-ato/3826722-vijska-rf-vikoristovuut-terminali-starlink-perevazno-na-okupovanih-teritoriah-ekspert.html

55. Russia is raining hellfire on Ukraine: New attacks push its air defences to saturation point. The Economist. 25.05.2025. URL: https://www.economist.com/europe/2025/05/25/russia-is-raining-hellfire-on-ukraine(Примітка: Дата "25.05.2025" вказана в URL та є майбутньою).

56. Сафронов Т. Над Україною збили “Шахед” з терміналом Starlink. Мілітарний. 25.09.2024. URL: https://militarnyi.com/uk/news/nad-ukrayinoyu-zbyly-shahed-z-terminalom-starlink/ (Примітка: Дата 25.09.2024 вказана на сайті, є майбутньою).

57. Paton Walsh N., Marquardt A., Davey-Attlee F., Gak K. Ukraine relies on Starlink for its drone war. Russia appears to be bypassing sanctions to use the devices too. CNN. 26.03.2024. URL: https://edition.cnn.com/2024/03/25/europe/ukraine-starlink-drones-russia-intl-cmd

58. Assured Positioning, Navigation & Timing. Raytheon UK. URL: https://www.raytheon.co.uk/what-we-do/weapons-and-sensors/assured-positioning-navigation-and-timing

59. Asia/Pacific Regional Aeronautical Radio Frequency Management Guidance Material. Edition 1.0. International Civil Aviation Organization. URL: https://www.icao.int/APAC/Documents/edocs/Asia%20Pacific%20Regional%20Aeronautical%20Radio%20Frequency%20Management%20Guidance%20Material%20Edition%201.0.pdf

60. Новітня українська система спуфінгу "Покрова" збиває з пантелику "Шахеди" - Forbes. БукІнфо. URL: https://bukinfo.com.ua/viyna-na-shodi/novitnya-ukrajinska-systema-spufingu-pokrova-zbyvaye-z-pantelyku-shahedy-forbes

61. Cook E. Ukraine Found Way to Divert Russian Drones into Neighbor's Airspace-Report. Newsweek. 28.11.2024. URL: https://www.newsweek.com/ukraine-russia-drones-belarus-spoofing-gps-1992969

62. Antoniuk D. Ukrainian military’s anti-drone GPS spoofing spills into civilians’ phones. The Record. 07.11.2024. URL: https://therecord.media/ukraine-anti-drone-gps-spoofing-affects-civilian-mobile-phones

63. Що таке засоби радіоелектронної боротьби (РЕБи)? KOLO. 2024. URL: https://koloua.com/news/shcho-take-zasobi-radioelektronnoyi-borotbi-rebi-34

64. Ян О. SpaceX обмежила використання українських терміналів Starlink. Мілітарний. 09.02.2023. URL: https://militarnyi.com/uk/news/spacex-obmezhyla-vykorystannya-ukrayinskyh-terminaliv-starlink/

ДОДАТОК А

Ключові фрагменти коду симулятора стійкості БПЛА з ППРЧ (fhss_final.py)

У цьому додатку представлено ключові фрагменти програмного коду, що демонструють основні алгоритми, реалізовані в симуляторі. Замість повного лістингу наведено функції, що відповідають за логіку перестрибування частоти (ППРЧ) та розрахунок впливу засобів РЕБ.

Фрагмент 1: Реалізація механізму перестрибування частоти

Наведений нижче метод perform_frequency_hop є центральним у реалізації технології ППРЧ. Він відповідає за зміну робочої частоти дрона залежно від обраного режиму: випадкового (RANDOM), послідовного (SEQUENTIAL) або адаптивного (ADAPTIVE), який обирає найкращу частоту на основі історії якості зв'язку

```
    def perform_frequency_hop(self):
        """Виконує перемикання частоти згідно з обраним режимом FHSS"""
        if not self.fhss_enabled or self.fhss_mode == FHSSMode.FIXED:
            return
        if self.fhss_mode == FHSSMode.RANDOM:
            new_idx = random.randint(0, len(self.fhss_channels)-1)
            while new_idx == self.current_channel_idx and len(self.fhss_channels)
> 1:
                new_idx = random.randint(0, len(self.fhss_channels)-1)
            self.current_channel_idx = new_idx
        elif self.fhss_mode == FHSSMode.SEQUENTIAL:
            self.current_channel_idx = (
                self.current_channel_idx + 1) % len(self.fhss_channels)
        elif self.fhss_mode == FHSSMode.ADAPTIVE:
```

```
            if len(self.adaptive_hop_history) >= self.adaptive_window_size:
                freq_quality = {freq: 0 for freq in self.fhss_channels}
                for time, freq, quality in self.adaptive_hop_history:
                    freq_quality[freq] += quality

                best_freq = max(freq_quality.items(), key=lambda x: x[1])[0]
                self.current_channel_idx = self.fhss_channels.index(best_freq)
            else:
                # На початку, поки історії немає, стрибає випадково
                self.current_channel_idx = random.randint(
                    0, len(self.fhss_channels)-1)
        self.drone_frequency = self.fhss_channels[self.current_channel_idx]
        self.target_line.set_xdata(
            [self.drone_frequency, self.drone_frequency])
        self.adaptive_hop_history.append((
            self.simulation_time,
            self.drone_frequency,
            self.signal_strength
        ))
        if len(self.adaptive_hop_history) > self.adaptive_window_size * 2:
            self.adaptive_hop_history.pop(0)
        self.last_hop_time = self.simulation_time
```

Фрагмент 2: Розрахунок якості сигналу під впливом РЕБ

Метод calculate_signal_strength моделює якість зв'язку, враховуючи три основні фактори: втрати сигналу через відстань, вплив середовища (погоди та місцевості) і, найголовніше, вплив системи РЕБ. Змінна reb_impactрозраховується на основі різниці між частотою дрона та

частотою подавлення, а також враховує перевагу, яку надає увімкнена технологія ППРЧ (fhss_advantage).

```
    def calculate_signal_strength(self):
        distance_loss = 1.0 / (1.0 + (self.drone_position / 3000) ** 1.5)
        env_impact = self.calculate_environment_impact()

        reb_impact = 1.0
        if self.reb_active:
            freq_diff = abs(self.reb_current_freq - self.drone_frequency)
            # ППРЧ дає невелику перевагу (зменшує ефективність РЕБ)
            fhss_advantage = 0.2 if self.fhss_enabled else 0
            # Якщо РЕБ "потрапила" на частоту дрона
            if freq_diff < self.suppression_bandwidth:
                suppression_power = 1.0 - (freq_diff / self.suppression_bandwidth)
                reb_impact = max(0.3 + fhss_advantage, 1.0 -
                                 suppression_power * (0.7 - fhss_advantage))
        noise = 1.0 + random.uniform(-0.03, 0.03)
        return min(100, max(10, 100 * distance_loss * env_impact * reb_impact *
noise))
```

ДОДАТОК Б

Ключові фрагменти коду симулятора стійкості БПЛА з супутниковим каналом (sat9.py)

У цьому додатку наведено фрагменти програмного коду, що ілюструють реалізацію різних типів атак засобами РЕБ на БПЛА, який використовує супутниковий канал зв'язку. Фрагменти взяті з центрального методу update_drone_state, що керує поведінкою дрона.

Фрагмент 1: Логіка неконтрольованого падіння при глушінні зв'язку

Цей блок коду перевіряє, чи активне глушіння супутникового каналу (jamming_active_effect) і чи впала якість каналу керування нижче критичного порога. Якщо умови виконуються, симулюється неконтрольоване падіння: висота різко зменшується (effective_fall_rate), а горизонтальна швидкість поступово згасає.

```
# --- Логіка падіння через глушіння/втрату зв'язку ---
control_lost_threshold_jamming = 30
control_lost_threshold_general = 10
is_falling_uncontrolled = False
# Перевірка умов для падіння
if self.jamming_active_effect and self.control_link_quality < control_lost_threshold_jamming:
    is_falling_uncontrolled = True
elif self.control_link_quality < control_lost_threshold_general: # Загальна втрата зв'язку
    is_falling_uncontrolled = True
if is_falling_uncontrolled:
    if not self.mission_failed:
        self.mission_failed = True
```

```
            print(f"Час {self.simulation_time:.1f}с: Місію провалено через втрату керування (падіння).")
            # Розрахунок швидкості падіння
            effective_fall_rate = self.climb_rate * self.uncontrolled_fall_rate_multiplier
            self.drone_position_actual[1] -= effective_fall_rate * dt
            # Втрата горизонтальної швидкості
            self.current_drone_speed -= self.acceleration_rate * dt * 1.5
            if self.current_drone_speed < 0: self.current_drone_speed = 0
            self.drone_position_actual[0] += self.current_drone_speed * dt
            # Перевірка аварії
            if self.drone_position_actual[1] <= 0:
                self.drone_position_actual[1] = 0
                self.crashed = True
                self.current_drone_speed = 0
                print(f"Час {self.simulation_time:.1f}с: Аварія через падіння!")
            return
```

Фрагмент 2: Розрахунок якості супутникового каналу та впливу глушіння

Наступний фрагмент коду, метод calculate_link_qualities, демонструє, як у симуляції моделюється якість супутникового зв'язку. Розрахунок базується на декількох факторах: початкова базова якість сигналу (100%), коефіцієнт впливу середовища (env_factor), який враховує погоду та тип місцевості, і найголовніше - ефект від активного глушіння РЕБ (jamming_active_effect). Якщо глушіння активне, якість каналу різко знижується (множиться на 0.05), що і призводить до втрати керування, як показано в інших частинах коду.

```
        def calculate_environmental_impact_factor(self):
            terrain_factor = 1.0
```

```
        if self.terrain == TerrainType.MISTO and self.drone_position_actual[1] <
500:
            terrain_factor = 0.9
        elif self.terrain == TerrainType.HORY and self.drone_position_actual[1] <
1500:
            terrain_factor = 0.8
        weather_factor = 1.0
        if self.weather == WeatherType.DOSHCH: weather_factor = 0.85
        elif self.weather == WeatherType.SHTORM: weather_factor = 0.65
        elif self.weather == WeatherType.TUMAN: weather_factor = 0.95
        elif self.weather == WeatherType.SONYACHNA_VSPYSHKA:
weather_factor = 0.4
        return terrain_factor * weather_factor
    def calculate_link_qualities(self):
        base_quality = 100.0
        # Враховуємо вплив середовища
        env_factor = self.calculate_environmental_impact_factor()
        current_link_quality = base_quality * env_factor
        # Якщо система РЕБ активувала глушіння, якість сигналу різко падає
        if self.jamming_active_effect:
            current_link_quality *= 0.05

        # Додаємо невеликий випадковий шум для реалістичності
        current_link_quality *= random.uniform(0.95, 1.05)
        self.satellite_link_quality = np.clip(current_link_quality, 0, 100)
        # Якість каналу керування та відео залежить від загальної якості
супутникового зв'язку
        self.control_link_quality = np.clip(self.satellite_link_quality * 1.0, 0, 100)
        self.video_link_quality = np.clip(self.satellite_link_quality * 0.8, 0, 100)
```