Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В. о. завідувач кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«__» червня 2025р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 «Кібербезпека»
(код і назва спеціальності)
освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Методи захисту каналів зв'язку безпілотних літальних апаратів»

Виконавець: студент IV курсу, групи КБ-41

_____ **Дмитро САВЧУК**
(підпис) (ім'я прізвище)

	Підпис	**Ім'я, прізвище**
Керівник		Яніна ШЕСТАК
Нормоконтроль		Іван БІЛОКОНЬ

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В. о. завідувач кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої-професійної програми)

студенту **КБ-41** **Савчуку Дмитру Васильовичу**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Методи захисту каналів зв'язку безпілотних літальних апаратів

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Безпека каналів зв'язку безпілотних літальних апаратів: загрози та методи захисту

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з методами захисту каналів зв'язку безпілотних літальних апаратів та розробити рекомендації до захисту інформаційного обміну в системах БпЛА.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розробка практичних рекомендацій та заходів для

підвищення рівня захищеності каналів зв’язку БпЛА

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім’я, прізвище)

Завдання прийняв до виконання _____ (підпис) Дмитро САВЧУК (ім’я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 22.01.2025	*виконано*
2	Аналіз літератури	29.01.2025 – 11.02.2025	*виконано*
3	Обґрунтування вибору рішення	12.02.2025 – 15.02.2025	*виконано*
4	Дослідження особливостей функціонування безпілотних літальних апаратів	16.02.2025 – 04.03.2025	*виконано*
5	Дослідження загроз безпеці каналів зв’язку БпЛА	05.03.2025 – 21.03.2025	*виконано*
6	Аналіз прикладів атак на комунікаційні канали БпЛА та підходів до забезпечення стійкості цих каналів.	22.03.2025 – 08.04.2025	*виконано*
7	Розробка рекомендацій для захисту інформаційного обміну в системах БпЛА	09.04.2025 – 10.05.2025	*виконано*
8	Оформлення пояснювальної записки	11.05.2025 – 27.05.2025	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2025 – 13.06.2025	*виконано*

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім’я, прізвище)

Завдання прийняв до виконання _____ (підпис) Дмитро САВЧУК (ім’я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, містить 73 сторінки основного тексту, 1 таблицю та 2 рисунки. Список використаних джерел містить 21 найменування і займає 3 сторінки.

Метою роботи є аналіз загроз безпеці каналів зв’язку безпілотних літальних апаратів, дослідження методів несанкціонованого втручання та розробка практичних рекомендацій щодо підвищення рівня захисту інформаційного обміну в комунікаційних системах БпЛА.

Для досягнення зазначеної мети поставлено наступні завдання:

- дослідити класифікацію, архітектуру систем управління та комунікаційні технології сучасних БпЛА;
- визначити та проаналізувати основні радіоелектронні й кібернетичні загрози, що впливають на безпеку каналів зв'язку БпЛА;
- розробити комплекс практичних рекомендацій для підвищення безпеки інформаційного обміну в комунікаційних системах БпЛА.

Об'єктом дослідження є процеси функціонування та забезпечення безпеки каналів зв’язку та систем управління безпілотних літальних апаратів.

Предметом дослідження є радіоелектронні та кібернетичні загрози безпеці, методи несанкціонованого втручання, а також підходи, технології та стратегії захисту інформаційного обміну в комунікаційних системах БпЛА.

Методи дослідження:

- аналіз науково-технічної літератури та відкритих джерел щодо функціонування БПЛА, їх комунікаційних систем та існуючих загроз;
- системний аналіз архітектури БПЛА, їх систем управління та обміну даними;
- класифікація та структурування типів БПЛА, каналів зв’язку, загроз та методів несанкціонованого втручання;

Практичної цінністю отриманих результатів є:

- систематизовано основні типи та класифікації безпілотних систем, проаналізовано структуру їхніх систем управління, архітектуру обміну даними, особливості комунікаційних модулів, каналів зв’язку та роботи станцій оператора;
- проведено комплексне дослідження основних типів радіоелектронних та кібернетичних загроз безпеці каналів зв’язку БПЛА;
- проаналізовано актуальні приклади атак на канали керування БПЛА;
- досліджено та систематизовано сучасні підходи до забезпечення стійкості каналів зв’язку БПЛА, зокрема апаратні, протокольні, алгоритмічні, інтелектуальні та комплексні методи нейтралізації загроз;
- розроблено практичні рекомендації щодо захисту інформаційного обміну в системах БПЛА.

Пропозиції щодо продовження досліджень включають поглиблене дослідження методів захисту від комбінованих та багатовекторних атак на БПЛА, розробку адаптивних систем безпеки на основі штучного інтелекту для динамічного виявлення та протидії новим загрозам, аналіз безпеки комунікацій в роях БПЛА, а також дослідження та впровадження стандартів безпеки для комунікаційних протоколів БПЛА та розробку квантово-стійких криптографічних алгоритмів.

Ключові слова: безпілотний літальний апарат, канали зв’язку, безпека інформації, радіоелектронні загрози, кібернетичні загрози, радіоелектронне придушення (РЕП), несанкціоноване втручання, глушіння, спуфінг, методи захисту, стійкість каналів зв’язку, кібербезпека, БПЛА, рекомендації.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AI	–	Artificial intelligence
DoS	–	Denial-of-service attack
DSSS	–	Direct Sequence Spread Spectrum
FHSS	–	Frequency Hopping Spread Spectrum
GCS	–	Ground Control Station
GNSS	–	Global Navigation Satellite System
GPS	–	Global Positioning System
IMU	–	Inertial Measurement Unit
IP	–	Internet Protocol
LWC	–	Lightweight Cryptography
LOS	–	Line of Sight
MAVLink	–	Micro Air Vehicle Link
MitM	–	Man-in-the-Middle
OFDM	–	Orthogonal Frequency-Division Multiplexing
SDR	–	Software-Defined Radio
UAV	–	Unmanned Aerial Vehicle
БПЛА	–	Безпілотний літальний апарат
ПЗ	–	Програмне забезпечення
НСК	–	Наземна станція керування (також GCS)
РЕБ	–	Радіоелектронна боротьба
РЕП	–	Радіоелектронне подавлення
ШІ	–	Штучний інтелект

ВСТУП

Назараз безпілотні літальні апарати (БПЛА) перетворилися на невід'ємний інструмент у численних сферах – від військових операцій та моніторингу критичної інфраструктури до цивільних завдань, таких як логістика, сільське господарство та картографування. Їх ефективне та безпечне функціонування критично залежить від надійності та захищеності каналів зв’язку, які забезпечують передачу команд керування, телеметричної інформації та даних корисного навантаження. Зі стрімким розвитком технологій БПЛА та розширенням їх застосування, питання забезпечення безпеки цих комунікаційних каналів набуває надзвичайної актуальності.

Канали зв’язку БПЛА все частіше стають об’єктами цілеспрямованих атак, що використовують як радіоелектронні, так і кібернетичні методи впливу. Подібні втручання можуть призвести не лише до значних фінансових збитків через втрату дороговартісних апаратів, але й до зриву виконання критично важливих завдань, компрометації конфіденційної інформації, а в окремих випадках – до створення загроз для безпеки людей та об'єктів.

Кваліфікаційна робота присвячена дослідженню загроз безпеці каналів зв’язку безпілотних літальних апаратів та розробці практичних рекомендацій щодо їх захисту. У рамках роботи розглядаються різні аспекти функціонування БПЛА та їх комунікаційних систем, аналізуються основні типи радіоелектронних та кібернетичних загроз, методи несанкціонованого втручання, а також сучасні підходи та технології для забезпечення стійкості та безпеки інформаційного обміну.

Актуальність роботи обумовлена необхідністю адаптації систем БПЛА до швидкозмінного ландшафту загроз та розробки надійних багаторівневих механізмів захисту їхніх комунікаційних каналів.

Основною метою роботи є проведення комплексного аналізу загроз безпеці каналів зв’язку БПЛА, дослідження методів несанкціонованого

втручання та розробка практичних рекомендацій, спрямованих на підвищення рівня захищеності інформаційного обміну в сучасних безпілотних системах.

Для досягнення зазначеної мети кваліфікаційної роботи поставлено наступні завдання:

- Проаналізувати основні типи та класифікації безпілотних систем, особливості їх функціонування та архітектуру комунікаційних систем.
- Дослідити структуру систем управління БПЛА, архітектуру обміну даними, а також основні характеристики комунікаційних модулів та каналів зв’язку.
- Проаналізувати актуальні приклади атак на канали керування БПЛА та фундаментальні механізми несанкціонованого втручання.
- Розробити практичні рекомендації щодо захисту інформаційного обміну в системах БПЛА на основі проведеного аналізу.

Структура роботи включає три основні розділи.

Перший розділ присвячений аналізу особливостей функціонування безпілотних апаратів та їх комунікаційних систем. У ньому розглядаються основні типи та класифікація БПЛА, детально аналізується структура системи управління та архітектура обміну даними, а також розглядаються комунікаційні модулі, канали зв’язку, особливості роботи станції оператора та бортових систем.

Другий розділ зосереджений на дослідженні загроз безпеці каналів зв’язку та методів їх нейтралізації. Проводиться аналіз основних типів радіоелектронних та кібернетичних загроз, розглядаються актуальні приклади атак на канали керування, аналізуються методи несанкціонованого втручання та досліджуються підходи до забезпечення стійкості каналів зв’язку.

Третій розділ присвячений розробці практичних рекомендацій щодо захисту інформаційного обміну в системах БПЛА, що базуються на результатах аналізу, проведеного в попередніх розділах.

У заключній частині роботи наведено загальні висновки та підсумовано результати дослідження, спрямовані на підвищення рівня безпеки

комунікаційних систем БПЛА. Тому, дана кваліфікаційна робота є комплексним дослідженням, яке охоплює ключові аспекти безпеки каналів зв’язку БПЛА та пропонує науково обґрунтовані підходи до їх захисту в умовах сучасних викликів.

РОЗДІЛ 1
ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ БЕЗПІЛОТНИХ АПАРАТІВ ТА ЇХ КОМУНІКАЦІЙНИХ СИСТЕМ

1.1. Основні типи та класифікація безпілотних систем

Безпілотна система — це комплекс, основною частиною якого є безпілотний літальний апарат (БпЛА). Його головна особливість полягає в тому, що керування здійснюється дистанційно, без фізичної присутності пілота на борту. Конструктивно БпЛА включає повітряну платформу, енергетичну установку, систему живлення, а також набір бортового обладнання: навігаційні системи, системи зв’язку, керуючі мікропроцесори, альтиметри, гіродатчики, сервоприводи тощо.

Один з найпоширеніших підходів до класифікації — це поділ безпілотників за функціональним призначенням. В цьому контексті виділяють апарати, що застосовуються для військових, антитерористичних або цивільних цілей. У межах цивільного використання також говоримо про державні, комерційні чи транспортні дрони, кожен з яких вирішує специфічні задачі, як-от доставка або зйомка.

Інший важливий критерій — дальність виконання завдань. Тут БпЛА умовно поділяють на тактичні (з радіусом до 80 км), оперативно-тактичні (до 300 км) та оперативно-стратегічні (до 700 км і більше). Відстань, на якій апарат може ефективно працювати, безпосередньо впливає на його конструктивні особливості, потужність обладнання і рівень енергозабезпечення.

Від маси апарата залежить як спосіб запуску, так і обсяг завдань, які він може виконувати. Зазвичай виділяють малорозмірні БпЛА масою до 200 кг, середні — до 2 тонн, великі — до 5 тонн, а також важкі безпілотники, які можуть перевищувати 5 тонн. Чим більша маса, тим складнішою є система управління та вищою вартість виготовлення та експлуатації.

Тривалість польоту — ще один параметр. Деякі дрони здатні перебувати в повітрі лише кілька годин (до 6 год), тоді як інші можуть працювати до 12 годин або більше. Цей показник залежить як від типу енергоносія, так і від особливостей конструкції крила, двигуна та системи енергозбереження.

Щодо висоти польоту, існують маловисотні апарати (до 1 км), середньовисотні (до 4 км), висотні (до 12 км) та навіть стратосферні моделі, які можуть сягати понад 12 км. Чим вище може піднятись БпЛА, тим більше вимог ставиться до його герметичності, навігації та зв’язку.

Класифікують їх і за типом літального апарата. Деякі створені за принципом літака з фіксованими крилами, інші — за схемою гелікоптера з можливістю вертикального злету і посадки. Також існують перехідні моделі, наприклад, конвертоплани, в яких поєднуються ознаки обох типів. Окремо варто згадати апарати, що легші за повітря, хоча вони є менш поширеними.

Місце експлуатації також є критерієм для поділу. Існують наземні, морські та навіть космічні безпілотні системи. Вони значно відрізняються за конструкцією, адже адаптовані до принципово різних умов — від земної поверхні до водного середовища і навколоземного простору.

Тип керування поділяє БпЛА на дистанційно пілотовані — коли оператор керує польотом в межах прямої видимості; дистанційно керовані — з можливістю втручання через системи зв’язку; та автоматичні — які діють на основі заданої програми, без втручання людини. Останні набули значної популярності завдяки розвитку штучного інтелекту і систем навігації.

Виділяють також типи керування польотом: візуальне, приладове та комбіноване. У візуальному режимі керування здійснюється у межах видимості, тоді як приладовий режим дозволяє літати в умовах недостатньої видимості або вночі — завдяки сенсорам, GPS та іншим системам. Комбіновані варіанти забезпечують найбільшу гнучкість.

Класифікують дрони і за типом енергоживлення. Монозаправні апарати заправляються один раз, часто на заводі, і зазвичай призначені для одноразового використання. Полізаправні — мають можливість багаторазової заправки як

наземним способом, так і через спеціальні морські або повітряні станції. Також можна виділити БпЛА з базовим або резервним паливним баком, що забезпечує їм більшу автономність.

За напрямком підйому та посадки зазвичай їх поділять на горизонтальні, вертикальні та мульти (підйомі/спускові). Проте, враховуючи специфіку посадки, сюди можна додати парашутні, мачтові, безпосадкові.

Також класифікують БпЛА за типом підйому та посадки. За першим критерієм вони поділяються на аеродромні, запускні, палубні, водні, ручні, мультипідйомні. А за лругим вони можуть бути аеродромні, точкові, палубні, водні, безпосадкові, нетипово-посадкові, мультипосадкові.

1.2. Структура системи управління та архітектура обміну даними

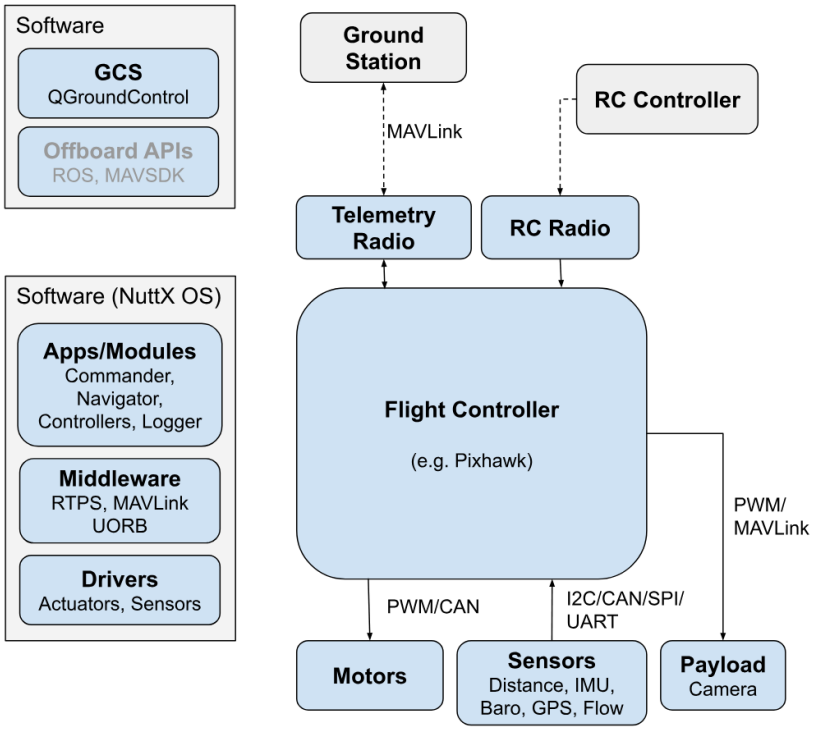

Рисунок 1.1 – Проста система управління БпЛА на основі польотного контролера

Проста система управління БПЛА складається з кількох функціональних блоків (рис. 1.1): блоку живлення, приймача команд оператора (модуль радіоуправління), польотного контролера (автопілота) з вбудованими сенсорами

(інерціальною системою IMU, барометром, магнітометром) та інтерфейсами для зовнішніх датчиків (GPS-приймач, дальноміри, датчики оптичного потоку тощо), а також виконавчих механізмів (електронних регуляторів швидкості ESC і сервоприводів на двигунах). Автопілот реалізує алгоритми стабілізації й навігації, отримуючи з сенсорів вимірювання (положення, швидкості, висоти) й формуючи керуючі сигнали на двигуни або керовані поверхні. У професійних системах для зв'язку між блоками часто застосовують шину CAN (UAVCAN) – диференційну цифрову шину, що дозволяє підключати багато пристроїв паралельно та забезпечує відмовостійкість через вбудований арбітраж повідомлень.[1]

Типові датчики включають IMU (комплект гіроскопів і акселерометрів), GPS, барометр та ультразвуковий/лазерний висотометр. Гіроскопи вимірюють кутові швидкості, які інтегруються для оцінки орієнтації (з накопиченням похибок на дрейф), а акселерометри фіксують лінійні прискорення (за відсутності руху це напрямок сили тяжіння, що служить абсолютним орієнтиром «вертикалі» для корекції нахилу).

Магнітометр (електронний компас) дає азимут за магнітним полем Землі. GPS-модуль забезпечує глобальне позиціювання (широта/довгота) і час для навігації. Барометр вимірює атмосферний тиск, що дозволяє оцінити висоту польоту над рівнем моря.

При наближенні до землі в роботу часто підключають ультразвуковий або лазерний дальномір для підвищення точності вимірювання висоти, оскільки барометр у низьких діапазонах може бути менш точним. Наприклад, в режимі утримання висоти (AltHold) автопілот ArduPilot використовує барометр як основне джерело висоти і покладається на дальномір для досягнення точного зниження при приземленні. [2]

Дані всіх сенсорів фільтруються та об'єднуються алгоритмом розширеного фільтра Калмана (EKF), що забезпечує стійку оцінку станів дрона (положення, швидкості, орієнтації).

Для стабілізації польоту застосовується каскадна система регулювання. У внутрішньому контурі регулюються кути (крен, тангаж), а зовнішній контур відповідає за положення (курс, швидкість, висота). Автопілот обчислює необхідні зусилля двигунів на основі встановлених завдань і поточного стану. Наприклад, позиційний регулятор перетворює бажані координати чи курс у цільові кути нахилу і величину тяги двигунів, що рухають БПЛА до заданої точки.

Регулятор висоти підтримує задане значення висоти: він порівнює покази барометра з еталонним рівнем і змінює подачу газу на двигуни. У режимі утримання висоти (AltHold) автопілот автоматично коригує тягу, щоб літак залишався на тій самій висоті. Таким чином, внутрішній контур стабілізує орієнтацію апарата (за даними IMU і магнітометра), а зовнішній – навігаційні параметри (за даними GPS, барометра, далекоміра).

Архітектура обміну даними всередині БПЛА базується на суміші зв’язків. Бортові сенсори підключаються до польотного контролера через стандарти I²C, SPI або UART (зіркоподібна топологія з контролером у центрі). Зокрема, I²C-шина дуже популярна для барометрів, IMU, компасів та інших датчиків, оскільки потребує лише двох проводів. SPI інтерфейс дозволяє підключати високошвидкісні сенсори (часто MEMS-гіроскопи/акселерометри, ультразвукові дальноміри тощо) з набагато вищими частотами обміну, використовуючи окремі лінії вибору для кожного пристрою.

Натомість CAN-шина (задіяна у протоколі UAVCAN) створює єдиний загальний канал: усі периферійні вузли (датчики, ESC та ін.) з’єднують послідовно («daisy chain») на одному кабелі з обов’язковим термінуванням на кінцях шини. Це спрощує прокладку проводів і забезпечує можливість гнучко додавати нові пристрої (порядок підключення не має значення). CAN використовує диференційну передачу і внутрішній арбітраж повідомлень, що робить зв’язок стійким до електромагнітних перешкод і зменшує ймовірність втрати пакетів. Однак сам протокол CAN не містить вбудованого шифрування, тому безпека переданих даних обмежена фізичним захистом лінії.[3]

Для високошвидкісної обробки даних (камери, LiDAR, зв’язок з доповненим комп’ютером тощо) застосовують інтерфейси Ethernet або USB, які забезпечують значну пропускну здатність. Зовнішня телеметрія і зв’язок з наземною станцією здійснюється по радіоканалах за протоколом MAVLink. MAVLink – легковажний протокол обміну командами та телеметрією між авіонікою літального апарату та наземною станцією або бортовим комп’ютером. Наприклад, у системі PX4 польотний контролер і допоміжний комп’ютер (mission computer) сполучені через послідовне або мережеве з’єднання, і взаємодіють за MAVLink. [1. 4]

Вибір протоколів та топологій залежить від вимог до затримки й надійності: інтерфейси I²C/SPI можуть опитувати IMU з частотою ~1000 Гц (дані публікуються у внутрішній шину управління з ≈250 Гц), що дає мінімальні затримки в контурі стабілізації. CAN має нижчу швидкість (до 1 Мбіт/с) і невелику затримку при малому навантаженні, але внаслідок арбітражу може додати деяке уповільнення при багатьох вузлах. MAVLink традиційно не використовує шифрування (лише контрольну суму), що створює потенційну вразливість для перехоплення; у безпечних системах це компенсують додатковим шифруванням чи автентифікацією. Таким чином, архітектура обміну даними БПЛА прагне забезпечити баланс між швидкістю реакції керуючого контуру та загальною надійністю та безпекою системи.

1.3. Комунікаційні модулі та канали зв’язку БпЛА

Забезпечення надійного та високошвидкісного зв’язку є критично важливим для ефективного функціонування безпілотних літальних апаратів. Залежно від завдань, умов експлуатації та технічних можливостей, у БПЛА застосовуються різні типи каналів зв’язку та відповідні модулі. Тому важливо знати і розуміти еволюцію цих рішень, їхні сучасні варіанти, технічні характеристики та особливості апаратної реалізації.

1.3.1 Еволюція та сучасні канали зв'язку БПЛА

Раннім етапом розвитку безпілотних систем були аналогові канали зв’язку – прості FM-відеолінки й радіомовлення з обмеженою смугою (~6 МГц) і незначною дальністю. Однак через високу чутливість до шумів і відсутність цифрового стиснення такі лінки мали низьку ефективність спектру. Перехід до цифрових рішень революційно збільшив якість і пропускну здатність каналів. Сучасні системи (напр., цифрові ISR-лінки EnerLinksIII) забезпечують передачу даних до горизонту, при цьому підтримують бітрейти від десятків кбіт/с до десятків Мбіт/с (EnerLinksIII – до 11 Мбіт/с). Цифрові модеми інтегрують стиснення відео (H.264) і багатоканальність, що дозволило в 10 разів збільшити кількість одночасних потоків у тому ж спектрі в порівнянні з аналоговими FM-лінками. Так відбувався поступовий перехід від громіздких аналогових рішень до компактних високошвидкісних цифрових каналів зв’язку зі значно вищою ефективністю.[5]

Сучасні БПЛА використовують різноманітні канали зв’язку залежно від призначення місії та умов середовища.

Радіоканали прямої видимості (LOS) - високочастотні UHF/VHF/C-діапазони з спрямованими антенами. Такі цифрові лінки (напр., модеми Aeronix, EnerLinksIII) забезпечують зв’язок «до горизонту» на десятки кілометрів і передають дані (IP, відео) на швидкостях до 11 Мбіт/с. Вони зазвичай підтримують повнодуплексну передачу і застосовуються для критичних C2- і відеопотоків у польоті.

OFDM/COFDM-системи - цифрові мультиплексовані модеми, що застосовують багатосмугову модуляцію. Стандарти на базі OFDM (наприклад, WiMAX 802.16, DVB, LTE/5G) добре протистоять мультишляху й перешкодам, а також мають високу спектральну ефективність. Наприклад, стандарт IEEE 802.16 забезпечує передачу на рівні 30–40 Мбіт/с на частотах від 2 до 6 ГГц.

Wi-Fi (IEEE 802.11) широко використовувані 802.11n/ac/ax в діапазонах 2.4/5/6 ГГц. Стандарт 802.11ac (Wi-Fi 5) підтримує сумарну пропускну здатність

≥1.1 Гбіт/с (до 500 Мбіт/с на один потік) з дальністю зв’язку у сотні метрів. Ці бездротові LAN-канали зручно використовувати для передачі HD-відео та телеметрії на невеликі відстані (наприклад, для FPV-відео чи поблизького зв’язку з GCS).

Мобільні мережі (4G/5G) - LTE/5G-доступ дає покриття на кілька кілометрів від базової станції і надає високу пропускну здатність. У 4G пікові швидкості сягають сотень Мбіт/с, а сучасні 5G-мережі експериментально досягають 1–5 Гбіт/с з дуже низькою затримкою. Це робить 5G перспективним для управління дронами в урбанізованих районах або реалізації сценаріїв URLLC, де потрібні швидкі реакції.[6]

Супутникові системи зв’язку - геостаціонарні (GEO) і низькоорбітальні (LEO) супутники забезпечують BLOS-з’єднання без обмеження дальності. Наприклад, мережа Starlink (LEO) забезпечує ~3900 супутників з глобальним покриттям і пропускною здатністю до 150 Мбіт/с завантаження, що робить її привабливою для військових і цивільних БПЛА на великих відстанях. Натомість мережі Iridium Certus дають сотні кбіт/с, але працюють будь-де у світі. Серед переваг – незрівнянне покриття, а серед недоліків – потреба у спеціальній антені та значній потужності.

WiMAX/WiBro технології на базі IEEE 802.16e/m для мобільного широкосмугового зв’язку у діапазоні ~3–6 ГГц. Забезпечують стійкий зв’язок на середні дистанції (кілька до десятків км) та швидкість близько 30–40 Мбіт/с. Використовувались як технологія «останньої милі» або проміжного бекхолу для БПЛА у віддалених регіонах.[7]

LPWAN (LoRa/LoRaWAN): енергоефективні мережі в підгігагерцових діапазонах (433, 868, 915 МГц) для телеметрії та IoT. Забезпечують великий радіус (до 2–5 км у місті, понад 10 км у відкритій місцевості) при дуже низькій швидкості (0.3–50 кбіт/с). Перевага – мінімальне енергоспоживання і простота, недолік – надто мала пропускна здатність для мультимедіа, тому LoRa застосовують в основному для передачі статусу та датчиків.

Таким чином, для кожного типу зв’язку існує компроміс між дальністю, пропускною спроможністю і інфраструктурою: високочастотні канали (Wi-Fi, 5G) дають гігабітні швидкості на сотні метрів, а низькочастотні канали (UHF, LoRa, 4G) – кілометрові дистанції при сотнях кілобіт/с. Супутники забезпечують безмежну дальність на шкалі сотень кілометрів чи більше (BLOS), але зі швидкостями від кбіт/с (Iridium) до сотень Мбіт/с (Starlink).

1.3.2 Основні характеристики каналів зв’язку. Комунікаційні модулі та антени.

Порівняння характеристик типових каналів зв’язку показує їхні сильні та слабкі сторони. Наприклад, лінійні LOS-канали (EnerLinksIII) працюють у L/S-діапазонах і мають дальність до горизонту, пропускну здатність до ~10 Мбіт/с – достатню для кількох HD-відеопотоків. Канали Wi-Fi на 5 ГГц забезпечують сотні Мбіт/с при відстанях до ~0.2 км. Стільниковий зв’язок 4G/5G на частотах 0.7–3 ГГц дає покриття до 10–20 км від базової станції і швидкості десятки Мбіт/с (LTE) чи одиниці Гбіт/с (5G). Супутникові канали LEO (Starlink) дають глобальне покриття та швидкість до ~150 Мбіт/с, тоді як LPWAN (LoRa) з підгігагерцовим сигналом зв’язку в радіусі кількох км знімають дуже малу швидкість (~0.3–50 кбіт/с).[8. 9]

Для реалізації цих каналів у БПЛА застосовують апаратні засоби, такі як модеми. Наприклад, Aeronix AerIDM – легкий тактичний модем, що підтримує формат VMF для C2. Система EnerLinksIII HD комбінує цифрове стиснення та передачу HD-відео зі швидкістю до 11 Мбіт/с. Модулі ADLS-2 та інші виконують подібні функції з підтримкою широкосмугових каналів.

Програмно-визначувані радіостанції (SDR) дозволяють гнучко змінювати протоколи і частотні настройки без апаратних змін. Ці SDR-рішення (платформи з ПЛІС/процесорами) використовують у сучасних UAV для підтримки різних стандартів зв’язку одним пристроєм.[10]

Антени - для підсилення зв’язку застосовують кілька типів антен. *Спрямовані антени* (Yagi, параболічні рефлектори тощо) дають високий коефіцієнт підсилення на великих відстанях, але вимагають точного наведення. *Фазовані решітки* можуть електронно формувати та спрямовувати промінь у бік БПЛА без механічного повороту. Наприклад, система Radionor Cordis Array II використовувала фазовану антену для зв’язку з БПЛА Penguin B(рис. 1.2) на відстані ~200 км. *Омоніскусні антени* забезпечують всенапрямлений зв’язок на коротких відстанях (до сотень метрів) і часто використовується як резервний канал зв’язку або для передачі телеметрії. Існують також комбіновані системи, що поєднують кілька антен для одночасної роботи у різних частотних діапазонах.[11]

Під час польоту БПЛА Penguin B використана система Radionor Cordis Array II з електронно-скерованою (фазованою) антеною для підтримки широкосмугового зв’язку на дистанції 200 км

Рисунок 1.2 – БпЛА Penguin B

1.3.3 Технології покращення якості каналу зв’язку

Удосконалення якості зв’язку в сучасних системах досягається за рахунок використання складних технік формування сигналу та обробки.

Адаптивне формування променя (beamforming) - алгоритми на базі фазованих антен скеровують енергію передавача в напрямку БПЛА, що підвищує сигнал/шум і дальність зв’язку. У прикладі з Cordis Array II такий промінь забезпечував надійний зв’язок у русі на відстані сотень кілометрів.

MIMO та MU-MIMO - використання багатьох антен одночасно дозволяє передавати декілька потоків даних паралельно (просторове мультиплексування), збільшуючи пропускну здатність каналу та стійкість до перешкод. Мультікористувацький MIMO (MU-MIMO) дає змогу обслуговувати кілька дронів одночасно на одних частотах, підвищуючи ефективність мережі.

Частотне перескакування - швидка зміна робочої несучої (frequency hopping), як у тактичних лінках (наприклад, Link-16), робить канал стійкішим до перехоплення і перешкод , що особливо важливо у забруднених ефіром ділянках.

Компенсація ефекту Доплера - через швидкий рух дронів відбувається зміщення частоти сигналу на приймачі. Сучасні системи зв’язку застосовують контури відстеження частоти (PLL) і цифрове вирівнювання частотно-часового ходу (напр., OFDM-еквалайзери, OTFS-модуляція) для корекції зсуву Доплера і збереження стабільного зв’язку при великих швидкостях руху.[12]

Кожен з каналів зв’язку має свої характеристики та особливості. Порівняння цих параметрів(табл. 1.1) допоможе визначити сильні та слабкі сторони кожного з них.

Таблиця 1.1

Порівняння типів каналів зв’язку

Тип каналу	**Дальність дії**	**Пропускна здатність (bps)**	**Частотний діапазон**	**Особливості та застосування**
Цифровий LOS-канал	До горизонту (≈20–30 км)	50 кбіт/с – 11 Мбіт/с	L/S-діапазони (0.2–3 ГГц)	Повнодуплексний, для C2 і HD-відео, потребує спрямованих антен

продовження таблиці 1.1

Wi-Fi (802.11ac)	≲0.2 км (5 ГГц)	до ~500 Мбіт/с на потік	2.4/5/6 ГГц	Висока швидкість, широко використовується для HD-відео/телеметрії; мала дальність
Мережі 4G (LTE)	До 10–20 км (макро-базова ст.)	≈50–300 Мбіт/с	700–2600 МГц	Широке покриття, використання комерційних SIM-карт; залежить від покриття мережі
Мережі 5G	≲0.3 км (mmWave) – декілька км (sub-6)	1–5 Гбіт/с	Sub-6 ГГц і ммWave (24–40 ГГц)	Дуже низька затримка, велика ємність мережі; потребує нових станцій та обладнання
Супутниковий (LEO, Starlink)	Військовий BLOS	до ~150 Мбіт/с	Ka-/Ku-діапазони (≥20 ГГц)	Глобальне покриття, висока пропускна здатність; висока вартість термінала, затримка ~20 мс
Супутниковий (LEO, Iridium)	«Світовий» зв’язок	~≤100 кбіт/с	L-діапазон (~1.6 ГГц)	Максимальне покриття земної кулі, дуже низька швидкість; стійкий і малопомітний зв’язок

продовження таблиці 1.1

WiMAX (802.16)	5–10 км (у місті), до 50 км LOS	30–40 Мбіт/с	2–6 ГГц	Широке покриття в місті/селі, використовувався для фіксованого широкосмугового доступу; потребує інфраструктури
LoRaWAN (LPWAN)	2–5 км (урбана зона), >10 км LOS	0.3–50 кбіт/с	433/868/915 МГц	Наднизька енергія, застосовується для телеметрії та датчиків; надмала швидкість, не підходить для передачі відео

1.4. Особливості роботи станції оператора та бортових систем

Ефективне функціонування безпілотного літального апарата базується на тісній взаємодії між його бортовими системами та станцією оператора. Бортові модулі забезпечують автономність, стабільність та здатність виконувати поставлені завдання в повітрі, тоді як наземна станція виступає координаційним центром для керування польотом, обміну даними та прийняття рішень у режимі реального часу.

1.4.1 Опис бортових систем БПЛА

Сучасний БПЛА складається з кількох ключових бортових модулів. Контролер польоту (автопілот) – це центральна апаратна плата, яка керує двигунами дрона, взаємодіє з датчиками і реалізує оцінку положення, навігацію

та підтримує керування польотом. Зазвичай автопілоти базуються на 32-розрядних мікропроцесорах (ARM, Atmel) і мають стандартні інтерфейси (CAN, PWM, UART) для під'єднання електронних контролерів двигунів (ESC) та датчиків. Навігаційна система БПЛА включає інерціальний вимірювальний блок (IMU) – акселерометри та гіроскопи (іноді з магнітометрами) для оцінки кута крену/тангажу, барометр для визначення висоти і супутниковий модуль GNSS (GPS/GLONASS/Galileo/BeiDou) для глобального позиціювання. Дані з IMU та GNSS фільтруються (наприклад, фільтром Калмана) для точної оцінки місцезнаходження та орієнтації.

Комунікаційні модулі забезпечують зв'язок з наземним пунктом керування та іншими БПЛА: це передусім радіотелеметрія (напр. на частотах 433 МГц, 915 МГц або 2.4 ГГц з протоколом MAVLink), а також дедалі частіше LTE/5G модеми та супутникові передавачі для передачі команд (C2) і відеопотоку. Камери та сенсори (оптичні, тепловізійні, LiDAR, мультиспектральні тощо) збирають зображення та дані оточення; більшість камер встановлені на 3-осьових гімах (стронґреалізованих підвісах) для стабілізації зображення. Системи стабілізації включають як механічні гіми й програмні алгоритми автопілоту, що згладжують рух БПЛА. Бортовий комп'ютер (companion computer) на базі Linux (наприклад, Raspberry Pi, NVIDIA Jetson, Intel NUC) може обробляти великі об'єми даних і застосовувати алгоритми розпізнавання чи планування в реальному часі.

Контролер польоту (автопілот) - основна плата з 32-бітним процесором, що керує двигунами та оброблює дані з датчиків для утримання курсу і висоти.

Навігаційна система - поєднує IMU (акселерометр, гіроскоп, магнітометр) для оцінки орієнтації та барометр для висоти, а також GNSS (GPS, GLONASS, Galileo, BeiDou) для глобального позиціювання.

Комунікаційні модулі - радіомодулі телеметрії (C2) із протоколом MAVLink для зв'язку з GCS; при цьому сучасні дрони можуть доповнюватися 4G/5G модемами або супутниковим зв'язком для BVLOS-польотів та передачі високоякісного відео.

Камери і сенсори - оптичні (RGB/відеокамери), тепловізійні, LiDAR, радіолокаційні та інші сенсори для збору даних про ціль і оточення; часто встановлені на стабілізованих гімбалах.

Системи стабілізації - механічні тривісні гіми для камери та ПЗ-алгоритми автопілоту, які забезпечують плавний і стабільний політ.

Бортовий комп'ютер - додатковий обчислювальний блок на базі Linux (напр., Raspberry Pi, NVIDIA Jetson) для виконання обробки відео, збору даних і розв'язання завдань ШІ.

1.4.2 Типова архітектура навігаційної системи

БПЛА зазвичай використовують інерційну навігацію (INS), що поєднує IMU із GNSS-модулями. Дані з акселерометрів, гіроскопів і супутникових приймачів зводяться разом фільтром Калмана для стабільного визначення положення і орієнтації в реальному часі. Барометр і магнітометр допомагають уточнити висоту та азимут курсу. Управління польотом здійснюється через канали PWM (керування ESC) і MAVLink-команди: автопілот генерує сигнали на ESC для регулювання швидкості двигунів та утримання кута крену/тангажу/курсоу, а коригування маршруту може надходити від GCS шляхом передачі команд польоту (waypoints). Таким чином, типова архітектура включає GNSS + INS + барометр/компас із програмним об'єднанням даних (фільтр Калмана) та інтерфейсами управління польотом (напр. PWM, UART).

1.4.3 Станція оператора (Ground Control Station, GCS)

Наземна станція управління – це центральний пункт керування дроном. Вона забезпечує розробку і завантаження плану польоту, відображення телеметрії (висота, швидкість, АКБ тощо), прийом відеопотоків і відправку команд управління. GCS обладнується комп'ютером чи планшетом з софтом для місійного планування, контролером (джойстиком або паралельно – мобільним

додатком), телеметричною радіостанцією та антеною. Функції GCS включають візуалізацію 2D/3D-карт місцевості, створення маршрутів з точками-прив’язками, реєстрацію польотних логів і моніторинг стану БПЛА в реальному часі.

Типові конфігурації GCS:

Стаціонарна наземна станція - має стаціонарну консоль із кількома HD-дисплеями, широким польотом огляду та спрямованою антеною. Використовується на базах і в лабораторіях (часто для великих систем, напр., Predator/Reaper), де ергономіка робочого місця (релаксовані крісла, регульовані монітори) і висока ситуаційна обізнаність є критичними.

Мобільна GCS - монтується в автомобіль чи на мобільний пункт; складається з ноутбука/планшета та антени на телескопічній стійці. Забезпечує надійну роботу в польових умовах при пересуванні (наприклад, для тактичних чи інспекційних місій).

Портативна GCS - легкі рішення на основі смартфона, планшета або портативного контролера (з вбудованими передавачем і екраном). Зазвичай використовується для простих/споживчих БПЛА або в екстрених ситуаціях завдяки максимальній мобільності.

Системи на інших платформах - GCS, інтегровані в інші транспортні засоби (корабель, літак, інші БПЛА), коли управління проводиться з нестандартного місця (наприклад, керування морським дрона-комплексом з корабля).[13]

1.4.4 Порівняння популярного програмного забезпечення для GCS

Mission Planner - безкоштовний GCS для автопілотів ArduPilot (Plane, Copter, Rover) під ОС Windows. Підтримує прошивку контролера, налаштування і калібрування системи. Дозволяє планувати місії зі створенням waypoint’ів на онлайн-картах (Google Maps та ін.), зберігати/завантажувати польотні плани, а також вести аналіз телеметрії та реєстрацію FPV-відео під час польоту.[14]

QGroundControl - відкрите кросплатформне ПЗ (Windows, Mac, Linux, iOS, Android) для MAVLink-дронів. Підтримує автопілоти PX4 і ArduPilot (і будь-які інші, що говорять MAVLink). Забезпечує інтуїтивне планування місій, візуалізацію 3D-карт, моніторинг телеметрії та вивід відеопотоку з борту. QGroundControl активно розвивається спільнотою і надає зручний користувацький інтерфейс для обох — початківців та профі.[15]

UgCS (Universal GCS) - комерційне програмне забезпечення з 3D-інтерфейсом і гнучкими можливостями планування. Підтримує ArduPilot (APM/Pixhawk) та деякі інші платформи (включно з DJI, Mikrokopter тощо). Дозволяє одночасно керувати кількома БПЛА, імпортувати цифрові моделі висот (DEM) для польотів з урахуванням рельєфу, підтримує ADS-B, «Click&Go» тощо. Має вбудований плеєр телеметрії та функції створення зон No-Fly. Програма працює на Windows, Mac і Linux (Ubuntu) і орієнтована як на ентузіастів, так і на професійні рішення.

DJI Pilot 2 / Ground Station Pro - фірмові додатки для керування комерційними безпілотними комплексами DJI (серії Matrice, Mavic 2 Enterprise тощо). DJI Pilot 2 — це мобільний застосунок (Android/RC), а DJI GS Pro — iPad-додаток. Обидва забезпечують автоматизоване планування польотів, 3D-моделювання місії й управління командою зберігання даних у хмарі (DJI FlightHub 2). ПЗ DJI підтримує лише власні автопілоти DJI і не сумісне з відкритими контролерами (ArduPilot/PX4).[16]

Сучасні GCS можуть одночасно використовувати кілька каналів зв’язку (радіо, LTE/5G, супутниковий) для передачі команд (C2) і відеопотоку. При цьому інтерфейс оператора проектується з урахуванням ергономіки та ситуаційної обізнаності: застосовуються великі HD-екрани і HUD, інтуїтивні елементи керування (джойстики, кнопкові панелі) і 3D-візуалізація маршрутів. Все це спрямовано на зменшення навантаження оператора, покращення прийняття рішень і безпеку виконання місій.

Висновки за розділом 1

У першому розділі дослідження детально розглянуто різні аспекти функціонування БПЛА та їхніх комунікаційних систем. Описано основні типи безпілотників і критерії їх класифікації, структуру системи управління і архітектуру обміну даними, а також компоненти комунікацій і особливості роботи наземної станції оператора й бортових систем.

Класифікація БПЛА (підрозділ 1.1): виявлено, що безпілотні літальні апарати поділяються на категорії за льотною масою, дальністю та тривалістю польоту, типом крила і галуззю застосування. Також розрізняють призначення апаратів (комерційне, громадське, військове тощо), що узагальнює існуючі моделі та міжнародні стандарти (UVSI, NATO) щодо систем БПЛА.

Структура системи управління (підрозділ 1.2): встановлено, що сучасний БПЛА являє собою складну модульну систему. Він складається з живильної установки (силової), бортового комп'ютера (автопілота) з різноманітними датчиками, навігаційної системи та виконавчих механізмів. Наземна станція оператора взаємодіє з бортовим комп'ютером через двонаправлені канали зв'язку, передаючи команди керування і приймаючи телеметричні дані. Така архітектура підкреслює важливість синхронної роботи всіх компонентів для успішного виконання польоту.

Комунікаційні модулі та канали (підрозділ 1.3): проаналізовано ключові модулі зв'язку – радіоприймачі/передавачі з вбудованими модемами (ADT) і антени – і їхні ролі. Система зв'язку створює двосторонні канали: uplink для передачі команд управління та downlink для телеметрії та даних корисного навантаження (наприклад, відео). До складу типового ADT входять радіоприймач, передавач і модем, що зв'язують цей комплекс з іншими підсистемами БПЛА. Для забезпечення різних потреб використовують різні частоти – від UHF/VHF для команд і телеметрії до C- та Ku-діапазонів (а також мобільні мережі чи супутниковий зв'язок) для передавання даних, що додає

архітектурній складності системи.Станція оператора та бортові системи (підрозділ 1.4): розглянуто функції наземної станції (GCS) і бортових систем.

Станція оператора відповідає за планування місії, передачу команд і прийом телеметрії, використовуючи персональний комп’ютер або пульт з відповідним програмним забезпеченням. Бортові системи обробляють інформацію з датчиків, виконують навігаційні розрахунки й безпосередньо управляють виконавчими механізмами. Таким чином, показано взаємодію наземного і повітряного сегментів: ефективне управління БПЛА забезпечується через чітко налагоджений обмін даними між цими рівнями.

Отже, проведений аналіз показує багаторівневу й модульну структуру безпілотних систем та високу складність їхніх комунікацій. Різноманітність типів БПЛА і конфігурацій каналів зв’язку підкреслює необхідність комплексного підходу до забезпечення надійного управління польотом і обміну даними. Актуальність подальшого дослідження зосереджена на аналізі можливих загроз (глушіння, спуфінг, перехоплення тощо) та розробці заходів захисту, що спираються на отримані висновки про особливості систем зв’язку БПЛА.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ЗАГРОЗ БЕЗПЕКИ КАНАЛІВ ЗВ'ЯЗКУ ТА МЕТОДИ ЇХ НЕЙТРАЛІЗАЦІЇ

2.1. Основні типи загроз у сфері БпЛА: радіоелектронні та кібернетичні

Функціонування безпілотних літальних апаратів безпосередньо залежить від стабільності каналів зв'язку, навігації та обміну даними. Уразливість цих каналів відкриває широкий спектр можливостей для реалізації як радіоелектронних, так і кібернетичних атак. Дані типи загроз відіграють ключову роль у гібридних конфліктах, протидії розвідувальній діяльності або у випадках порушення критичної інфраструктури, де застосовуються БпЛА.

2.1.1 Радіоелектронні загрози каналам зв'язку БпЛА

Радіоелектронні загрози становлять одну з найбільш серйозних та актуальних небезпек для безпілотних літальних апаратів, особливо в умовах ведення бойових дій, розвідувальних операцій або у зоні контролю ворожих РЕБ-комплексів. Такі загрози реалізуються за рахунок навмисного впливу на електромагнітне середовище функціонування БпЛА з метою порушення його нормальної роботи або виведення з ладу каналів управління, зв'язку та навігації.

Радіоелектронні загрози базуються на застосуванні електромагнітного випромінювання, яке створює завади або впливає на роботу радіоелектронних засобів, що забезпечують функціонування БпЛА. Основні цілі такого впливу:

порушення каналів управління та зв'язку — створення умов, за яких БпЛА втрачає контакт із наземною станцією, що може призвести до аварійного приземлення або втрати апарата;

зрив прийому сигналів супутникової навігації (GPS/GNSS) — блокування або фальсифікація координат з метою дезорієнтації апарата;

розвідка та перехоплення даних — отримання інформації про параметри сигналів, канали зв’язку або маршрути польоту;

введення в оману — симулювання сигналів управління або навігації для спотворення функціонування БпЛА;

Радіоелектронні загрози умовно поділяються на такі категорії за функціональним призначенням – РЕП, РЕР та :

Радіоелектронне подавлення (РЕП) - це основний інструмент активного впливу на БпЛА. Метою РЕП є виведення з ладу або значне ускладнення роботи каналів:

командного управління – перешкоди на частотах, які використовуються для передачі команд на БпЛА;

телеметрії та відео – блокування передачі даних від БпЛА до оператора;

супутникової навігації – глушіння GPS-сигналу, особливо в L1/L2 діапазонах.

Методи РЕП реалізуються через активне випромінювання завадових сигналів, які накладаються на корисні сигнали або замінюють їх, що призводить до деградації сигнал/шум (SNR) на приймальному боці.

Радіоелектронна розвідка (РЕР) є інструментом збору інформації та аналізу електромагнітного випромінювання БпЛА з метою визначення частот роботи та протоколів обміну, виявлення місцеположення та ідентифікації цілі підготовки до застосування точних завадових впливів. РЕР зазвичай передує застосуванню РЕП, оскільки дозволяє виявити параметри, які підлягають ураженню.

Хоча пасивні завади не створюють активного випромінювання, вони можуть використовуватись для маскування об'єктів від радіолокаційних БпЛА або введення в оману систем виявлення через створення хибних цілей (наприклад, за допомогою дипольних або кутникових відбивачів).

Такі методи актуальні в оборонних сценаріях, де важливо захистити критичні об'єкти або дезорієнтувати розвідувальні апарати противника.

Активні завади — основний компонент РЕП — класифікуються за способом дії та спектральною характеристикою. За способом дії:

постійні (constant jamming) – безперервне випромінювання сигналу, що перекриває частоту каналу. Найбільш енерговитратний спосіб, але ефективний для придушення фіксованих каналів;

реактивні (reactive jamming) – випромінювання відбувається лише при виявленні активного сигналу цілі. Енергоефективний метод, складний для виявлення та блокування.;

періодичні/випадкові (periodic/random jamming) – сигнали створюються з перервами, що дозволяє зменшити витрати енергії, створити ілюзію нестабільного середовища

зі змінною частотою (frequency sweeping) – постійна зміна частоти завадового сигналу з метою охоплення більшої частини діапазону та ускладнення адаптації каналів зв’язку БпЛА.

За спектральною характеристикою:

вузькосмугові (spot jamming) – точкове блокування визначеної частоти, що дозволяє сконцентрувати енергію і знизити витрати. Потребує точної інформації про частоти цілі (отримується через РЕР);

широкосмугові (barrage jamming) – масове блокування широкого спектру частот, застосовується для зриву роботи всіх можливих каналів. Вимагає значних енергетичних ресурсів і ефективна проти мультичастотних систем.

Уразливість безпілотних систем до радіоелектронних загроз залежить від:

протоколів зв’язку та навігації – системи з фіксованою частотою або відсутністю шифрування є легкою мішенню;

потужності сигналу та чутливості приймача – низький рівень сигналу робить систему вразливою до навіть помірних завад;

пикористання GPS без резервного позиціонування – створює залежність від одного типу навігації, яку можна легко зруйнувати;

підсутності анти-РЕБ заходів – відсутність резервних каналів або технологій адаптації (наприклад, frequency hopping) підвищує ризик втрати керування.[17]

2.1.2 Кібернетичні загрози каналам зв’язку та системам БпЛА

Кібернетичні загрози є одними з найнебезпечніших для систем безпілотних літальних апаратів, оскільки вони здатні впливати не лише на передавання інформації, а й на саме функціонування апарата, наземної станції керування (GCS) та інфраструктури обміну даними. В умовах сучасної гібридної війни чи терористичної діяльності, коли БпЛА використовуються як у військових, так і в цивільних цілях, атаки в кіберпросторі стають критичним інструментом впливу на противника. Уразливості, притаманні протоколам зв’язку, апаратному забезпеченню та програмному коду, роблять системи БпЛА привабливою ціллю для кібератак.

Кібернетичні загрози умовно поділяються на основні категорії:

Атаки на конфіденційність спрямовані на несанкціонований доступ до чутливої інформації, що передається або зберігається в системах БпЛА. Наприклад, розвідувальні дані, координати маршруту, криптографічні ключі чи відеопотоки можуть бути перехоплені внаслідок слабкого шифрування або повної його відсутності. Часто використання відкритих протоколів (зокрема MAVLink без захисту) відкриває шлях до пасивного прослуховування каналів зв’язку між апаратом і GCS.

Атаки на цілісність – зловмисник модифікує передані або збережені дані, змінює конфігурації системи або впроваджує шкідливий код. Це може призвести до маніпуляції траєкторією польоту, видачі хибних команд або викривлення інформації, яку отримує оператор. Наприклад, зміна координат у телеметричному пакеті може направити БпЛА у небезпечну зону або змусити його приземлитися в зоні, контрольованій противником.

Атаки на доступність (DoS / DDoS) спрямовані на виведення з ладу або перевантаження систем управління, зв’язку чи обробки даних. Вони можуть реалізовуватися через масові запити до GCS або мережевого шлюзу, що унеможливлює нормальний обмін інформацією між оператором та БпЛА. Наслідком може стати втрата контролю над апаратом, відмова в управлінні або аварійне завершення польоту.

Наземна станція є критичним вузлом управління, тому її компрометація відкриває зловмиснику повний контроль над БпЛА. Через соціальну інженерію, фішинг, використання вразливостей операційної системи або вразливостей ПЗ для керування можна впровадити шкідливе ПЗ, перехопити сеанси зв’язку або викрасти облікові дані оператора.

Ін’єкція команд (Command Injection) - тип атак, що полягає у навмисному вставленні або підміні команд управління в протоколах зв’язку, особливо коли не реалізовано криптографічного захисту. Зловмисник може, наприклад, подати команду на зміну маршруту, примусову посадку або навіть знищення апарата.

Атаки на оновлення програмного забезпечення (Firmware Attacks) - шкідливе або скомпрометоване оновлення прошивки апарата або GCS дозволяє зловмиснику впровадити бекдори або інші форми шпигунського/руйнівного коду. Особливо небезпечно, коли оновлення не перевіряються за цифровими підписами або завантажуються з неперевірених джерел.

Навіть без активного втручання у роботу системи, зловмисник може отримати цінну інформацію, яка використовується для подальших атак. Наприклад, аналіз трафіку дозволяє ідентифікувати типи протоколів, структуру команд, частотні діапазони, тощо. Ця інформація часто використовується як перший етап складнішої багатовекторної атаки.

Більшість сучасних БпЛА використовують відкриті або напіввідкриті протоколи зв’язку – наприклад, MAVLink, які спочатку розроблялися без належного рівня захисту. Унаслідок цього: дані передаються у відкритому вигляді; відсутня автентифікація команд; не передбачено перевірки цілісності пакетів.

Це створює передумови для ін’єкцій, перехоплення або підміни команд. Інші часто використовувані протоколи – Wi-Fi, LTE, Zigbee – також можуть бути вразливими через застарілі налаштування безпеки, погано реалізоване шифрування або відкриті порти.[17]

Дедалі частіше атаки на БпЛА набувають комбінованого характеру. Наприклад, створення радіоперешкод змушує систему перемкнутися на незахищений канал, що відкриває вікно для кібератаки. Успішна кібератака на наземну станцію може, у свою чергу, надати зловмиснику повний набір частот та ключів для запуску РЕБ-операції.

2.2. Актуальні приклади атак на канали керування безпілотниками

З активізацією використання БПЛА в цивільному секторі, логістиці, аграрному моніторингу, нагляді, а особливо в зоні бойових дій, вони дедалі частіше стають об’єктом атак. У сучасних умовах канали керування розглядаються як «вузьке місце» в архітектурі БПЛА, яке найпростіше вивести з ладу або використати для отримання контролю над апаратом. Особливо яскраво це проявляється у війні в Україні, де сторони конфлікту активно використовують засоби радіоелектронної боротьби (РЕБ), глушіння GPS та спуфінг для нейтралізації ворожих дронів. Як свідчить практика, на багатьох ділянках фронту розгортання РЕБ-комплексів стало стандартною тактикою захисту від БПЛА.

Ще один аспект — "демократизація" атакувальних технологій. Завдяки широкій доступності програмно-визначуваних радіосистем (SDR), таких як HackRF One або BladeRF, та відкритого ПЗ для аналізу радіочастот (GNU Radio, GQRX), навіть непрофесійні користувачі здатні розробити інструменти для глушіння, перехоплення чи спуфінгу. Крім того, пристрої на кшталт Wi-Fi Pineapple, призначені спочатку для тестування безпеки, масово використовуються для атак на бездротові канали комерційних БПЛА. Це

створює ситуацію, коли навіть дешеві дрони стають легкою ціллю, якщо не мають належного рівня захисту.

Радіоелектронне глушіння каналів керування та навігації - це одна з найпростіших і водночас найефективніших форм атаки. Суть полягає у створенні радіозавад на частотах, на яких функціонує канал зв’язку між оператором і дроном. Наприклад, частоти 2.4 ГГц та 5.8 ГГц, які масово використовуються у комерційних БПЛА, легко заглушити широкосмуговими генераторами шуму.

У реальних умовах застосовуються як ручні системи глушіння (наприклад, "антидрон-рушниці"), так і стаціонарні або мобільні РЕБ-комплекси. Один із прикладів — українська система К-1000, яка створює "купол" із завад на критичних частотах управління FPV-дронами, порушуючи як передачу команд, так і відео.

Оскільки GPS-сигнал є дуже слабким (близько -130 дБм на вході приймача), його надзвичайно просто заглушити. Наприклад, достатньо сигналу завади потужністю всього 30–100 мВт для того, щоб позбавити дрон орієнтації. У таких умовах дрон не зможе виконувати автономну навігацію або повернутися на базу, особливо якщо RTH-функція пов’язана саме з GPS.

Типи завад:

Загороджувальні (Barrage Jamming) - створення широкосмугових перешкод, що охоплюють весь спектр. Ефективні, але енерговитратні.

Прицільні (Spot Jamming) - точкове глушіння однієї частоти або вузького діапазону. Потребує знання частотної характеристики цілі.

Маскувальні шумові завади - імітація природного шуму або фонових сигналів. Мета — зробити сигнал управління "невидимим" для приймача.

Інтелектуальні завади - аналізують сигнал та формують заваду, яка максимально ефективна для конкретного типу модуляції або протоколу (наприклад, для DSSS або FHSS).

Наслідки атак:

- Втрата зв’язку з оператором.
- Втрата GPS-навігації.

- Активація аварійного режиму (RTH, зависання, посадка).
- Повна або часткова втрата керованості.
- Ймовірне перехоплення або знищення БПЛА.

Кібернетичні атаки на канали керування Хоча РЕБ є найпоширенішим засобом протидії дронам, кібернетичні атаки не менш небезпечні, а подекуди ще ефективніші. Зловмисники можуть отримати контроль над БПЛА або заблокувати його роботу без застосування фізичних засобів глушіння.

Перехоплення управління. Одним із найрезонансніших прикладів є випадки, коли дрони DJI були "перемкнені" на інший пульт через вразливості у протоколах автентифікації. Такі атаки можливі у випадку використання незашифрованих або слабко захищених каналів передачі. Зловмисник з SDR або спеціалізованим приймачем перехоплює сигнал, аналізує команди, імітує оригінального оператора — і під’єднується як "головний" користувач.

Спуфінг GPS. Інша категорія атак — це навмисне підміщення фальшивих GPS-сигналів. Відомо, що дрони, не маючи альтернативи GPS, довіряють координатам, які надходять від супутників. Таким чином, зловмисник може змусити дрон змінити маршрут або приземлитися в зазначеній ним точці. Прикладом є дослідження НТЦ "Інститут спеціальної техніки і зв’язку", яке демонструє спуфінг GPS дронів із відхиленням координат на десятки метрів.

Атаки типу "man-in-the-middle" (MITM). Уразливі протоколи зв’язку дозволяють атакуючому стати "посередником" між дроном і оператором. Він може читати, змінювати або блокувати команди. Такий сценарій може реалізовуватися при використанні Wi-Fi або мобільного зв’язку (LTE), особливо якщо не застосовано додаткового шифрування.

Експлуатація вразливостей комунікаційних протоколів (наприклад, MAVLink) - протоколи типу MAVLink часто не мають шифрування та надійної автентифікації, що дозволяє зловмисникам змінювати параметри польоту, підмінювати або повторювати команди. Серед вразливостей — атаки типу DoS, командні ін'єкції, "inaccurate bounds" тощо. Приклад: надсилання MISSION_COUNT може стерти маршрут, ICMP-флуд — викликати failsafe.

Наслідки — зависання, збій, виконання шкідливих команд, захоплення керування.

Атаки на ПЗ та прошивки - шкідливий код може бути впроваджено через вразливості в ПЗ або під час оновлення прошивки. Основні проблеми — відсутність перевірки автентичності, вразливості нульового дня, слабкий захист від модифікацій. Наслідки — зміна логіки польоту, бекдори, повна компрометація керування.

SkyJack — атака, що дозволяє перехопити керування дроном Parrot AR.Drone через Wi-Fi.

WiFi Pineapple — пристрій, що дозволяє створювати фальшиві точки доступу та змушувати дрони підключатися до них.

BlueDrone — демонстрація Bluetooth-атаки на системи, які використовують BLE-зв’язок.[17]

Загалом, атаки на канали керування БПЛА є не лише технічно можливими, але й уже широко реалізуються як у конфліктах державного рівня, так і в локальних інцидентах. Їх реалізація варіюється від грубого радіоглушіння до тонких кібероперацій. Проблема ускладнюється масовим використанням комерційних дронів із обмеженим захистом та широкою доступністю засобів атаки. Як наслідок, підвищення стійкості каналів керування — один із пріоритетів у розвитку БпЛА, особливо у військовому застосуванні.

2.3. Аналіз методів несанкціонованого втручання

Несанкціоноване втручання в канали керування безпілотних літальних апаратів здійснюється за допомогою методів, що належать до двох раніше визначених основних категорій: радіоелектронне придушення, яке використовує електромагнітну енергію для порушення функціонування каналів, та кібератаки, що експлуатують вразливості програмного забезпечення, протоколів і апаратних компонентів. Часто ці методи комбінуються для досягнення максимальної ефективності.

2.3.1 Методи радіоелектронного придушення

Радіоелектронний вплив на канали керування БПЛА використовує два основні механізми: пригнічення сигналу переважною потужністю та фальсифікацію змісту сигналу.

Перший механізм, пригнічення сигналу переважною потужністю, полягає у створенні в радіоефірі електромагнітного випромінювання, енергетичні характеристики якого (зокрема, потужність) значно перевищують аналогічні характеристики корисного сигналу на вході приймача БПЛА або наземної станції керування (НСК). Це призводить до критичного погіршення співвідношення сигнал/шум (SNR) або сигнал/завада (SIR), унеможливлюючи коректну демодуляцію та декодування інформації, що передається. Реалізація цього механізму здійснюється за допомогою шумових завад різного типу: загороджувальні (широкосмугові) завади створюють високий рівень шуму в широкому діапазоні частот, що перекриває весь робочий спектр системи зв'язку БПЛА, тоді як прицільні (вузькосмугові) завади концентрують енергію в вузькій смузі частот, що відповідає конкретній несучій частоті каналу керування.

Ефективність таких завад проти сучасних протоколів зв'язку (наприклад, FHSS, DSSS, OFDM) залежить від здатності завади перекрити використовуваний спектральний ресурс або адаптуватися до динамічної зміни параметрів сигналу. Важливо, що цей механізм впливає на фізичний рівень передачі, тому шифрування корисного сигналу не забезпечує захисту від його енергетичного придушення.

Другий механізм, фальсифікація змісту сигналу (дезінформаційний вплив), спрямований на введення в оману систем керування та навігації БПЛА. Це досягається шляхом генерації та випромінювання сигналів, які за своїми параметрами (частота, модуляція, структура) максимально точно імітують легітимні сигнали, але містять заздалегідь сформовану хибну або спотворену

інформацію. Така фальсифікація може стосуватися як команд керування, так і навігаційних даних.

Прикладом є імітаційні завади, що надсилають хибні команди (зміна курсу, висоти, повернення до невірної точки) або спотворені телеметричні дані, та спуфінг сигналів глобальних навігаційних супутникових систем (GNSS), де БПЛА "нав'язуються" неправдиві координати, швидкість або час. Успішна реалізація цього механізму вимагає не лише здатності генерувати радіосигнали потрібної структури, але й потенційно глибокого розуміння протоколів зв'язку та логіки роботи цільової системи БПЛА.[18]

2.3.2 Методи кібернетичних атак

Кібернетичний вплив використовує логічні недоліки та вразливості в інформаційних системах БПЛА та НСК.

Один з ключових механізмів – експлуатація конструктивних недоліків та вразливостей комунікаційних протоколів. Багато стандартних (наприклад, Wi-Fi) та спеціалізованих (наприклад, MAVLink) протоколів, що використовуються в БПЛА, можуть мати слабкості в реалізації механізмів шифрування, автентифікації сторін обміну та забезпечення цілісності даних, або ж ці механізми можуть бути опціональними чи некоректно налаштованими. Це дозволяє зловмисникам реалізовувати атаки, спрямовані на пасивне перехоплення даних (eavesdropping), активне втручання в інформаційний потік (Man-in-the-Middle, ін'єкція або модифікація пакетів, атаки повтору), або викликати відмову в обслуговуванні на рівні протоколу.

Інший фундаментальний механізм – експлуатація вразливостей програмного та апаратного забезпечення. Програмний код операційних систем, прошивок (firmware) БПЛА та його компонентів (контролер польоту, приймач, сенсори), а також програмного забезпечення НСК, може містити помилки (наприклад, переповнення буфера, логічні помилки), які створюють вразливості. Їх експлуатація дозволяє зловмиснику ін'єктувати та виконувати шкідливий код,

підвищувати свої привілеї в системі, модифікувати конфігураційні параметри, обходити захисні механізми або отримувати несанкціонований доступ до критичних функцій керування та даних. Вразливості в механізмах оновлення ПЗ або незахищені фізичні інтерфейси (JTAG, UART, USB) також є поширеними векторами для компрометації.

Третій механізм – маніпуляція довірою до сенсорних даних та зовнішніх систем. Системи керування БПЛА часто покладаються на дані, отримані від бортових сенсорів (акселерометри, гіроскопи, магнітометри, барометри, LiDAR) та зовнішніх систем (наприклад, GNSS). Якщо ці дані не проходять належну валідацію та перевірку на достовірність, зловмисник може спробувати їх спотворити або підмінити. Найбільш відомим прикладом є GNSS-спуфінг, але теоретично можливі атаки і на інші типи сенсорів, що призводять до неадекватної оцінки БПЛА власного стану або навколишнього оточення і, як наслідок, до несанкціонованої зміни його поведінки або траєкторії.[18]

2.3.3 Методи комбінованих та багатовекторних атак

Комбінований вплив реалізується через принцип синергетичного посилення ефекту атаки**,** який полягає у цілеспрямованому поєднанні радіоелектронних та кібернетичних методів для досягнення результату, недосяжного або значно ускладненого при їх окремому застосуванні. Один тип впливу використовується для створення "вікна можливостей" або полегшення реалізації іншого. Наприклад, радіоелектронне придушення основного захищеного каналу зв'язку може змусити систему БПЛА перейти на резервний, менш захищений канал, який потім стає об'єктом кібератаки. Або ж, кібератака на НСК може дозволити отримати критично важливу інформацію про параметри каналів зв'язку БПЛА (частоти, ключі шифрування, особливості протоколів), що значно підвищить точність та ефективність подальшого радіоелектронного придушення. Фізичне виведення БПЛА з ладу або примусова посадка за допомогою РЕБ може передувати фізичному доступу до апарата з метою аналізу

його систем та вилучення даних або впровадження шкідливого ПЗ. Таким чином, розуміння механізмів комбінованого впливу є критичним для побудови комплексної системи захисту.[18]

2.4. Підходи до забезпечення стійкості каналів зв’язку

Забезпечення стійкості каналів зв'язку безпілотних літальних апаратів вимагає застосування багатоаспектної стратегії, що охоплює апаратні, протокольні, алгоритмічні та інтелектуальні рішення, а також їх комплексну інтеграцію.

Апаратні підходи - спрямовані на підвищення фізичної стійкості каналів зв'язку до зовнішніх впливів, зокрема до засобів радіоелектронної боротьби (РЕБ).

Адаптивні антенні решітки та технології формування променя (Beamforming) - використання решіток дозволяє динамічно керувати діаграмою спрямованості антени. Технологія формування променя концентрує енергію випромінювання в напрямку легітимного кореспондента (наприклад, наземної станції керування – НСК) та/або формує нулі діаграми спрямованості в напрямках джерел завад. Це призводить до значного покращення співвідношення сигнал/завада (Signal-to-Interference-plus-Noise Ratio, SINR), підвищення стійкості до прицільних завад та зменшення ймовірності перехоплення (Low Probability of Intercept, LPI) і виявлення (Low Probability of Detection, LPD) сигналу.

Системи MIMO (Multiple-Input, Multiple-Output) також сприяють покращенню пропускної здатності та надійності. Перспективним доповненням є інтелектуальні відбиваючі поверхні (Intelligent Reflecting Surfaces, IRS), які можуть пасивно керувати поширенням радіохвиль для покращення якості сигналу та обходу перешкод.

Диверсифікація каналів зв'язку за частотними діапазонами та фізичними принципами передачі даних є ключовим елементом підвищення відмовостійкості.

Міліметрові хвилі (mmWave): діапазони частот від 30 до 300 ГГц пропонують широкі смуги пропускання, що дозволяє досягати високих швидкостей передачі даних. Вузька спрямованість антен на цих частотах та значне атмосферне поглинання (особливо на певних частотах, наприклад, навколо 60 ГГц) забезпечують природні властивості LPI/LPD. Однак, ці ж фактори обмежують дальність зв'язку та підвищують чутливість до атмосферних умов (дощ, туман). Сучасні дослідження спрямовані на подолання цих обмежень та розробку ефективних систем формування променя для mmWave.

Оптичні лінії зв'язку (Free Space Optics, FSO) - передача даних за допомогою лазерного випромінювання в атмосфері забезпечує надзвичайно високу пропускну здатність (терабіти на секунду) та повну невразливість до радіочастотних завад. Основними викликами є необхідність точного наведення, захоплення та супроводу (Pointing, Acquisition, and Tracking, PAT) між передавачем та приймачем, особливо для мобільних платформ, а також чутливість до атмосферних умов (туман, хмари, опади, турбулентність). Досліджуються методи адаптивної оптики, використання модулюючих ретро-рефлекторів (MRR) та диференціального детектування для підвищення надійності.

Супутниковий зв'язок (Satellite Communication, SATCOM) забезпечує зв'язок на великих відстанях, за межами прямої видимості (Beyond Line of Sight, BLOS). Основні діапазони – L, Ku, Ka. Вразливості включають можливість постановки завад на висхідних та низхідних лініях, а також спуфінг супутникових сигналів. Для підвищення безпеки застосовуються VPN-тунелювання, шифрування трафіку та методи адаптивного перемикання між різними супутниковими каналами та діапазонами. Інтеграція різнорідних каналів зв'язку вимагає розробки ефективних механізмів управління та перемикання, а також комплексної оцінки безпеки кожного каналу та інтерфейсів між ними.

Протокольні та алгоритмічні підходи - зосереджені на вдосконаленні методів передачі сигналів, їх кодування, шифрування та автентифікації для протидії перехопленню, модифікації та придушенню.

Методи розширення спектру (Spread Spectrum Techniques):

FHSS (Frequency Hopping Spread Spectrum) - несуча частота сигналу псевдовипадковим чином змінюється в межах широкого діапазону. Це забезпечує стійкість до вузькосмугових завад та ускладнює перехоплення. Ефективність залежить від швидкості стрибків та ширини діапазону. Вразливий до слідкуючих (follow-on) завад, якщо швидкість адаптації завади перевищує швидкість стрибків.

DSSS (Direct Sequence Spread Spectrum) - інформаційний сигнал модулюється псевдовипадковою послідовністю (кодом), що має значно вищу швидкість, ніж інформаційний потік. Це розширює спектр сигналу, забезпечуючи процесинговий виграш на приймачі, що дозволяє виділяти корисний сигнал на фоні шуму та завад. Сигнал стає шумоподібним, що ускладнює його виявлення. Вразливий до потужних широкосмугових завад, якщо співвідношення завада/сигнал перевищує процесинговий виграш.

OFDM (Orthogonal Frequency-Division Multiplexing) - дані передаються паралельно на великій кількості близько розташованих ортогональних піднесучих. Це забезпечує високу спектральну ефективність та стійкість до багатопроменевого поширення завдяки використанню циклічного префіксу. Певна стійкість до вузькосмугових завад досягається за рахунок того, що завада вражає лише частину піднесучих, а дані можуть бути відновлені за допомогою прямої корекції помилок (FEC). Часто застосовуються гібридні схеми (наприклад, FHSS-OFDM, DSSS-OFDM) для поєднання переваг різних методів.

Шифрування каналів зв'язку та управління криптографічними ключами. Наскрізне шифрування (End-to-End Encryption, E2EE) є обов'язковою вимогою для захисту конфіденційності та цілісності команд керування (C2), телеметрії та корисного навантаження (наприклад, відеопотоків).

Криптографічні алгоритми: використовуються сучасні симетричні (наприклад, AES з довжиною ключа 256 біт) та асиметричні (наприклад, ECC з відповідним рівнем безпеки) алгоритми. Вибір алгоритму залежить від обчислювальних можливостей платформи БПЛА та вимог до затримки.

Управління ключами включає безпечну генерацію, розподіл, оновлення, зберігання та відкликання криптографічних ключів. Це є складним завданням, особливо для систем з обмеженими ресурсами, децентралізованих роїв БПЛА та при необхідності забезпечення довготривалої безпеки. Для зберігання ключів можуть використовуватися захищені апаратні елементи (Secure Elements, SE) або модулі довіреної платформи (Trusted Platform Modules, TPM). Фізично неклоновані функції (PUF) можуть використовуватися для генерації унікальних для пристрою ключів або ідентифікаторів. Важливою проблемою є опціональність багатьох функцій безпеки в комерційних та відкритих протоколах. Пріоритетом має бути впровадження принципів "безпеки за замовчуванням" (secure-by-default).

Автентифікація повідомлень - застосування кодів автентифікації повідомлень (Message Authentication Codes, MAC), наприклад, HMAC-SHA256, для перевірки автентичності джерела та цілісності повідомлень. Протокол MAVLink версії 2.0 підтримує підпис повідомлень на основі спільного секретного ключа.

Безпека на транспортному рівні - використання протоколів TLS (Transport Layer Security) або DTLS (Datagram Transport Layer Security) для захисту каналів зв'язку на основі TCP або UDP відповідно.

Автентифікація пристроїв - використання цифрових сертифікатів в рамках інфраструктури відкритих ключів (PKI) для взаємної автентифікації БПЛА та НСК. Можливе застосування полегшених схем PKI або альтернатив на основі блокчейну для середовищ з обмеженими ресурсами.

Безпека Wi-Fi - для БПЛА, що використовують Wi-Fi, обов'язковим є застосування протоколу WPA3, який пропонує покращені механізми

автентифікації (наприклад, Simultaneous Authentication of Equals, SAE) та більш стійке шифрування порівняно з WPA2.

Автентифікація сигналів GNSS - сервіси, такі як Galileo OSNMA (Open Service Navigation Message Authentication), надають можливість перевірки автентичності навігаційних даних, що є критично важливим для протидії GPS/GNSS-спуфінгу. Це вимагає наявності сумісних приймачів та інфраструктури управління ключами.

Безпечні протоколи для технологій інтернет-речей (IoT): для БПЛА, інтегрованих в екосистеми IoT, важливо використовувати захищені версії протоколів:

MQTT (Message Queuing Telemetry Transport) захищається за допомогою TLS. Перспективним є використання MQTT через QUIC (Quick UDP Internet Connections), що забезпечує зменшену затримку встановлення з'єднання та вбудовану безпеку на рівні TLS 1.3.

CoAP (Constrained Application Protocol) захищається за допомогою DTLS. Для пристроїв з дуже обмеженими ресурсами можуть використовуватися полегшені схеми сертифікатів. Розробка та стандартизація полегшених криптографічних бібліотек та протоколів є актуальним завданням для забезпечення безпеки ресурсномістких БПЛА.

Інтелектуальні підходи - вистовують методи штучного інтелекту (ШІ) та машинного навчання (МН) для створення адаптивних систем зв'язку, здатних динамічно реагувати на зміну умов та загроз.

Когнітивне радіо (Cognitive Radio, CR) та динамічний доступ до спектру (Dynamic Spectrum Access, DSA): Системи CR дозволяють БПЛА аналізувати поточний стан радіочастотного спектру, виявляти наявність завад, інтерференції та вільних частотних ресурсів. На основі цього аналізу БПЛА може динамічно змінювати параметри свого каналу зв'язку (частоту, потужність, модуляцію, протокол) для ухилення від завад та забезпечення опортуністичного використання спектру. Це підвищує гнучкість та стійкість системи.[19. 20]

Застосування штучного інтелекту та машинного навчання (AI/ML). Адаптивне управління параметрами зв'язку - алгоритми МН (зокрема, навчання з підкріпленням – Reinforcement Learning, RL) можуть використовуватися для оптимізації параметрів зв'язку в реальному часі на основі аналізу якості каналу, енергоспоживання та поточного рівня загроз.

Виявлення аномалій та загроз - моделі МН (нейронні мережі різних архітектур – CNN, RNN, LSTM; методи типу Isolation Forest, SVM) навчаються на даних про нормальну та аномальну поведінку радіосигналів, мережевого трафіку та телеметрії для виявлення завад, спуфінгу, кібератак (наприклад, DoS, ін'єкції команд) та інших шкідливих дій.

Інтелектуальна протидія загрозам - на основі виявлених загроз AI-системи можуть ініціювати автономні контрзаходи: адаптивну перебудову частоти, зміну маршрутизації даних, активацію резервних каналів, виконання маневрів ухилення (у випадку фізичних атак). Ключовими проблемами для ефективного застосування AI/ML є доступність репрезентативних та якісних наборів даних для навчання моделей, а також ризик "гонки озброєнь ШІ", де атакуючі також використовують ШІ для створення більш складних загроз. Техніки, такі як генеративно-змагальні мережі (GAN) для генерації синтетичних даних та федеративне навчання для навчання на розподілених даних зі збереженням конфіденційності, можуть допомогти у вирішенні цих проблем.

Комплексні підходи та принципи глибоко ешелонованого захисту (Defense-in-Depth). Ізольовані засоби контролю є недостатніми для протидії складним та багатовекторним атакам. Ефективна стратегія забезпечення стійкості каналів зв'язку БПЛА базується на принципі глибоко ешелонованого захисту.

Багаторівнева архітектура безпеки передбачає інтеграцію численних контролів безпеки на різних рівнях системи: фізичному (захист апаратних компонентів), програмному (безпека прошивки та ОС), мережевому (захист протоколів передачі даних), прикладному (безпека програмного забезпечення керування та обробки даних) та операційному (політики, процедури, навчання

персоналу). Відмова одного рівня захисту має компенсуватися ефективністю інших.

Безпечне завантаження (Secure Boot) забезпечує перевірку криптографічного підпису програмного забезпечення (прошивки, ОС, завантажувача) перед його виконанням, встановлюючи апаратний корінь довіри (Hardware Root of Trust). Це запобігає завантаженню неавторизованого або модифікованого коду.

Підписані оновлення прошивки та програмного забезпечення - усі оновлення мають бути криптографічно підписані розробником, а їх цілісність та автентичність – перевірятися перед встановленням. Бажаним є використання багатофакторної автентифікації (MFA) для авторизації процесу оновлення.

Зміцнення операційної системи (OS Hardening) на НСК та, по можливості, на БПЛА, необхідно застосовувати практики зміцнення ОС: видалення непотрібних сервісів та програм, обмеження прав доступу, регулярне встановлення патчів безпеки, налаштування брандмауерів.

Фізична безпека – запобігання несанкціонованому фізичному доступу до БПЛА та НСК для унеможливлення модифікації апаратного забезпечення, встановлення шкідливого ПЗ або викрадення даних/ключів. Захист налагоджувальних портів (JTAG, UART).[19]

Людський фактор та операційні процедури - розробка та впровадження чітких політик безпеки, регулярне навчання операторів БПЛА щодо існуючих загроз та методів протидії, правил безпечної конфігурації систем, управління паролями та оновленнями є невід'ємною частиною комплексної безпеки.

Інтеграція цих підходів дозволяє створити стійку та адаптивну систему зв'язку БПЛА, здатну ефективно функціонувати в умовах складного радіоелектронного середовища та протистояти кібернетичним загрозам.

Висновки за розділом 2

У ході даного розділу було проведено дослідження загроз безпеці каналів зв’язку безпілотних літальних апаратів та розглянуто ключові методи їх нейтралізації. Аналіз підтвердив, що забезпечення надійного та захищеного функціонування каналів зв'язку є критично важливим завданням, зважаючи на стрімке розширення сфер застосування БПЛА та ескалацію відповідних загроз.

Встановлено, що загрози безпеці каналів зв’язку БПЛА мають переважно двоякий характер: радіоелектронний та кібернетичний. Радіоелектронні загрози спрямовані на фізичний рівень передачі сигналів. Вони реалізуються через радіоелектронне подавлення (РЕП), що включає постановку активних завад, як шумових, так і імітаційних/дезінформуючих, з метою порушення співвідношення сигнал/шум або введення в оману систем БПЛА. Важливою складовою є також радіоелектронна розвідка (РЕР) для збору даних про канали зв'язку. Актуальні приклади демонструють широке застосування глушіння каналів керування та навігації (GPS/GNSS) за допомогою загороджувальних, прицільних, маскувальних та інтелектуальних завад.

З іншого боку, кібернетичні загрози експлуатують вразливості програмного забезпечення, протоколів зв’язку та апаратних компонентів БПЛА і наземних станцій керування. Ці загрози реалізуються через атаки на конфіденційність (наприклад, перехоплення даних), цілісність (включаючи модифікацію команд, ін'єкцію шкідливого програмного забезпечення та експлуатацію вразливостей прошивок) та доступність (зокрема, DoS/DDoS атаки). Аналіз методів виявив ключові механізми таких атак, серед яких експлуатація слабкостей комунікаційних протоколів (Wi-Fi, MAVLink, пропрієтарні протоколи), програмного та апаратного забезпечення, а також маніпуляція довірою до сенсорних даних, як-от GPS-спуфінг.

Для протидії цим комплексним загрозам було розглянуто багатоаспектні підходи до забезпечення стійкості каналів зв’язку. Апаратні рішення включають застосування адаптивних антенних решіток з формуванням променя, систем MIMO, а також диверсифікацію каналів зв’язку шляхом використання

альтернативних частотних діапазонів та фізичних принципів передачі даних, таких як міліметрові хвилі, оптичні лінії зв’язку та супутниковий зв’язок.

Протокольні та алгоритмічні підходи зосереджені на впровадженні методів розширення спектру (FHSS, DSSS, OFDM), забезпеченні надійного наскрізного шифрування (із застосуванням алгоритмів AES, ECC) з ефективним управлінням криптографічними ключами, а також на реалізації багатофакторної автентифікації та механізмів забезпечення цілісності даних (наприклад, MAVLink signing, WPA3, PKI, OSNMA) та використанні безпечних протоколів Інтернету речей.

Суттєву роль відіграють інтелектуальні підходи, що передбачають застосування технологій когнітивного радіо, динамічного доступу до спектру та методів штучного інтелекту і машинного навчання для адаптивного управління параметрами зв'язку, своєчасного виявлення аномалій та автономної протидії загрозам.

Таким чином, дослідження підтверджує, що безпека каналів зв'язку БПЛА є динамічною проблемою, яка вимагає безперервного аналізу загроз та вдосконалення методів захисту. Ефективна нейтралізація існуючих та майбутніх загроз можлива лише за умови застосування проактивного, багаторівневого та інтегрованого підходу до забезпечення стійкості та безпеки безпілотних систем.

РОЗДІЛ 3
ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ДО ЗАХИСТУ ІНФОРМАЦІЙНОГО ОБМІНУ В СИСТЕМАХ БПЛА

3.1. Рекомендації для криптографічного захисту каналів зв’язку

Надійний криптографічний захист є однією з найважливіших умов забезпечення інформаційної безпеки в системах безпілотних літальних апаратів, оскільки більшість таких систем працюють через бездротові канали зв’язку, які піддаються ризикам перехоплення, модифікації або несанкціонованого доступу. Враховуючи обмежені обчислювальні ресурси більшості БПЛА, високу критичність переданої інформації та потенційно агресивне середовище, в якому працює система, вибір правильних криптографічних рішень є ключовим.

Основним засобом захисту безперервних потоків даних (команд управління, телеметрії, відео) є симетричне шифрування. У сучасних системах де-факто стандартом є алгоритм AES (Advanced Encryption Standard), а саме його варіант з довжиною ключа 256 біт — AES-256. Цей алгоритм поєднує високу стійкість до криптоаналітичних атак із широкою підтримкою в апаратному та програмному забезпеченні.

Особливу увагу варто приділити режимам роботи AES: з міркувань захисту цілісності та автентичності даних пріоритетним є використання режимів AEAD (Authenticated Encryption with Associated Data), таких як AES-GCM (Galois/Counter Mode). Цей режим дозволяє не лише зашифрувати інформацію, але й вбудувати автентифікаційний тег, що запобігає можливості її підміни або фальсифікації.

Водночас, у майбутньому варто звернути увагу на нові ініціативи, зокрема щодо Rijndael-256, варіанта AES з 256-бітним блоком, який розглядається NIST. Таке розширення може стати актуальним для систем, що оперують великими обсягами чутливих даних, хоча його практичне застосування потребує

додаткових досліджень щодо продуктивності та сумісності з апаратними платформами.

Асиметрична криптографія, попри більші обчислювальні витрати, залишається невід'ємною частиною криптозахисту в системах БПЛА — перш за все для безпечного обміну симетричними ключами та перевірки цифрових підписів. Найбільш доцільним вибором у таких системах є використання еліптичних кривих, які забезпечують той самий рівень безпеки, що і RSA, при суттєво коротших ключах.

Наприклад, 256-бітний ключ ECC дорівнює за безпекою 3072-бітному RSA, але вимагає значно менше пам’яті, енергії та часу на обчислення. Цей аспект особливо важливий для БПЛА, які мають обмежені обчислювальні ресурси або працюють у режимі реального часу. Крім того, менші ключі означають менші цифрові підписи та легші сертифікати, що оптимізує трафік у системах із вузькою пропускною здатністю.

В умовах надзвичайно обмежених ресурсів (наприклад, у мініатюрних або енергозалежних БПЛА), навіть AES або ECC можуть бути надмірними. У таких випадках доцільно використовувати алгоритми легковажної криптографії. Їх спеціально розроблено для пристроїв з низькою потужністю, обмеженою пам’яттю та обчислювальними можливостями, з урахуванням сучасних вимог безпеки.

Одним із найперспективніших кандидатів є ASCON — фіналіст конкурсу NIST LWC. ASCON поєднує криптостійкість рівня AES-128 із винятковою ефективністю, що робить його придатним для реалізації на мікроконтролерах, що керують дроном або сенсорами.

Під час впровадження LWC-алгоритмів важливо звертати увагу на наявність сертифікацій, результати незалежного аудиту та готовність оптимізованих реалізацій для цільових платформ.Особливої уваги заслуговує наскрізне шифрування, яке гарантує, що дані можуть бути прочитані лише на пристрої-одержувачі. Це означає, що навіть якщо інформація проходить через публічні або напівдовірені середовища (хмарні сервіси, ретранслятори, VPN-

шлюзи), вона залишається недоступною для сторонніх. Для БПЛА E2EE має критичне значення при передаванні даних корисного навантаження — зокрема фото- або відеоматеріалів, даних розвідки або сканування місцевості.

Успішне впровадження E2EE потребує ретельно спроектованої архітектури управління ключами**,** зокрема можливості їх безпечного розповсюдження, відкликання та оновлення. Складнощі можуть виникати в ситуаціях, коли дані передаються не одній, а кільком довіреним сторонам (наприклад, спостерігачам, аналітикам, операторам у режимі реального часу). У таких випадках можливим рішенням є реалізація мультиадресної схеми розповсюдження ключів або використання криптографічних контейнерів з ієрархічним доступом.

Якщо система БПЛА використовує публічні мережі (стільниковий зв'язок, Wi-Fi, супутникові канали), шифрування каналів зв'язку повинне бути посилене за допомогою VPN. Це дозволяє створити захищений тунель, що унеможливлює підслуховування або зміну переданих даних.

Найбільш ефективними протоколами VPN для БПЛА сьогодні є:

- *IPsec* — класичне рішення, широко підтримується апаратно і програмно, забезпечує захист на мережевому рівні. Однак складність налаштування, проблеми з NAT та зниження продуктивності у мобільних мережах можуть стати обмеженнями.
- *OpenVPN* — відкритий стандарт, який працює поверх TLS та підтримує TCP/UDP на різних портах. Його гнучкість — велика перевага, але обчислювальні витрати можуть бути занадто високими для обмежених пристроїв.
- *WireGuard* — новий, легкий і високопродуктивний протокол, який використовує сучасну криптографію (ChaCha20, Poly1305, Curve25519). WireGuard ідеально підходить для дронів, особливо у поєднанні з мобільними або супутниковими каналами. Його мінімалістичний код, низька затримка та швидке встановлення з'єднання роблять його переважним варіантом для систем із високими вимогами до продуктивності.

У випадку використання супутникових каналів, де характерні високі затримки та втрата пакетів, особливо важливо обирати протоколи з низьким рівнем накладних витрат і здатністю працювати у нестабільних умовах. Саме тут WireGuard демонструє значну перевагу, оскільки функціонує поверх UDP і добре адаптований до подібних середовищ.

Для забезпечення надійного захисту каналів зв'язку БПЛА надзвичайно важливо використовувати захищені версії протоколів зв'язку. Зокрема, протокол MAVLink у версії 2.0 підтримує підпис повідомлень, що дозволяє автентифікувати відправника та гарантувати цілісність переданих даних управління і телеметрії.

Правильне налаштування цього механізму з використанням надійних секретних ключів є критично важливим для безпеки системи. Окрім цього, у сучасних програмних комплексах, таких як ArduPilot чи Mission Planner, доступні інструменти для впровадження та підтримки захисту MAVLink. Існують також розробки, які пропонують додаткове шифрування протоколу, наприклад MAVShield, що посилює конфіденційність передачі даних.

Якщо для зв'язку застосовується Wi-Fi, рекомендується використовувати найновіший стандарт безпеки WPA3. Цей стандарт забезпечує значне підвищення захисту від атак, зокрема від атак підбору пароля завдяки протоколу SAE, а також підтримує посилені механізми для корпоративного використання з EAP-TLS та надійними серверами автентифікації. Це дає змогу мінімізувати ризики несанкціонованого доступу в корпоративних та комерційних сценаріях.

Для передачі телеметричних даних часто використовується протокол MQTT, який сам по собі не має вбудованого шифрування. Тому надзвичайно важливо застосовувати MQTT поверх TLS, що гарантує конфіденційність та автентифікацію серверів і клієнтів за допомогою цифрових сертифікатів. Для БПЛА з обмеженими ресурсами корисним є застосування протоколу CoAP із захистом DTLS, що забезпечує захист повідомлень на основі UDP.

Сучасні дослідження спрямовані на підвищення безпеки CoAP/DTLS через використання легкових сертифікатів на блокчейн-технологіях та протоколів

автентифікації з доказом з нульовим розголошенням, що є особливо актуальним у ресурсно-обмежених умовах.[20]

Окрім захисту самих протоколів, важливо впроваджувати практики безпечного життєвого циклу розробки програмного забезпечення (Secure SDLC). Це означає інтеграцію заходів безпеки на всіх етапах створення програмного забезпечення — від аналізу вимог і проектування до кодування, тестування та подальшої підтримки. Зокрема, на початкових етапах необхідно проводити моделювання загроз, що дозволяє ідентифікувати потенційні вразливості, специфічні для БПЛА. Розробники повинні дотримуватися принципів безпечного кодування, уникаючи типових помилок, які можуть призвести до серйозних вразливостей, таких як переповнення буфера чи SQL-ін’єкції. Важливо також регулярно застосовувати статичний та динамічний аналізи безпеки коду, а також проводити тестування на проникнення, щоб виявляти та усувати слабкі місця в системі захисту.

Також не можна оминути і застосування механізмів безпечного завантаження (Secure Boot) та захищеного оновлення прошивки. Secure Boot гарантує, що при запуску пристрою завантажується лише автентичне та не змінене програмне забезпечення. Це реалізується через перевірку цифрових підписів кожного етапу завантаження, починаючи з апаратно реалізованого кореня довіри. Таким чином, Secure Boot запобігає запуску шкідливих компонентів, які могли бути встановлені зловмисником.

Безпечне оновлення прошивки, яке здійснюється «по повітрю», також має бути організоване таким чином, щоб кожен пакет оновлення був цифрово підписаний виробником і передавався через захищені канали зв’язку. Важливо забезпечити механізми для відкату до попередніх стабільних версій прошивки у випадку проблем під час оновлення.

Очікувано, що навіть найнадійніші криптографічні методи захисту каналу будуть марними, якщо програмне забезпечення або прошивка БПЛА чи наземної станції мають вразливості. Наприклад, зловмисник може скористатися

помилками в коді (типу переповнення буфера) для отримання контролю над системою управління і доступу до криптографічних ключів.[20]

Аналогічно, якщо прошивка не захищена Secure Boot, можливе встановлення модифікованого шкідливого ПЗ, яке обійде всі криптографічні перевірки. Тому безпека протоколів зв'язку і безпека програмного забезпечення є нерозривно пов'язаними і однаково важливими компонентами загальної системи захисту БПЛА. Ігнорування хоча б одного з цих аспектів неминуче призведе до послаблення всієї системи захисту.

3.2. Рекомендовані технічні засоби для захисту БпЛА

З розвитком безпілотних літальних апаратів зростає важливість забезпечення надійності та безпеки каналів управління і навігації. Вразливість цих каналів до різноманітних перешкод і зовнішніх впливів створює необхідність застосування ефективних засобів радіоелектронної протидії. Активне створення завад дозволяє ускладнити або повністю заблокувати роботу небажаних БпЛА, забезпечуючи контроль над радіочастотним середовищем. У цьому підпункті розглядаються основні принципи, типи і сучасні тенденції розвитку систем радіоелектронної боротьби (РЕБ) для захисту каналів управління та навігації безпілотних літальних апаратів.

3.2.1. Радіоелектронна протидія ворожим впливам на канали управління та навігації БпЛА

Одним з ефективних способів боротьби з ворожими БпЛА є створення активних завад – навмисне глушіння каналів управління та навігації за допомогою електромагнітних сигналів високої потужності. Основне завдання таких систем – перевищити рівень корисного сигналу на вході приймача БпЛА настільки, щоб зробити неможливою його демодуляцію чи декодування. Успішність залежить від співвідношення потужності завади до потужності

сигналу (J/S), яке, в свою чергу, визначається низкою технічних параметрів: потужністю передавача, чутливістю приймача, типом модуляції, дистанцією та характеристиками антен.

Сучасні БпЛА дедалі частіше використовують стрибкоподібну перебудову частоти (FHSS) або DSSS-модуляцію, що потребує більшої потужності глушіння – іноді до 20–40 дБ вище за корисний сигнал. З огляду на це, зростає потреба в інтелектуальних, адаптивних системах РЕБ, здатних аналізувати радіообстановку та швидко змінювати частотний профіль завад.

Розрізняють кілька основних типів завад:

- Загороджувальні (широкосмугові, перекривають увесь діапазон, але потребують великої потужності й можуть шкодити власним системам);
- Прицільні (вузькосмугові, енергоефективні, але вимагають точного знання частоти);
- Маскувальні шумові (створюють шум для ускладнення виявлення та супроводу).

Вибір між ними визначається тактичною ситуацією, рівнем розвідданих і потребою уникати впливу на власні мережі.

«Купольні» РЕБ-системи формують зону радіоелектронного захисту, яка накриває певну територію або об'єкт. Вони створюють електромагнітну «бульбашку», у межах якої БпЛА втрачає можливість керування чи навігації. Такі системи охоплюють як комерційні, так і військові діапазони – переважно в межах 0.1–6 ГГц – з радіусом дії від кількох сотень метрів до декількох кілометрів. Деякі мобільні комплекси розгортаються за лічені хвилини.

У контексті російсько-української війни подібні системи стали звичним інструментом для захисту позицій від FPV-дронів і малих розвідувальних БпЛА. Наприклад, «окопний РЕБ» здатен ефективно глушити сигнали на відстані понад 2 км, тоді як російські системи на кшталт «Шиповник-Аэро» мають радіус близько 1 км і час реакції до 25 секунд. Новітні зразки типу К-1000 призначені для захисту бронетехніки й працюють у діапазонах 800/900 МГц із потужністю до 20 Вт.

Серед переваг таких систем – можливість одночасного впливу на кілька цілей, мобільність та відносна простота у використанні. Проте їхня дія носить невибірковий характер, що створює ризики для власних засобів зв'язку. Крім того, ефективність «купольного» РЕБ обмежена проти автономних або технологічно просунутих БпЛА з нестандартними каналами зв'язку. Окремі моделі мають низький енергопотенціал і не інтегровані з системами розвідки, що знижує швидкість реагування.

Водночас розвиток таких систем триває – з акцентом на програмну гнучкість (SDR), розширення частотного покриття та інтеграцію з розвідувальними засобами. Ефективна робота РЕБ дедалі більше залежить від синхронізації з засобами РТР, які забезпечують оперативне виявлення параметрів ворожих каналів зв’язку.[21]

3.2.2. Засоби протидії GPS-спуфінгу та забезпечення стійкості навігації

Супутникові навігаційні системи, зокрема GPS, GLONASS, Galileo та BeiDou, є ключовими для визначення місцезнаходження та навігації більшості сучасних безпілотних літальних апаратів. Проте цивільні навігаційні сигнали GNSS залишаються незахищеними і мають низьку потужність, що робить їх вразливими до спеціалізованих атак, серед яких особливе місце займає спуфінг.

Для ефективного протистояння GPS-спуфінгу потрібен комплексний підхід, що включає апаратні рішення, програмні методи виявлення аномалій, автентифікацію навігаційних сигналів та використання альтернативних систем навігації.

Одним із ключових способів захисту є використання приймачів, які працюють з декількома системами та частотами одночасно (GPS, Galileo, GLONASS, BeiDou, L1, L2, L5). Це ускладнює підробку сигналів, адже треба фальсифікувати одразу багато джерел. Приймачі порівнюють дані та можуть відкидати підозрілі сигнали.

Ще один потужний засіб — CRPA-антени, які мають кілька антенних елементів і за допомогою цифрової обробки формують спрямовану діаграму, блокуючи сигнали з напрямків, де знаходяться джерела перешкод або спуфінгу, і посилюючи справжні супутникові сигнали.

Такі рішення зараз стандартні у військових дронах і критично важливих цивільних застосуваннях. Водночас вони коштують дорого і мають великі розміри, тож їх важко використовувати на масових чи малих БпЛА. Проте ринок розвивається, і з’являються більш компактні та енергоефективні модулі.

Для підвищення довіри до сигналів з’являються технології автентифікації, які дозволяють перевірити, чи сигнал справжній і не підроблений. Приклад — Galileo OSNMA, що додає до навігаційних повідомлень криптографічні підписи.

Приймач з підтримкою OSNMA може впевнено відкинути фальшиві дані. Система вже пройшла тестування та скоро стане доступною для комерційного використання.

Однак OSNMA не захищає від усіх типів атак — наприклад, від атак повтором сигналу. Для неї потрібні спеціальні приймачі, а також є затримка у підтвердженні даних через особливості протоколу.

Якщо GNSS недоступний або ненадійний через глушіння чи спуфінг, використовують інші методи:

- Інерціальні навігаційні системи (INS) — за допомогою акселерометрів і гіроскопів обчислюють рух і позицію, але з часом накопичують похибки і потребують корекції.
- Візуальна одометрія та SLAM — камери та LiDAR допомагають орієнтуватися по навколишньому середовищу і будувати його карту.
- Навігація за місцевими радіомаяками або ландшафтом — порівняння даних з сенсорів з попередньо відомими картами.
- Лазерні датчики швидкості — новітні технології для точного визначення руху.

3.2.3. Технології захищеного зв'язку, стійкі до РЕБ

Для успішної роботи БпЛА дуже важливо мати надійний зв’язок із наземною станцією. Традиційні радіоканали легко глушаться або перехоплюються засобами радіоелектронної боротьби (РЕБ). Тому зараз активно шукають нові, більш захищені способи передачі даних, які б витримували потужні перешкоди. Особливо це актуально через загострення бойових дій і використання РЕБ у війні в Україні.

Один із найбільш надійних способів — це волоконно-оптичний кабель, який фізично з’єднує БпЛА з оператором. Кабель розмотується під час польоту, і дані передаються світлом — це практично не піддається глушінню або перехопленню. ВОЛЗ дає високу якість відео і не випромінює сигналів, тож виявити дрон дуже складно.

Недоліки — це обмежена маневреність через кабель, вага котушки з кабелем, можливість пошкодження дроту, а також те, що кабель може вказати ворогу місце запуску. Попри це, такі дрони показали себе дуже ефективними, особливо в умовах насиченого РЕБ.

Для безпечної роботи БпЛА використовують спеціальні військові або комерційні канали з додатковим захистом:

- FHSS (Frequency-Hopping Spread Spectrum) — швидко змінює робочу частоту, ускладнюючи глушіння.
- DSSS (Direct-Sequence Spread Spectrum) — розширює спектр сигналу, щоб його було важче виявити.
- OFDM (Orthogonal Frequency-Division Multiplexing) — підвищує стійкість зв’язку в складних умовах.

Для конфіденційності та цілісності даних застосовують шифрування (AES-256, ECC) та автентифікацію (наприклад, HMAC). Протоколи, як MAVLink 2.0, підтверджують, що дані не були змінені під час передачі.

Приклади таких систем — військові БпЛА MQ-9 Reaper і Bayraktar TB2, а також комерційні рішення DJI OcuSync, Mobilicom SkyHopper та інші.[19. 21]

Ці технології значно ускладнюють роботу РЕБ, але повністю уникнути атак вони не можуть. Сучасні «розумні» засоби РЕБ навчаються адаптуватися навіть до захищених каналів, що робить протидію дуже складною. Війна в Україні показала, що цей технологічний «поєдинок» — безперервний процес вдосконалення як засобів захисту, так і методів атаки.

3.3. Приклади захищених архітектур каналів управління

Захист каналів управління БПЛА сьогодні ефективно реалізується через багатошарову радіочастотну архітектуру, засновану на принципі *«оборони в глибину»*. Вона включає низку рівнів безпеки — від шифрування до апаратного захисту.

Конфіденційність даних забезпечується AES-256 (у перспективі — Rijndael-256), що унеможливлює перехоплення команд. Цілісність і автентичність гарантують HMAC-SHA256 та протоколи на зразок MAVLink 2.0 із цифровими підписами.

Для складніших систем застосовується PKI та фізично неклоновані функції (PUF), які забезпечують унікальність та захист ключів навіть при фізичному доступі до пристрою.

Захист від радіоелектронних загроз реалізується через FHSS, DSSS, OFDM, а також адаптивне формування променя. Новітні технології, як-от когнітивне радіо з машинним навчанням, дозволяють БПЛА в реальному часі адаптувати сигнал.

Нарешті, апаратна безпека (TPM, Secure Elements, Secure Boot) гарантує надійне зберігання ключів і захищене завантаження ПЗ.

Щодо конкретних прикладів реалізації таких архітектур, варто звернути увагу на технологію DJI OcuSync. В останніх версіях — 3.0 та 4.0 — виробник впровадив шифрування AES-256 та динамічне перемикання частот для підвищення безпеки. Система забезпечує передачу відео високої якості на великі відстані, зберігаючи стабільність навіть у складних умовах міста.Але є і нюанс,

який полягає в тому, що пропрієтарний характер OcuSync не дозволяє незалежного аудиту. Це створює ризик прихованих вразливостей. Дослідження, зокрема інцидент з CVE-2023-6951, доводять, що навіть у добре захищених системах можуть існувати критичні прогалини. У випадку DJI виявлено, що компрометація пульта дистанційного керування може призвести до витоку криптографічних ключів, що ставить під загрозу безпеку всієї системи.

Іншим прикладом є відкритий протокол MAVLink 2.0, який використовується в автопілотах ArduPilot і PX4. Його основною перевагою є прозорість — можливість дослідження та вдосконалення безпекових механізмів усією спільнотою. MAVLink 2.0 передбачає підписання повідомлень, що дозволяє захиститися від модифікації або повторного використання команд. Водночас, слід пам’ятати, що цей захист є опціональним, а шифрування даних у базовій конфігурації відсутнє. Це означає, що без впровадження додаткових рішень — таких як MAVShield — передані повідомлення залишаються відкритими для перехоплення. Таким чином, хоча відкриті рішення й забезпечують гнучкість і прозорість, їхній рівень захисту значною мірою залежить від реалізації на конкретному обладнанні.[21]

Загалом, багатошарові захищені радіочастотні архітектури демонструють високу ефективність при правильному поєднанні механізмів безпеки. Їхня успішність залежить від комплексного підходу, де жоден елемент не залишений без уваги: ні криптографія, ні управління ключами, ні фізичний захист, ні адаптація до змін середовища.

В умовах надзвичайно потужної радіоелектронної боротьби, коли звичні радіочастотні канали зв'язку з безпілотниками стають вкрай вразливими до глушіння, спуфінгу або повного блокування, дедалі більшого значення набуває застосування оптоволоконних каналів управління. На відміну від традиційних засобів передачі даних, оптоволокно забезпечує фізичне з'єднання між БПЛА та оператором, що дозволяє повністю уникнути впливу радіочастотної агресії.

Технологія полягає у використанні тонкого, легкого, але дуже ефективного оптоволоконного кабелю, який з’єднує дрон із наземною станцією управління.

Через цей кабель передаються команди управління, телеметрія та відеопотік у вигляді світлових імпульсів, що робить передачу практично невразливою до електромагнітного впливу. Світлові сигнали, що проходять через оптоволокно, не піддаються впливу глушилок і не можуть бути перехоплені на відстані, на відміну від радіохвиль. Щоб отримати доступ до такої інформації, супротивнику довелося б фізично перехопити кабель — завдання майже нереальне в бойових умовах.

Під час російсько-української війни, яка стала прикладом сучасного конфлікту з безпрецедентним рівнем РЕБ, обидві сторони почали масово впроваджувати оптоволоконні дрони, зокрема FPV-моделі, які під'єднуються до оператора кабелем. Ця тактика дозволила зберігати повноцінне управління та високу якість відеозв’язку навіть у районах, де будь-який інший дрон «глухне» або повністю втрачає контакт. Зокрема, українські підрозділи активно використовували такі дрони для проведення корегування артилерійського вогню та точкових ударів по складах, командних пунктах, техніці в укриттях. Завдяки високій стабільності зв’язку та повній нечутливості до РЕБ, ці дрони також застосовувалися для виявлення пересування ворожих підрозділів у густих лісосмугах, де звичайні БПЛА не могли б діяти через перешкоди або сигналове заглушення.

Величезною перевагою стала майже повна відсутність радіовипромінювання, що значно знижує ймовірність виявлення БПЛА радіотехнічними засобами супротивника. Візуально оптоволоконний дрон також важче зафіксувати, особливо на фоні ландшафту, а кабель, прокладений по землі, часто залишався непоміченим.

Водночас така технологія має низку важливих обмежень. Основною проблемою є фізична довжина кабелю, яка прямо обмежує дальність і висоту польоту дрона. Як правило, це кількасот метрів, хоча іноді використовуються кабелі до 1–2 км, але з очевидними тактичними ризиками. Маневреність дрона також знижується — він не може вільно облітати перешкоди, а у складному рельєфі чи серед дерев кабель може легко заплутатись, обірватися або

зачепитися. До того ж сам кабель залишається вразливим до фізичного пошкодження — його можуть перебити уламки снарядів, кулі або навіть уламки будівель. Це вимагає від оператора високого рівня підготовки, щоб постійно контролювати розгортання кабелю, уникати небезпеки та змінювати позицію, оскільки протягнутий по землі шлейф може демаскувати точку управління.

Також проблемою є і логістика. Якісні оптоволоконні кабелі, стійкі до натягів та температурних змін, є дорогими і не завжди доступними у потрібному обсязі, особливо на передовій. Крім того, потрібна відповідна котушка, обладнання для змотування, а іноді й додаткове живлення, що збільшує загальну вагу комплексу.

Навіть попри «виклики», досвід бойових дій підтвердив, що оптоволоконні дрони — це не тимчасове рішення, а повноцінна технологічна відповідь на нову реальність війни, де домінує РЕБ. Їх застосування дозволяє ефективно діяти там, де інші системи виявляються безсилими, а головне — зберігати контроль над БПЛА у найнебезпечніших ділянках фронту.

Коли безпілотник працює на значній відстані від оператора або в умовах, де пряма видимість ускладнена (наприклад, у гірській місцевості чи в міській забудові), для передачі команд управління та отримання телеметрії зазвичай використовуються загальнодоступні мережі — зокрема мобільний зв’язок (LTE/5G) або супутникові канали. Однак такі мережі не можна вважати цілком надійними: вони піддаються ризику перехоплення, підміни чи втручання. У зв’язку з цим виникає потреба у додатковому захисті каналу зв’язку між оператором і самим дроном. Одним із найефективніших способів є використання VPN (віртуальної приватної мережі), яка створює зашифрований «тунель» між обома сторонами.

Фактично VPN діє як екран, що ховає весь обмін даними всередині шифрованого каналу, навіть якщо самі дані проходять через загальнодоступні або ненадійні мережі. Це дає змогу зберегти в таємниці не лише самі команди, а й унеможливити їх зміну сторонніми особами. У ролі VPN-рішень сьогодні дедалі частіше використовують протокол WireGuard, який вирізняється

простотою архітектури, високою продуктивністю та сучасними криптографічними алгоритмами — наприклад, ChaCha20 для шифрування та Poly1305 для перевірки автентичності. Окрім нього, у практиці залишаються поширеними IPsec та OpenVPN — особливо у поєднанні з алгоритмом AES-256.

Є важливим і процес взаємної автентифікації — тобто підтвердження, що під'єднаний пристрій справді є тим, за кого себе видає. Це реалізується або за допомогою цифрових сертифікатів, або заздалегідь узгоджених ключів шифрування, що значно ускладнює доступ до системи для зловмисника.

Сьогодні використання VPN у сфері БПЛА — це не просто додаткова опція, а стандарт безпеки, особливо коли йдеться про військові місії, моніторинг об'єктів інфраструктури чи доставку вантажів у важкодоступні райони. У деяких випадках вже реалізовано й національні ініціативи: наприклад, в Україні тестуються VPN-з'єднання на базі WireGuard у поєднанні з супутниковим інтернетом Starlink. Такі проєкти демонструють, що навіть за складних умов можна організувати надійний захищений зв'язок.

Важливо враховувати і технічні нюанси, а саме те, що VPN додає певну затримку до передавання даних, що може бути критичним у випадках, де потрібна швидка реакція дрона. Це особливо відчутно, коли використовується супутниковий канал, де сама по собі латентність досить висока. Також VPN може трохи знижувати швидкість передачі через шифрування та інші накладні витрати.

Результатом є те, що VPN може бути дієвим засобом захисту каналу управління БПЛА, але його впровадження потребує ретельного налаштування, контролю ключів шифрування та адаптації до конкретних умов роботи. Лише за такого підходу можна досягти оптимального балансу між безпекою, стабільністю зв'язку та його швидкодією.

Висновки за розділом 3

У цьому розділі ми розглянули практичні шляхи зміцнення інформаційної безпеки в системах безпілотних літальних апаратів. Розуміючи, що канали зв'язку БПЛА є вразливими, ми запропонували низку рекомендацій, що охоплюють як основи криптографічного захисту, так і конкретні технічні засоби та архітектурні підходи, покликані протистояти сучасним загрозам.

Основою безпеки є надійна криптографія: від стандартів AES-GCM та ECC для шифрування й обміну ключами до наскрізного шифрування та VPN (особливо WireGuard) для захисту даних у будь-яких мережах. Це має поєднуватися з використанням захищених протоколів та впровадженням безпеки на всіх етапах життєвого циклу ПЗ.

Водночас, сучасні реалії, особливо досвід бойових дій, диктують необхідність протистояти радіоелектронній боротьбі. Це вимагає як засобів активного придушення ворожих дронів, так і захисту власних від GPS-спуфінгу та глушіння. Тут волоконно-оптичні лінії зв'язку (ВОЛЗ) довели свою виняткову ефективність, забезпечуючи зв'язок там, де інші методи безсилі, попри притаманні їм обмеження.

Найбільш стійкий захист досягається через багатошарову архітектуру ("оборона в глибину"), де різні рівні безпеки доповнюють один одного. Як показує аналіз існуючих рішень, навіть просунуті системи потребують ретельного налаштування та постійного аудиту.

Отже, забезпечення безпеки БПЛА – це складне завдання, що вимагає неперервного вдосконалення та гнучкого поєднання криптографічних, технічних та архітектурних методів для протидії постійно еволюціонуючим загрозам.

ВИСНОВКИ

Безпілотні літальні апарати стрімко перетворилися з нішевої технології на ключовий інструмент у багатьох галузях — від оборони та безпеки до цивільних застосувань, таких як логістика, моніторинг та сільське господарство. Однак їхня ефективність та безпека нерозривно пов'язані з надійністю та захищеністю каналів зв’язку, які забезпечують керування, передачу телеметрії та даних. Зростаюча залежність від БПЛА та одночасне підвищення рівня загроз роблять питання безпеки цих каналів надзвичайно актуальним. Втручання в роботу БПЛА може мати серйозні наслідки, включаючи фінансові втрати, зрив критично важливих місій, компрометацію даних та навіть створення фізичних загроз. Метою даної кваліфікаційної роботи було проведення глибокого аналізу цих загроз та розробка практичних рекомендацій для підвищення рівня захищеності інформаційного обміну в системах БПЛА.

У першому розділі ми заклали фундамент для розуміння об'єкта дослідження, систематизувавши основні типи та класифікації безпілотних систем. Було проаналізовано складну модульну структуру систем управління БПЛА, включаючи польотний контролер, навігаційні системи, сенсори та виконавчі механізми, а також архітектуру обміну даними між ними. Особливу увагу приділено комунікаційним системам: розглянуто еволюцію та сучасні канали зв'язку (від радіоканалів прямої видимості до мобільних та супутникових мереж), їх характеристики та відповідні апаратні модулі й антени. Також було описано функціональність наземних станцій керування (GCS) та їх програмного забезпечення, підкресливши тісну взаємодію між наземним та повітряним сегментами. Цей аналіз виявив значну різноманітність та складність сучасних безпілотних систем, що вказує на необхідність комплексного підходу до їх захисту.

Другий розділ було присвячено дослідженню загроз, що стоять перед комунікаційними системами БПЛА, та методів їх нейтралізації. Ми встановили,

що ці загрози мають переважно двоякий характер: радіоелектронний та кібернетичний. Радіоелектронні загрози, такі як глушіння (jamming) та спуфінг, спрямовані на фізичний рівень передачі сигналів. Аналіз актуальних прикладів, зокрема з досвіду війни в Україні, підтвердив широке застосування РЕБ для порушення роботи каналів керування та навігації. Кібернетичні загрози, у свою чергу, експлуатують вразливості програмного забезпечення та протоколів. Ми розглянули атаки на конфіденційність, цілісність та доступність, включаючи перехоплення даних, ін'єкцію команд, компрометацію GCS та атаки на прошивки. Було показано, що багато протоколів, як MAVLink, спочатку не мали належного захисту, що робить їх вразливими. Важливим висновком стало розуміння зростаючої ролі комбінованих атак, де радіоелектронні та кібернетичні методи посилюють один одного. Для протидії цим загрозам було систематизовано підходи до забезпечення стійкості, що охоплюють апаратні, протокольні, алгоритмічні та інтелектуальні рішення.

На основі проведеного аналізу, третій розділ запропонував конкретні практичні рекомендації щодо захисту інформаційного обміну. У сфері криптографії рекомендовано застосування сучасних алгоритмів (AES-256-GCM, ECC), легковажної криптографії для ресурсномістких пристроїв, наскрізного шифрування та VPN (особливо WireGuard) при використанні публічних мереж. Наголошено на важливості захисту протоколів (MAVLink 2.0, WPA3, MQTT/TLS) та інтеграції безпеки в життєвий цикл ПЗ (Secure SDLC, Secure Boot). Щодо технічних засобів, розглянуто методи радіоелектронної протидії ("купольні" системи), засоби боротьби з GPS-спуфінгом (CRPA-антени, OSNMA, альтернативна навігація) та технології зв'язку, стійкі до РЕБ, з особливим акцентом на волоконно-оптичні лінії (ВОЛЗ) як надзвичайно стійке рішення в умовах інтенсивного РЕБ. Нарешті, було підкреслено необхідність побудови багатошарових архітектур за принципом "оборони в глибину", що поєднують усі ці елементи.

Підсумовуючи, дана кваліфікаційна робота систематизувала знання про функціонування БПЛА та їхні комунікаційні системи, провела комплексне

дослідження радіоелектронних та кібернетичних загроз, проаналізувала сучасні методи захисту та, що найважливіше, розробила конкретні практичні рекомендації для підвищення рівня безпеки інформаційного обміну. Водночас, поле для подальших досліджень залишається широким: необхідно поглиблено вивчати комбіновані атаки, розробляти адаптивні системи безпеки на основі ШІ, аналізувати безпеку роїв БПЛА та впроваджувати квантово-стійкі криптографічні алгоритми.

Забезпечення безпеки каналів зв'язку БПЛА є динамічною та складною проблемою. Як показало дослідження, не існує єдиного універсального рішення. Лише комплексний, багаторівневий та проактивний підхід, що гнучко поєднує криптографічні, технічні та архітектурні методи й постійно адаптується до нових викликів, може забезпечити надійний захист цих критично важливих систем у сучасному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. PX4 System Architecture [Електронний ресурс] / PX4 Autopilot. – Режим доступу: https://docs.px4.io/main/en/concept/px4_systems_architecture.html.

2. AltHold Mode [Електронний ресурс] / ArduPilot Development Team. – Режим доступу: https://ardupilot.org/copter/docs/altholdmode.html.

3. CAN Bus on UAVs [Електронний ресурс] / Anyleaf Blog. – Режим доступу: https://www.anyleaf.org/blog/can-bus-on-uavs.

4. UAV Data Transmission and Communication Protocols [Електронний ресурс] / Robolabor.ee. – Режим доступу: https://robolabor.ee/img/cms/projektid/UAV%20Data%20Transmission%20and%20Communication%20Protocols.pdf.

5. EnerLinksIII ISR Datalink System [Електронний ресурс] / Viasat. – Режим доступу: https://www.viasat.com/products/terminals-and-radios/enerlinks/.

6. Overview of Drone Communication Requirements in 5G [Електронний ресурс] / Technical University of Denmark (DTU). – Режим доступу: https://backend.orbit.dtu.dk/ws/portalfiles/portal/293927450/Overview_of_Drone_Communication_Requirements_in_5G.pdf.

7. Navigating the Unseen: A Comprehensive Review of Communication Technologies for Unmanned Aerial Vehicles (UAVs) in 5G and Beyond-5G Networks [Електронний ресурс] / PubMed Central / NCBI. – Режим доступу: https://pmc.ncbi.nlm.nih.gov/articles/PMC11237935/.

8. WiMAX [Електронний ресурс] / Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/WiMAX.

9. Satellite Communications for UAVs: Enabling Global Line of Sight [Електронний ресурс] / Iridium Blog. – Режим доступу: https://www.iridium.com/blog/satellite-communications-uav/.

10. The Future of UAS Communications: The Starlink Revolution [Електронний ресурс] / Unmanned Network. – Режим доступу: https://unmanned-network.com/the-future-of-uas-communications-the-starlink-revolution/.

11. Phased Array Communications Used for Long-Distance UAS Flight [Електронний ресурс] / Unmanned Systems Technology, May 2020. – Режим доступу: https://www.unmannedsystemstechnology.com/2020/05/phased-array-communications-used-for-long-distance-uas-flight/.

12. Radar-like communications system extends signal range for millimeter wave frequencies [Електронний ресурс] / MIT News, 02.V.2025. – Режим доступу: https://news.mit.edu/2025/radar-communications-system-extends-signal-range-millimeter-wave-frequencies-0502.

13. Advanced Cockpit Ground Control Station [Електронний ресурс] / General Atomics Aeronautical Systems, Inc. (GA-ASI). – Режим доступу: https://www.ga-asi.com/images/products/ground_control/pdf/AdvCockpit021915.pdf.

14. Mission Planner Overview [Електронний ресурс] / ArduPilot Development Team. – Режим доступу: https://ardupilot.org/planner/docs/mission-planner-overview.html.

15. QGroundControl - Open Source Ground Control Station [Електронний ресурс] / QGroundControl Team / Dronecode Foundation. – Режим доступу: https://qgroundcontrol.com/.

16. DJI GS Pro (Ground Station Pro) [Електронний ресурс] / DJI. – Режим доступу: https://www.dji.com/global/ground-station-pro.

17. What is an Intrusion Detection System (IDS)? [Електронний ресурс] / Palo Alto Networks. – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids.

18. Cyber-Physical Intrusion Detection System for Unmanned Aerial Vehicles [Електронний ресурс] / ResearchGate. – Режим доступу: http://researchgate.net/publication/376738569_Cyber-Physical_Intrusion_Detection_System_for_Unmanned_Aerial_Vehicles.

19. Resilient UAV Swarm Communications: A Deep Reinforcement Learning Approach for Anti-Jamming in Dynamic Spectrum Environments [Електронний ресурс] / Frontiers in Energy Research, 2024. – Режим доступу: https://www.frontiersin.org/journals/energy-research/articles/10.3389/fenrg.2024.1491332/full.

20. Blockchain-based Secure Firmware Updates for UAVs [Електронний ресурс] / Preprints.org, April 2025. – Режим доступу: https://www.preprints.org/manuscript/202504.1585/v1.

21. Enhancing UAV Communication Security Using Quantum Key Distribution: A Feasibility Study [Електронний ресурс] / PubMed Central / NCBI. – Режим доступу: https://pmc.ncbi.nlm.nih.gov/articles/PMC11820592/.