МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
«____» _____2021 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 Кібербезпека

на тему: **МЕТОДИКА ПІДВИЩЕННЯ ЗАХИСТУ РАДІОКАНАЛУ УПРАВЛІННЯ ВІД ПЕРЕХОПЛЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ**

Виконав: студент 6 курсу, групи СЗДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Технічні системи інформаційного та кібернетичного захисту»
(шифр і назва спеціальності)
Ганусяк С.І.
(прізвище та ініціали)
Керівник Шуклін Г.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Гребенніков А.Б.

Київ – 2021

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
к.т.н. Шуклін Г.В
“__” _____ 2020р.

З А В Д А Н Н Я
на магістерську атестаційну роботу
студенту Ганусяку Степану Ігоровичу

1. Тема роботи: Методика підвищення захисту радіоканалу управління від перехоплення безпілотних літальних апаратів, керівник Шуклін Герман Вікторович, к.т.н., затверджені наказом вищого навчального закладу від “__” _____ 2020 року №____.

2. Термін здачі студентом оформленої роботи “___” _____ 20__ р.

3. Предмет дослідження: методика захисту радіоканалів управління безпілотними літальними апаратами.

4. Об’єкт дослідження: безпілотні літальні апарати.

5. Мета роботи: підвищення точності розрахунку функції надійності захисту радіоканалу управління при передачі інформації від безпілотних літальних апаратів.

6. Перелік питань, які мають бути розроблені:

1. Проаналізувати особливості функціонування безпілотних літальних апаратів;
2. Дослідити проблеми безпеки безпілотників;
3. Виконати аналіз існуючих методів захисту безпілотних літальних апаратів проти атак з використанням радіозасобів;
4. Розробити рекомендації щодо підвищення безпеки безпілотників та безпілотних літальних апаратів;
5. Вдосконалити методику захисту радіоканалів управління безпілотними літальними апаратами.

7. Перелік публікацій:

8. Перелік ілюстративного матеріалу:

1. Презентація виконана на ____ слайдах для подання за допомогою оверхедів (світлопроекторів) та комп’ютерних засобів.

9. Дата видачі завдання “__” вересня 2020 р.

Науковий керівник _____ Шуклін Г.В.
(підпис)

Завдання прийняв до виконання _____ Ганусяк С.І.
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір наукової літератури	до 30.09.20 р.	виконано
2	Написання першого розділу роботи	до 23.10.20р.	виконано
3	Написання другого розділу роботи	до 15.11.20 р.	виконано
4	Написання третього розділу роботи	до 29.11.20 р.	виконано
5	Написання висновків по роботі	до 09.12.20 р.	виконано
6	Підготовка демонстраційних матеріалів	до 17.12.20 р.	виконано
7	Захист у ДЕК	18.01.2021 р.	виконано

Студент: СЗДМ - 61 Ганусяк С.І. _____
(підпис)

Науковий керівник: к.т.н. Шуклін Г.В. _____
(підпис)

РЕФЕРАТ

Текстова частина магістерської роботи: 76 сторінка, 19 рисунків, 6 таблиць, 52 джерела.

Об'єкт дослідження - безпілотні літальні апарати.

Предметом дослідження є методика захисту радіоканалів управління безпілотними літальними апаратами.

Мета роботи - підвищення точності розрахунку функції надійності захисту радіоканалу управління при передачі інформації від безпілотних літальних апаратів.

Методи дослідження – методи теорії інформації, методи математичного моделювання, теорії управління, теорії складних систем, методи теорії системного аналізу, імітаціне моделювання.

В роботі описано архітектуру безпілотника, типи зв'язку та типи БПЛА. Розроблено рекомендації щодо підвищення безпеки безпілотників/БПЛА з урахуванням обговорення основних загроз безпеці та конфіденційності, атак та відповідних технічних рішень. Розроблено алгоритм, який забезпечує встановлення факту належності прийнятого радіовипромінювання до класу радіосигналів систем дистанційного керування БПЛА з імпульсно-позиційною та імпульсно-кодовою модуляціями.

Зазначено, що алгоритм базується на послідовних перевірках енергетичної, модуляційної та структурної ознак сигналу, передбачає можливість автоматичного виявлення сигналу супроводження його за частотою. Запропоновано конкретні апаратні та програмні рішення для побудови прототипу БПЛА. Наведено результати практичного тестування можливих рішень задач на готовому прототипі і наведено результати функціонування розроблених компонентів зв'язку.

БПЛА, БЕЗПІЛОТНИКИ, АВТОМАТИЗОВАНА СИСТЕМА, ІНФОРМАЦІЯ, БЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, РАДІОКАНАЛИ, РАДІОЕЛЕКТРОННИЙ ЗВ'ЯЗОК, ЗАХИЩЕННИЙ ЗВ'ЯЗОК, МОДУЛЯЦІЯ, КАНАЛИ.

ЗМІСТ

ВСТУП

Впровадження та широке використання безпілотних літальних апаратів постійно зростає у багатьох сферах. Це пов’язано з можливістю безпілотників робити запис та ретранслювати у режимі реального часу відео та зображення разом із можливістю літати та перевозити вантажі. Як результат, понад 100 000 безпілотників вже працюють в комерційних цілях по всьому світу. Це пов’язано головним чином з їхніми перевагами перед комерційними літаками та гвинтокрилами. Особливо коли мова йде про комерційну складову.

Більше того, розвиток науки і техніки призвів до того, що здійснювати управління безпілотними літальними апаратами легко можна за допомогою смартфонів (замість використання дистанційних контролерів). Важливо відмітити, що використання дронів не обмежується лише комерційними цілями. Безпілотниками користуються правоохоронні та прикордонні служби, МЧС та лікарні.

У разі стихійних лих пошуково-рятувальні групи використовують їх для збору інформації або для скидання необхідних запасів. Однак під час використання безпілотників виникає ціла низка проблем, адже доступ до каналів передачі інформації можуть отримати і злочинці, для задоволення власних потреб. Як і проводові мережі, безпілотні літальні апарати потрапляють під вплив різних атак.

В більшості випалків, вони вразливі до різних атак. Ці атаки призводять до суттєвих наслідків, включаючи комерційні та некомерційні втрати. В цьому контексті бракує належного розуміння того, як хакери виконують свої атаки та викрадають дрон, щоб його перехопити або навіть розбити. Насправді, безпілотники також можуть бути скомпрометовані в зловмисних цілях. Отже, існує потреба їх виявити та запобігти заподіянню шкоди. Точніше – бракує розуміння того, яким чином будується та може бути підвищенний захист радіоканалів управління безпілотними літальними апаратами.

Об’єкт дослідження - безпілотні літальні апарати.

Предметом дослідження є методика захисту радіоканалів управління безпілотними літальними апаратами.

Мета роботи - підвищення точності розрахунку функції надійності захисту радіоканалу управління при передачі інформації від безпілотних літальних апаратів.

Методи дослідження. Для рішення поставлених задач у роботі використовуються методи теорії інформації, методи математичного моделювання, теорії управління, теорії складних систем, методи теорії системного аналізу, імітаціне моделювання.

Для досягнення поставленої мети у роботі сформовані і вирішені наступні завдання:

– аналіз особливостей функціонування безпілотних літальних апаратів;

– дослідження проблеми безпеки безпілотників;

– аналіз існуючих методів захисту безпілотних літальних апаратів проти атак з використанням радіозасобів;

– розробка рекомендацій щодо підвищення безпеки безпілотників та безпілотних літальних апаратів;

– вдосконалення методики захисту радіоканалів управління безпілотними літальними апаратами.

У зв'язку з викладеним, тематика магістерської роботи є актуальною, а отримані в роботі результати мають важливе прикладне значення.

Апробація результатів. Основні положення і результати магістерської роботи доповідались і обговорювались на 2-х науково-практичних конференціях.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ ФУНКЦІОНУВАННЯ БПЛА

За даними Федеральної авіаційної адміністрації (FAA), в даний час понад 2,5 мільйони безпілотників літають лише над США. Фактично, вже в 2020 році ця позначка досягла показника в 7 мільйонів активних безпілотників [1]. Більше того, технологічне та економічне зростання електронної комерції дозволило застосувати багато програм, які використовують використання безпілотників. З іншого боку, це створює можливості для кіберзлочинців компрометувати або навіть експлуатувати доступність та здатність безпілотників для зловмисних цілей [2].

Починаючи з перших кроків впровадження безпілотних літальних апаратів (БПЛА), вони розглядаються як пов'язані з основними проблемами безпеки, що робить їх цілями для різних типів кібератак. Більше того, їх також можна використовувати як потенційний вектор атаки для зловмисних користувачів. Насправді, БПЛА працюють на різних частотах безпроводового зв'язку, як показано в таблиці 1.1, яка порівнює дві основні частоти зв'язку дронів, 2,4 ГГц і 5 ГГц.

Таблиця 1.1

Порівняння між 2,4 ГГц та 5 ГГц.

Параметри	**2.4 ГГц**	**5 ГГц**
Діапазон частот	Нижня частота	Більш висока частота
Вартість	Дешевше	Дорожчий
Діапазон	Охоплює великі діапазони	Охоплює короткі дальності
Вплив шуму	Шумний	Менш галасливий
Втручання	Висока ймовірність втручання	Низька ймовірність втручання
Фізичні бар'єри	Здатний подолати певні фізичні бар’єри	Неможливо подолати фізичні бар’єри
Продуктивність	Впливає на швидкість мережі Wi-Fi	Не впливає на швидкість мережі Wi-Fi

Таблиця 1.2

Світові вимоги та норми функціонування безпілотних літальних апаратів

Країна	**Початковий регламент**		**Експлуатаційні вимоги**					**Шлях польоту**			
	Вага (<25 кг)	Вимоги	Просторове обмеження	Радіозв'язок	Візуальна лінія зору	Особливості безпеки	Конфіденційність	Юрисдикція	Реєстрація та маркування	Подроби ці дозволу польоту	Кваліфікація оператора
Україна	Якщо застосовується	Відсутність реєстрації	Військові об'єкти, аеропорти, в'язниці, атомні електростанції	2.4–5 ГГц	В межах прямої видимості	Невстановлений	Жодних твердих обмежень	Місцевий уряд	Ім'я, адреса, номер телефону, призначення	Мета використання	Національний, дорослий
Німеччина	Якщо застосовується	Конкретний дозвіл на дозвіл на політ	Військові об'єкти, аеропорти, в'язниці, атомні електростанції	2.4–5 ГГц	100м-1км	Сертифікат проекту, виклик на базу	Обмежений запис осіб	Місцевий уряд	Ім'я, адреса, дата народження, мета	Попередньо визначений шлях, мета використання та деталі	Підтвердження досвіду, знань та тренінгів

Продовження Таблиці 1.2

Китай	Якщо застосовується	Не вимагається	Військові об'єкти, аерорти, в'язниці, атомні електростанції	2.4–5 ГГц	В межах прямої видимості	Не застосовується	Все ще дискусійне	Китайське законодавство щодо цивільних польотів	Назва, адреса, номер телефону польоту	Призначення польоту, місця зйомки, шлях	Національний, дорослий, ліцензований
Сполучені Штати	Якщо застосовується	Ліцензія / дозвіл	Військові об'єкти, аерорти, в'язниці, атомні електростанції	2.4–5 ГГц	В межах прямої видимості	Сертифікат проекту, виклик на базу, безпечна посадка	Федеральної авіаційної адміністрації	Обмежений запис осіб	Ім'я, адреса, дата народження, мета	Попередньо визначений шлях, мета використання та деталі	Дорослий, посвідчення польоту

Уряди багатьох країн світу, включаючи держави-члени ЄС, США, Великобританію та Південно-Африканську Республіку, декілька разів вже піднімали питання отримання офіційних ліцензій власникам БПЛА (табл.1.2).

Особливо гостро це питання відчувається, коли беспілотники вносять загози приватним територіям, стратегічним об’єктам чи військовим центрам.

1.1 Аналіз архітектури безпілотних літальних апаратів

Як правило, будь-яка архітектура БПЛА або безпілотника складається з трьох основних елементів: безпілотний літак (UmA), наземна станція управління (GCS) та лінія зв'язку даних (CDL) [4].

Ці компоненти коротко описані нижче:

- Контролер польоту – класифікується як центральний процесорний апарат безпілотника;
- Наземна станція управління - базується на наземному об'єкті (OLF), який надає операторам (користувачам) необхідні можливості контролювати та/або контролювати БПЛА під час їх експлуатації на відстані. GCS відрізняються залежно від розміру, типу та місій безпілотників.
- Посилання для передачі даних – це безпроводові зв’язки, що використовуються для управління інформаційним потоком між дроном та GCS. Це залежить від діапазону експлуатації БПЛА.

На основі досліджень, проведених у роботі [4], управління безпілотниками можна класифікувати на основі їх відстані від GCS:

- Візуальна відстань прямої видимості (VLOS): дозволяє передавати та приймати контрольні сигнали за допомогою прямих радіохвиль.
- Відстань до зори прямої видимості (BVLOS): дозволяє керувати безпілотниками за допомогою супутникового зв'язку [5].

1.2 Типи комунікації та взаємодії безпілотників

Зв'язок безпілотників можна класифікувати на чотири основних типи: безпілотник-безпілотник (D2D), безпілотник до наземної станції (D2GS), безпілотник до мережі (D2N) і безпілотник до супутника (D2S). Структура спілкування проілюстрована на рис.1.1.

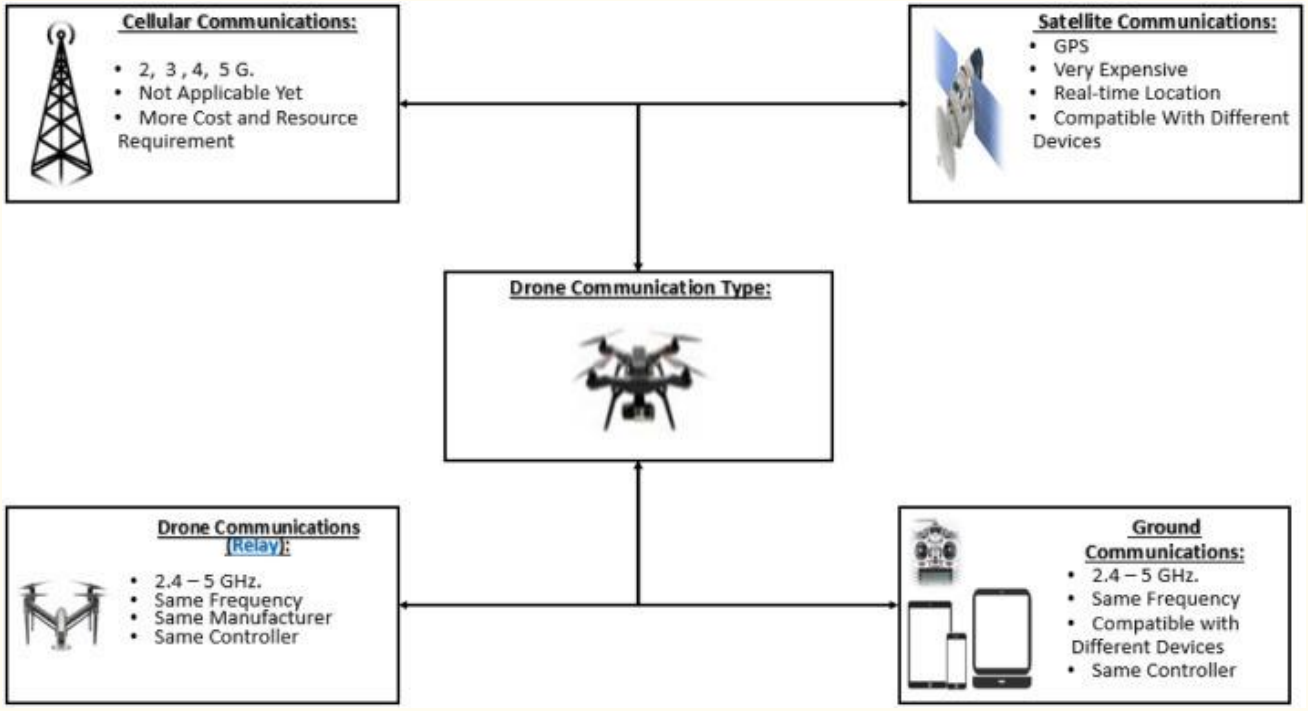


Рис.1.1. Варіації можливих каналів комунікації з дронами

1. Безпілотний зв’язок. Така комунікація ще не стандартизована. Насправді, машинне навчання можна використовувати для розробки та оптимізації інтелектуальної системи безпроводового зв'язку на базі БПЛА. У більшості випадків комунікація «безпілотний зв’язок» (D2D) може бути змодельований як підключення Peer-to-Peer (P2P). Це зробить його вразливим для різних типів атак P2P, включаючи такі як відмова в обслуговуванні (D-DoS) та атаки sybil [7].

2. Наземний зв’язок. Цей тип зв'язку базується на вже відомих та стандартизованих протоколах, які базуються на безпроводових комунікаціях, таких як Bluetooth та Wi-Fi 802.11, включаючи 2,4 ГГц та 5 ГГц. Однак більшість дронів, які комунікують наземним зв’язком, можуть стати вразливими до пасивних (підслуховування) та активних (людина всередині) атак.

3. Стільниковий зв’язок.Цей тип зв'язку дозволяє вибрати мережу, виходячи з необхідного рівня безпеки. Він також може включати стільниковий зв'язок, що означає покладання на 3 ГГц, 4 ГГц, 4G + (LTE) та 5 ГГц. Важливо забезпечити захист таких мереж безпроводового зв'язку під час використання.

4. Супутниковий зв’язок. Це тип зв'язку, необхідний для надсилання координат у реальному часі через GPS. Це дозволяє будь-якому безпілотнику викликати його назад до початкової станції у випадку, якщо він вийшов за лінію управління або поза лінію зору. Супутниковий зв'язок вважається захищеним і безпечним. Однак пред'являє високу вартість та вимоги до обслуговування. Ось чому даний тип зв’язку широко використовуються збройними силами.

1.3 Різновид існуючих БПЛА

Всі БПЛА є безпілотниками, однак, не всі безпілотники є БПЛА. Різниця між безпілотниками, безпілотниками та безпілотними авіаційними системами (БПЛА) представлена на рис.1.2.

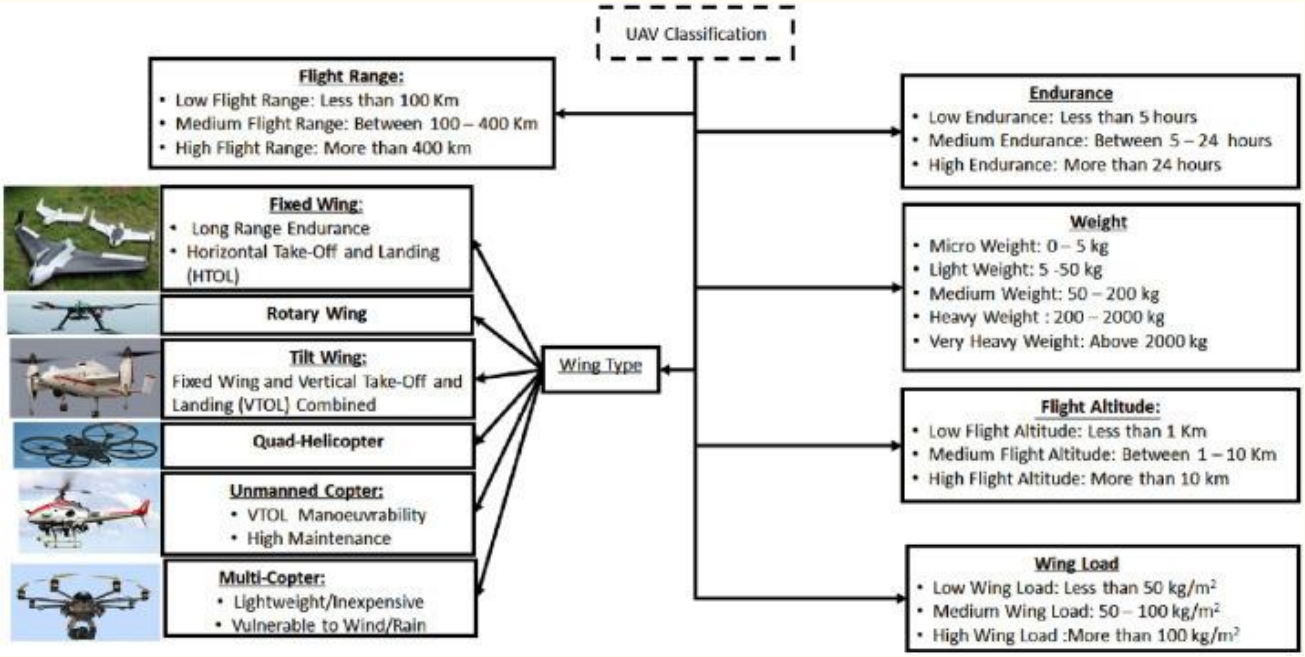


Рис.1.2. Класифікація безпілотних літальних апаратів

1. Дрони. Цей термін зазвичай використовується для позначення літаків з дистанційним (автономним) керуванням. Цей термін також описує різні

транспортні засоби, включаючи підводні човни або наземні автономні транспортні засоби. Насправді, безпілотники можна класифікувати на три основні типи відповідно до їх літаючих механізмів [8]:

- Мультироторні безпілотники: вони також відомі як безпілотники з поворотним крилом. Вони засновані на принципі вертикального зльоту та посадки (VTOL). Більше того, завдяки своїй маневреності, вони можуть зависати над фіксованим місцем розташування, що дозволяє їм забезпечувати постійне стільникове покриття на певних ділянках. Тому багатороторні безпілотники можуть виступати в якості базових станцій у передбачуваних місцях з високою точністю та точністю. Однак їх рухливість дуже обмежена, і вони споживають велику кількість енергії.
- Безпілотники з фіксованими крилами: вони більш енергоефективні, ніж багатороторні безпілотники. Це пов’язано з їх здатністю ковзати та рухатися з великою швидкістю, одночасно перевозячи важкі вантажні навантаження. Основним недоліком безпілотників із фіксованим крилом є необхідність злітно-посадкової смуги для зльоту та посадки [9] через їх характер горизонтального зльоту та посадки (HTOL). Іншим недоліком є їх неможливість переміщення курсору над фіксованими місцями, крім їх дорогого програмного/апаратного характеру.
- Безпілотники з гібридними крилами: це безпілотники з фіксованим/поворотним крилом, які нещодавно вийшли на ринок. Цей тип безпілотників може швидко дістатися до місця призначення, ковзаючи по повітрю та витаючи за допомогою чотирьох роторів.

2. БПЛА. Можуть літати дистанційно/автономно, використовуючи контролер, мобільний телефон, комп’ютер або навіть планшет [10]. Вони характеризуються своїми автономними льотними можливостями та здатністю експлуатувати на великі відстані при безпечній передачі живильної подачі. Крім того, управління БПЛА можна класифікувати та розділити на три основні категорії:

- Дистанційне управління пілотом: відоме як статична автоматизація оператора, коли всі рішення приймає людина-віддалений оператор.

- Дистанційне контрольоване управління: відоме як адаптивна автоматика. Він пропонує безпілотникам можливість запускати та виконувати певний процес місії самостійно, одночасно дозволяючи втручання людини, якщо це необхідно.
- Повний автономний контроль: відомий як статична автоматична система, коли безпілотники можуть приймати всі необхідні рішення для успішного завершення місії, без потреби в будь-якому втручанні людини.

3. П (С) БО. До них належать БПЛА та безпілотники та оператори, що керують ними. БПЛА - це тип безпілотників, який відноситься до керованого транспортного засобу або літака [11].

4. RPA. Розшифровується як дистанційно керований літак, який вимагає інтенсивних навичок та навчання протягом тривалого періоду часу (кілька років) для експлуатації та управління цими складними польотами [38].

1.4 Аналіз узагальнених методів функціонування всіх категорій безпілотних літальних апаратів

1) Методи уникнення аварії. Зараз різні типи безпілотних літальних апаратів оснащені системами запобігання аварій, для навігації навколо об’єктів та повернення на базу за запрограмованим маршрутом. Це можливо за допомогою радіочастотної ідентифікації (RFID) та радіочастотних передавачів низької потужності, які постійно передають свої ідентифікаційні дані. Це гарантує захист та постійне розміщення в легальних точках входу.

2) Методи запобігання зіткненням (СА). Через постійні та близькі зіткнення між літаками та БПЛА критично важливо уникати будь-яких зіткнень між ними. Як результат, методи моделювання та оцінки безпеки безпілотників та їх застосування на безпілотних авіаційних системах (БПЛА) представляють собой головну ідею. Метою було розробити систему UA-Sense-and-Avoid (SAA), засновану на здатності відчувати та уникати завади та перешкоди, в координації зі стандартом Федеральної авіаційної адміністрації (FAA) (RTCA SC-203) [13]. Метод

заснований на автономній системі CA, яка пропонує захист для запобігання будь-яких зіткнень. Це було успішно зроблено, не спричинивши жодних збоїв в польоті. Насправді, алгоритми CA були розроблені для виконання певних завдань, включаючи Індивідуальне уникнення зіткнень (ICA) у двовимірних та Уникнення групових зіткнень (GCA) у площині 3D. Інший метод був представлений Yang et al. у [14], і воно базується на плануванні 3D шляху БПЛА, яке полягає у визначенні шляху без зіткнень у заваленому 3D середовищі на основі трьох основних обмежень, геометричного, фізичного та часового.

3) Методи уникнення перешкод і зіткнень.Також були представлені різні методи уникнення зіткнень із перешкодами для подолання будь-якої перешкоди, яка стикається з БЛА. У [15] Ueno та співавт. представив закон, який дозволяє літаку точно локалізувати предмети, що знаходяться поблизу. У [16] Брандт та ін. заявив, що чотириротові ротори більш придатні для роботи в приміщенні через їх гнучку роботу на невеликих та обмежених площах. Крім того, алгоритм ручного управління БПЛА за допомогою автоматичного запобігання зіткненню перешкод (OCA) було досліджено.

4) Маршрутизація БПЛА. Важливо забезпечити безпечний шлях маршруту для безпілотників, щоб уникнути нещасних випадків, пошкодження та/і травм. Для цього потрібно враховувати загрозу, ризик, ціль та рельєф, а також обмеження БПЛА. Як результат, було запроваджено підхід на основі агента до проблеми планування маршруту БПЛА, використовуючи алгоритми усвідомлення ситуації. Більше того, детерміновані та імовірнісні стратегії планування шляху для автономних мереж БЛА дотримувались шляхом вивчення перешкод. У роботі [17] Ернандес та ін. застосував графічний метод для багатоцільового планування маршруту змодельованого БПЛА для дотримання необхідних міркувань безпеки.

1.5 Аналіз сфер використання безпілотних літальних об’єктів

Найближчим часом безпілотники відіграватимуть важливу роль, доставляючи товари або навіть виконуючи функції літаючих мобільних гарячих

точок для широкосмугового безпроводового доступу. Насправді, коли безпілотні літаки розгортаються на пікових точках підходящим рішенням для розподілу смуги пропускання є біноміальний та пуассоновський кластерні процеси. Основна мета - обслуговувати величезну кількість користувачів у певній області. Більше того, безпілотники можуть використовуватися для підтримання всіх необхідних методів безпеки та спостереження, які застосовуються для забезпечення безпечного, надійного та належного використання цих безпілотників.

Тому основна увага приділяється багатоцільовому використанню цих безпілотників як у цивільній, так і у військовій сферах. Сфери використання безпілотників показано на рис.1.3.

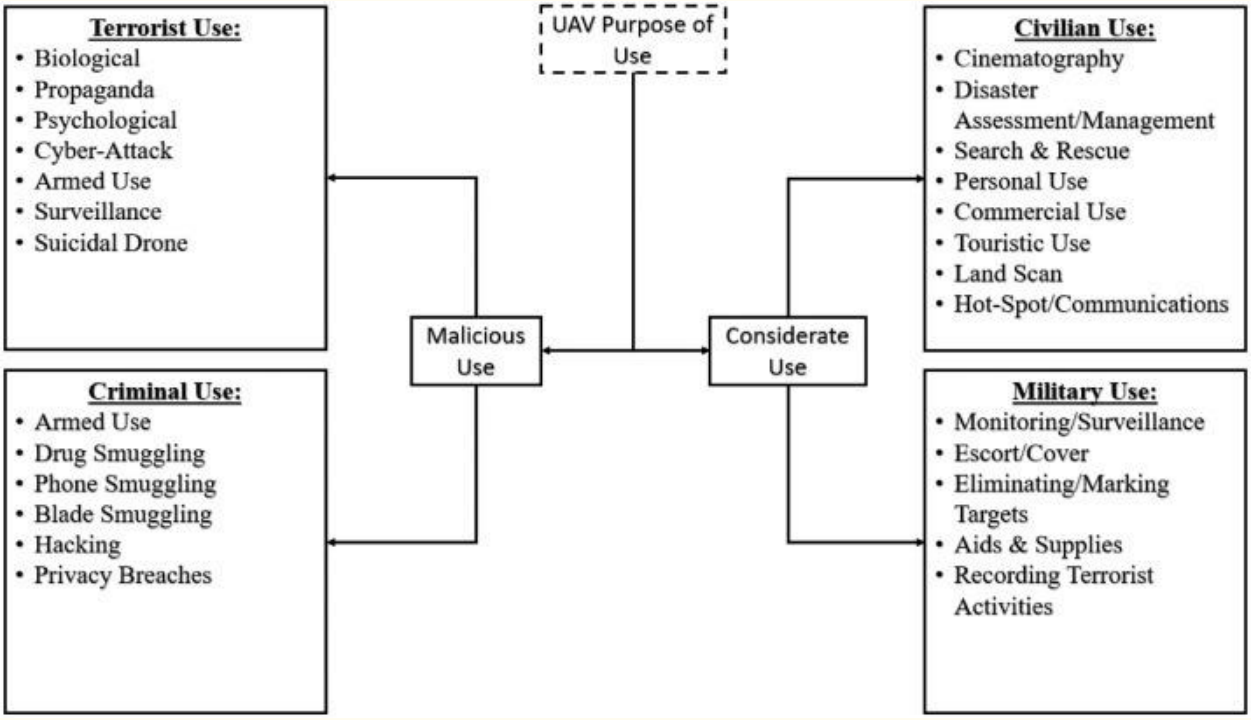


Рис.1.3. Сфери використання беспілотників

1. Цивільне використання. Останнім часом безпілотники використовуються в різних цивільних областях, включаючи пошук та порятунок та управління катастрофами. Основні цивільні програми безпілотників включають:

- Кінематографія. Безпілотники в даний час використовуються різними кінематографістами для забезпечення аерофотозйомок, як ніколи раніше, забезпечуючи новий рівень творчості з висоти пташиного польоту.

- Реагування та боротьба зі стихійними лихами. БПЛА використовуються для боротьби зі стихійними лихами та їх оцінки.
- Пошук та порятунок. БПЛА можуть використовуватися з метою пошуку загублених, розсіяних або скручених людей, особливо коли присутність людини вважається небезпечною або обмеженою.
- Туризм. Беспілотники також можна використовувати для захоплення приголомшливих краєвидів, включаючи вид пташиного польоту. Це може бути використано для залучення туристів та просування туристичних місць та визначних місць, що покращує загальну туристичну галузь.
- Комерційна реклама. Дрони також використовуються в комерційній рекламі, оскільки їх можна використовувати для зйомки (зйомки) сцени з якістю високої чіткості (HD) і протягом певного періоду часу. Це зменшує потребу у дорогому обладнанні та взаємодії людей.
- Управління кризисними ситуаціями. У випадку теракту чи стихійного лиха (повені землетрусів) БПЛА можуть виступати в якості гарячих точок або базових станцій, що дозволяє збирати короткі повідомлення, надіслані постраждалими людьми, або використовуватися для попередження групи реагування. В інших випадках це допомагає знаходити людей на основі їх місцезнаходження GPS або MAC-адрес. Однак у випадку теракту вони можуть виступати в якості точки доступу (ДП) для детонатора смертника, що полегшує активацію та детонацію бомби.
- Реагування на надзвичайні ситуації. На даний момент безпілотники використовуються в якості мобільних медичних наборів, які можна надіслати групам реагування на першу допомогу на місці події. Це пропонує необхідну допомогу без затримок, на відміну від автомобілів швидкої допомоги. Фактично, безпілотники були розгорнуті по вулицях Іспанії та Китаю (головним чином Ухань), використовуючи камери та динаміки для підвищення обізнаності та обігрівання людей, використовуючи повітряний спрей та дезінфекцію для боротьби з поширенням вірусу корона (COVID-19) [18]. Крім того, безпілотні літальні апарати використовувались як літаючий засіб для доставки

ізольованих/інфікованих пацієнтів товарами (тобто продуктами харчування та ліками), а також як літаючий засіб для швидшого транспортування тестових зразків, зменшуючи людську взаємодію.

- Управління навколишнім середовищем. Безпілотники можуть бути використані для виконання завдань із вимірювання забруднення (тобто безпілотники для вимірювання та аналізу якості повітря), сільськогосподарські завдання (тобто аналіз грунту, управління посівами/насінням/худобою та боротьба зі шкідниками), або дослідження/охорона природи/дикої природи (тобто боротьба з браконьєрством, захист зникаючих видів).
- Підводні/морські цілі. Підводні безпілотники або безпілотні океанічні транспортні засоби (UOV) зафіксували все більше використання підводних пошуково-рятувальних операцій, збору екологічних та прибережних даних та виявлення та моніторинг морської фауми (тварин).

2. Використання в правоохоронних структурах. Безпілотники використовуються для відстеження підозрюваних за допомогою повітряного спостереження. Це виявилося дешевшим і більш маневреним, ніж вертоліт. Насправді, безпілотники незабаром матимуть здатність утримувати виявлення тепла, руху та нічного бачення, які можна використовувати для відстеження підозрюваних у будь-який час доби. Крім того, безпілотники можуть бути використані для підвищення ефективності руху, пропонуючи швидку реакцію та ідентифікацію дорожніх умов. Це допомагає уникнути заторів та реагувати на дорожньо-транспортні пригоди чи надзвичайні ситуації. Більше того, ці безпілотники можуть використовуватися для цілей спостереження, з можливістю виявляти підозрілі цілі, приховані в суспільних доменах, що виявилося більш гнучким, ніж стаціонарні камери. Причина пов’язана з їх здатністю ідентифікувати та розпізнавати підозрюваних за їх зростом, розміром та розпізнаванням обличчя, а отже, дуже ускладнює підозрюваним ховатися на публіці.

В результаті автономного та експлуатаційного характеру безпілотників, вони ставали дедалі більш пристосованими та працездатними. Це зменшує та замінює використання вертольотів, зменшуючи час відгуку та необхідні ресурси.

Безпілотники здатні зафіксувати живий огляд птахів на різні типи інцидентів, починаючи від злочинів, крадіжок і навіть заворушень. Це призводить до більш твердої реакції з розширеним планом завдяки можливості ідентифікувати підозрюваних під час їх пошуку та відстеження перед тим, як їх заарештувати.

Також БПЛА можуть використовуватися поліцією та іншими відомствами для збору важливої інформації в небезпечних ситуаціях із меншою робочою. До основних причин використання безпілотників для випадку повітряного спостереження на основі реальних випадків, належать:

- Моніторинг дорожнього руху. БПЛА використовуються для спостереження за дорожнім рухом та місцями аварій;
- Відстеження втікачів. БПЛА використовувались для спостереження за втечами з місць злочинів та в'язниць;
- Криміналістичний пошук та порятунок. БПЛА використовувались для розкриття інцидентів із злочинами;
- Захист від заворушень. БЛА нещодавно використовувалися в контрпротестах як частину тактики контролю натовпу.

3. Військові програми. БПЛА стали ідеальним вибором для військового використання, особливо для розвідувальних та розвідувальних цілей, здійснюючи спостереження, прицілювання та розвідку цілей (STAR), радіолокаційну атаку об’єднаних спостережних цілей (JSTAR), розвідку, спостереження та комплектування (RSTA) завдання. Їх розгортання є ключовою складовою для протидії повстанцям та тероризму, пропонуючи можливість відстеження та ідентифікації особового складу (TIDP) у міському середовищі, особливо в районах операцій (АО).

- P-CAS. Додаткові зусилля спрямовані на те, щоб дати БПЛА запропонувати стійку та близьку повітряну підтримку (P-CAS)/точні удари для захисту наземних військ у режимі реального часу, і для швидкого знищення цілей завдяки використанню лазерних керованих ракет і не чекаючи виклику авіаудару. Цей метод застосовували американські, (британські) та французькі збройні сили. Ці безпілотники також можуть бути використані для допомоги (елітним) військам

у їх прихованих, явних або підпільних операціях, пропонуючи керівництво, близьку підтримку з повітря або активний/пасивний рух ворога в рамках спостереження, придбання цілей та розвідки (STAR), розвідки Придбання цілей спостереження (RSTA) та/або бойові дії, розвідка, спостереження, розвідка (CISR) для посилення ролі командування, управління, зв'язку, комп'ютерів, розвідки, спостереження та розвідки (C4ISR) та подолання обмежена роль розвідки, спостереження та розвідки (ISR) безпілотних наземних транспортних засобів (БПЛА).

- Точний обстріл. БПЛА також використовувались для точного обстрілу терористичних цілей.
- Повітряне спостереження/розвідка. На відміну від залежності від розвідки людини (HUMINT), БПЛА також були розгорнуті як частина повітряної розвідки та збору інформації, що дозволяє ідентифікувати та відстежувати повстанців (тобто навчання, переміщення та табори), транспортні засоби (тобто переміщення , типи), зброя, схованки зброї та імпровізовані вибухові пристрої (СВУ) (тобто заводи, обладнання, ринок та посадки).
- Викрадення БПЛА. Це робиться в основному за допомогою спуфінгу/перешкод за допомогою GPS.
- Приховане повітряне спостереження/розвідка. БПЛА розроблялися та виготовлялися ще в першу світову війну, використовуючи прийоми радіокерування.
- Ухилення від радіолокаційного виявлення.
- Перехоплення кадру. Військові аналітики можуть аналізувати кадри, зроблені та зняті безпілотником терориста, намагаючись зірвати внутрішній теракт. Це дозволяє їм визначити свою тактику, оперативне географічне розташування, а також свої навички, зброю та навчання.
- Підводний нагляд. Підводні безпілотники використовувались для прихованого підводного спостереження та розвідувальних операцій, особливо ВМС США. Такі операції включають різні підводні безпілотники, такі як безпілотні підводні машини (UUV), підводні десантні машини (AUV) та підводні

морські транспортні засоби (UMV), які також використовуються як частина військово-морських сил протимінна війна.

Таблиця 1.3

Кібер-атаки на безпілотники

Атака	**Ціль**			**Заходи безпеки**	
Тип	**Конфіденційність даних**	**Доступність**	**Аутентифікація**	**Некриптографічний**	**Криптографічний**
Зловмисне програмне забезпечення	✓	✓	✓	Гібридна IDS	Контролюйте доступ, рішення щодо цілісності системи та багатофакторну автентифікацію
Соціальна інженерія	✓	X	✓	Підвищення обізнаності, навчання операторів	Н/д
Ін'єкція / модифікація	X	X	X	Гібридні IDS машинного навчання, позначки часу	Аутентифікація повідомлення або цифровий підпис
Scanning	✓	X	X	Гібридна легка IDS або Honeypot	Зашифрований трафік / потік
Man-in-the-Middle	✓	X	X	Гібридна IDS	Багатофакторна автентифікація та легкий потужний протокол криптографічної автентифікації
Злом паролю	X	X	✓	Лайт IDS	Міцні періодичні паролі, надійне шифрування
Wi-Fi Aircrack	X	X	✓	Легкі IDS на фізичному рівні	Сильні та періодичні паролі, потужний алгоритм шифрування

Продовження Таблиці 1.3

Перешкоди Wi-Fi	X	X	✓	Перехід частоти, зміна діапазону частот	Н/д
Переповнення буфера	X	X	✓	Перехід частоти, зміна діапазону частот	Н/д
Denial of Service	X	X	✓	Перехід частоти, зміна діапазону частот	Н/д
ARP Cache Poison	X	X	✓	Перехід частоти, зміна діапазону частот	Н/д
GPS Spoofing	X	X	✓	Повернення до бази, зміна діапазону частот	Н/д

Висновки до першого розділу

Описано архітектуру безпілотника, типи зв'язку та типи БПЛА. Також різниця між безпілотниками, БПЛА та БПЛА.

Зауважено те, що все ще необхідні більш жорсткі правила, щоб забезпечити більш безпечне використання БПЛА та БПЛА, особливо внаслідок нещодавніх зустрічей між безпілотниками/БПЛА та іншими літаками.

Зазначено неохідність виокремлення безпеки основних програм БПЛА.

2 ДОСЛІДЖЕННЯ ПРОБЛЕМ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ БЕЗПІЛОТНИКІВ

Використання дронів дало переваги на багатьох рівнях - від комерційного до особистого. Однак безпілотні системи страждають від різних питань безпеки та конфіденційності. Порушення безпеки та конфіденційності, спричинені безпілотниками, повинні вирішуватися на найвищому національному рівні. Більше того, повинен існувати дуже суворий підхід, щоб обмежити можливість безпілотників збирати зображення та записувати відео людей та майна без дозволу.

З точки зору безпеки та аналізу загроз, мережа громадської безпеки за допомогою безпілотника відрізняється від традиційних безпроводових мереж, таких як безпроводові сенсорні мережі (WSN) та мобільні спеціальні мережі (MANET).

Це пояснюється тим, що вони несуть менше інформації та потребують менше енергії порівняно з мережею громадської безпеки за допомогою безпілотника. Більше того, зона охоплення безпілотника ширша та ширша, ніж WSN та MANET. Отже, виклики безпеці в першу чергу пов’язані з обмеженням ресурсів, а також обмеженнями затримки БПЛА. Крім того, важливо забезпечити дотримання конфіденційності, цілісності, доступності, автентифікації та невідмови від використання каналів зв'язку.

Це робиться відповідно до алгоритму AAA:

- Авторизація: шляхом надання привілеїв персоналу, який контролює БПЛА.
- Аутентифікація: шляхом забезпечення багатофакторної автентифікації з використанням чогось, що ви знаєте (сильний постійно мінливий пароль), чогось, що маєте (ім’я користувача), чогось, що є (біометричними) властивостями.
- Аудит: шляхом відстеження та/або арешту законних власників безпілотників/БПЛА у разі злочинної/зловмисної діяльності.

Застосування безпілотників зловмисними організаціями для здійснення фізичних та кібератак загрожує суспільству, порушуючи приватне життя його жителів, а також загрожуючи безпеці громадськості. Насправді різні технічні та експлуатаційні властивості безпілотника використовуються та використовуються з метою використання для потенційних атак. Сюди входить виконання критичних операцій, заснованих на наступальній розвідці, а також спостереження, спрямоване на відстеження конкретних людей та певних об'єктів, що викликає проблеми безпеки та конфіденційності [19].

З іншого боку, важливо запобігти використанню безпілотних літальних апаратів над житловими районами, що призводить до порушення конфіденційності через необдуману поведінку, оскільки зняті кадри можуть бути використані як для шахрайства, так і для шантажу. Порушення техніки безпеки також може статися у випадку несправності дрона та врізання в сусідній будинок, парк, припарковану машину або цивільних осіб. Це може призвести до матеріальних втрат/збитків та людських жертв/смертей.

Більше того, дрони переважно використовуються для націлювання на гостьові з'єднання Wi-Fi та/або на короткий діапазон Wi-Fi, Bluetooth та інших безпроводових пристроїв, таких як підключені через Bluetooth клавіатури. Такі з'єднання не захищені через поточні заходи безпеки, які передбачають, що ніхто не міг підійти настільки близько, щоб скомпрометувати їх або отримати доступ до внутрішніх мереж за допомогою безпроводових сигналів.

Ці припущення призводять до слабкої однофакторної автентифікації та використання типових паролів, які можна легко зламати, особливо за відсутності зашифрованого з'єднання. Це полегшує перехоплення інформації в приватній будівлі та в громадському кафе [20].

Зловмисник використовує такі вразливі місця, щоб порушити безпеку та/або конфіденційність. На рис.2.1 перелічені основні загрози безпеці безпілотників, а також відповідні методи їх подолання.

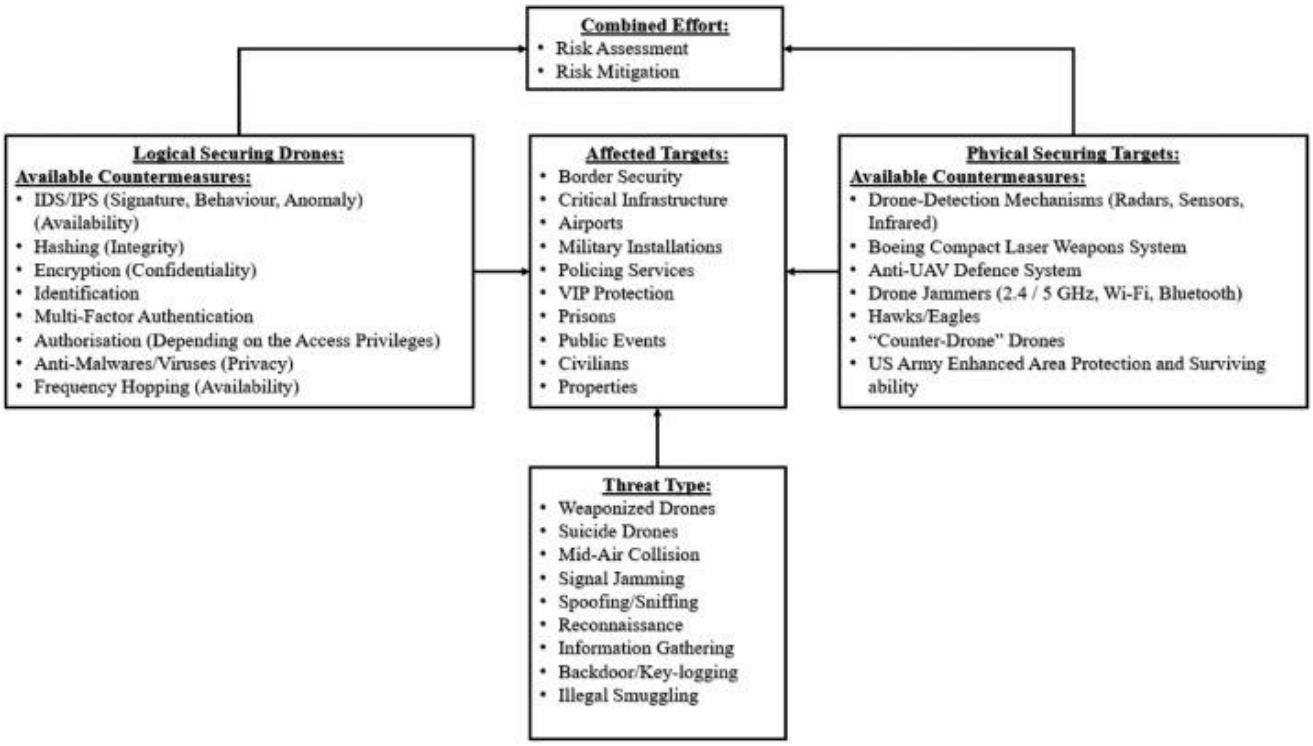


Рис.2.1 Основні загрози безпеці безпілотників

2.1 Дослідження проблем безпеки

До основних характеристик безпілотників відносяться невеликий розмір, низька вартість та простота маневреності та обслуговування. Це в свою чергу зробило їх кращим вибором для злочинців. Крім того, терористи почали спрямовувати свою увагу на використання цих безпілотників для здійснення терактів, головним чином через природу безпілотників, що робить їх менш схильними до виявлення.

Насправді, безпілотники можуть бути озброєні та модифіковані для перевезення небезпечних хімічних речовин, або бути оснащені вибухівкою для атаки критичних об'єктів інфраструктури. Більше того, безпілотники, що перевозять вибухівку, можуть бути підірвані навколо людей, які збираються у важкодоступних місцях. Це полегшує виконання терористом завдання, тим більше, що безпілотники забезпечують стелс смертника з радіусом дії літака. Військові аналітики стурбовані використанням безпілотників проти США з метою

шпигунства. Це пов’язано з тим, що ІДІЛ змогла переозброїти комерційні безпілотники та зробити їх придатними для бойових дій над Іраком та Сирією.

Тому безпека не завжди означає безпеку, і навпаки. Поза межами військового дому цивільні безпілотники/БПЛА також можуть вийти з ладу та врізатися в сусідній будинок або групу людей, спричинивши майновий/матеріальний збиток та людські травми/летальні випадки, починаючи від травми/тупи силова травма, травми глибоких порізів.

В результаті цього нижче перераховані основні проблеми безпеки:

- Відсутність конструктивних характеристик безпеки: це може призвести до того, що безпілотники вийдуть з-під контролю і полетять безцільно та автономно, не маючи можливості вимкнути його або відновити контроль.
- Відсутність технологічних та експлуатаційних стандартів: особливо, що стосується механізмів запобігання аварій, що призведе до нездатності БПЛА розпізнавати та ідентифікувати літаки та повітряно-десантні об’єкти та уникати їх.
- Перешкоджання викривленню сигналів: це робить БПЛА схильним до злому, викрадення та GPS/Signal-глушення в рамках кібертероризму чи кіберзлочинної діяльності, головним чином через те, що командно-контрольний оперативний центр БПЛА схильний до експлуатації.
- Відсутність урядового регулювання та обізнаності: особливо з точки зору практик безпеки та функцій, що забезпечують безпечну інтеграцію UAs до національного домену повітряного простору [21].

2.2 Дослідження проблем конфіденційності

Конфіденційність людей також ризикує бути викритою небажаними літаючими гостями, які можуть записати їх пересування та зробити знімки в будь-який час без їх відома чи дозволу. Це свідчить про те, наскільки наше приватне життя вразливе до такої загрози, що виникає.

Загалом загрози конфіденційності можна розділити на три основні категорії.

1. Фізична конфіденційність: базується на польоті безпілотних літальних апаратів над чиєюсь власністю або на рівні їхніх вікон. Це дозволяє зловмисникам таємно збирати зображення та записувати відео певних людей, можливо, невідповідними способами, загрожуючи їх особистій свободі.

2. Конфіденційність місцезнаходження: заснована на відстеженні та виявленні людей, які летять і гудуть над ними безпілотником, не знаючи, що вони перебувають під наглядом.

3. Конфіденційність поведінки: це те, коли присутність літаючого безпілотника може вплинути на те, як люди діють і реагують, особливо коли знають, що вони перебувають під наглядом. Як наслідок, це також обмежує їх свободу, порушує конфіденційність та обмежує свободу.

Безпека та конфіденційність є ключовими вимогами до впровадження будь-якої нової технології IoT, особливо безпілотників та БПЛА.

2.3 Аналіз існуючих загроз та вразливостей безпілотним літальним апаратам

БПЛА та безпілотники сприймаються як життєздатні та життєво важливі загрози для інформаційної безпеки. Багато БЛА мають серйозні конструктивні недоліки, і більшість із них розроблені без захисту безпроводового захисту та шифрування каналів.

- Схильність до спуфінгу. Аналіз конфігурації та контролерів польоту моделей БПЛА з кількома роторами виявив багато слабких місць. Вони пов'язані як з телеметричними посиланнями, що передають дані до/з дрону через з'єднання послідовних портів, особливо через слабкий характер зв'язку, який у більшості випадків не шифрується. Проведені експерименти показали, що за допомогою спуфінгу GPS інформація може бути легко захоплена, змінена або введена [22]. Ця вразливість у каналі передачі даних дозволяє перехоплювати та підробляти, надаючи хакерам повний контроль над дроном.

- Схильність до зараження шкідливим програмним забезпеченням. Протоколи зв'язку ввімкнені в БПЛА, щоб дозволити користувачам керувати безпілотниками за допомогою безпроводового пульта дистанційного керування, такого як планшети, ноутбуки та мобільні телефони. Однак ця техніка виявилась небезпечною, адже дозволяє хакерам створити корисне навантаження TCP із зворотнім зв’язком, вводячи його в пам'ять безпілотника, який приховано встановлюватиме шкідливе програмне забезпечення в системах, що працюють на наземних станціях.
- Схильність до втручання та перехоплення даних. Канали телеметрії використовуються для моніторингу транспортних засобів та полегшення передачі інформації через відкриту незахищену безпроводову передачу, роблячи їх вразливими до різних загроз. Сюди входять перехоплення даних, зловмисне введення даних та зміна заздалегідь встановлених шляхів польоту. Це дозволяє встановлювати та вставляти багато заражених цифрових файлів (відео, зображень) з безпілотника на наземну станцію. Ще одна вразливість була виявлена та пов’язана з модулем зв'язку БПЛА, який використовує безпроводовий зв’язок для обміну даними та командами із наземною станцією [23].
- Схильність до маніпуляцій. Оскільки безпілотні літальні апарати літають за попередньо запрограмованими та заздалегідь визначеними маршрутами, може відбуватися маніпуляція, яка потенційно може мати серйозні наслідки. Варіюється від викрадення вантажів високої вартості, до перенаправлення БПЛА для доставки вибухівки, біологічної зброї чи іншого корисного вантажу терористів через підробку RF або GPS, що дозволяє зловмиснику отримати контроль над безпілотником, надсилаючи фальшиві сигнали, або глушить його мета його збою.
- Схильність до технічних проблем. Багато дронів страждають від різних технічних несправностей. Сюди входять помилки додатків, такі як збій з'єднання між пристроєм користувача та дроном, внаслідок чого він або виходить з ладу, або злітає. Інші питання пов’язані з відсутністю стабільного зв’язку, особливо за складних природних причин; тривалість роботи акумулятора, що призводить до дуже обмеженого часу польоту, перш ніж готувати знову. Зверніть увагу, що в

холодну погоду термін служби акумуляторів скорочується, що призводить до коротшого часу польоту, а також можливих несправностей.

- Схильність до експлуатаційних питань. Ще однією головною проблемою є відсутність навичок польоту власників безпілотників та тип використовуваних безпілотників. Це може завдати серйозної шкоди та/або травмувати майно та/або персонал. Насправді, безпілотники виготовляються чутливо, тому невелика аварія може збити дрон. У багатьох випадках, якщо одна з ротацій порушує роботу або перестає працювати, це може спричинити серйозну турбулентність, важко зберегти контроль над безпілотним апаратом. Це, в більшості випадків, призвело б до падіння безпілотника.
- Схильність до природних проблем. У багатьох випадках дрони не витримують вітру через свою легку конструкцію. Більш того, екстремальні спекотні умови можуть призвести до поломки двигуна. Крім того, акумулятор може вибухнути та спричинити серйозні пошкодження та шкоду. Інше питання - нездатність дронів літати під дощем, оскільки вони не оснащені водонепроникним захистом. Зазвичай, коли дрони врізаються в озера, річки, пляжі або навіть басейни, вони відразу ж припиняють роботу. Крім того, під час туману власникам не рекомендується керувати безпілотниками через обмежену видимість, яка зменшується з кількох метрів до менш ніж метра, що призводить до порушення комунікації між безпілотником і GPS, відправляючи дрон за межі його зони управління до аварій.
- Схильність до перешкод Wi-Fi. Безпілотники також можуть бути викрадені, надіславши процес зняття автентичності між точкою доступу та пристроєм, що керує дроном, що можна зробити тимчасово або назавжди, наприклад, перешкодити передбачуваній частоті дронів та заманити його для підключення до Wi-Fi хакера; це можна зробити, встановивши та налаштувавши raspberry-pi для такої роботи.

2.4 Дослідження існуючих кіберзаходів для захисту безпілотних літальних апаратів

Основні контрзаходи, які можна вжити для захисту безпілотників від атак безпеки, можна класифікувати на декілька типів, що базуються на основних мотивах, цілях та ідеях зловмисника. Далі обговорюються існуючі рішення для захисту мереж, комунікацій та даних безпілотників. Крім того, перераховані та описані існуючі криміналістичні рішення, що використовуються під час розслідувань атак безпілотників та спрямовані на виявлення першопричин таких атак.

2.4.1 Захист мереж безпілотників/БПЛА

Безпроводові мережі страждають від кількох загроз безпеці. Нещодавно були розгорнуті Системи виявлення вторгнень (IDS) для виявлення зловмисних дій БПЛА/безпілотників та виявлення підозрілих атак, які можуть бути націлені на них. Як правило, IDS контролює вхідний та вихідний мережевий трафік та аналізує їх для виявлення аномалій. Їх метою є виявлення та ідентифікація кібератак шляхом вивчення перевірок даних (слідів), які були зібрані в різних частинах мережі.

Різні підходи IDS для захисту дронівських мереж від зловмисників представлені нижче.

1. Виявлення вторгнень на основі правил. В домені БЛА використовуються системи виявлення вторгнень на основі правил для захисту зв'язку між літаком та наземною станцією. Метою є виявлення неправдивих атак введення даних, особливо тих, що націлені на потужність сигналу. Вони довели, що нападників можна виявити протягом 40 секунд. У [24] Мітчелл і Чен представили методику виявлення, засновану на специфікації, для захисту системи БПЛА від різних типів кібератак. Автори спиралися на UAV-IDS на основі правил поведінки. Правила поведінки були побудовані на основі визначених моделей атак, включаючи необдумані, випадкові та опортуністичні атаки. Це дозволило

мінімізувати помилки виявлення, включаючи хибнопозитивні та помилково негативні показники, з критичним компромісом між безпекою та характеристиками БПЛА. У роботі [25] Мітчелл та ін. представив BRUIDS, адаптивну систему поведінки на основі специфікації правил поведінки, яка виявляє зловмисні БПЛА в повітряно-десантних системах. Автори також дослідили ефективність BRUIDS щодо необдуманої, випадкової та кон'юнктурної поведінки зловмисників, щоб швидко оцінити виживаність БПЛА проти зловмисних атак. Результати моделювання показали, що BRUIDS досягає більш високого рівня виявлення в порівнянні з підходом IDS на основі багатоцільової аномалії та з меншим коефіцієнтом помилково позитивних. Однак IDS на основі правил страждають від управління їх складністю, що вимагає втручання людини для конфігурації правил. Крім того, цей тип IDS не здатний виявляти невідомі атаки.

2. Виявлення вторгнень на основі підписів. У [26], Kacem et al. представив систему виявлення вторгнень ADS-B для захисту літака від кібератак, спрямованих на повідомлення ADS-B. Така структура базується на методах виявлення підписів, які аналізують GPS-положення літального апарату. У роботі [27] Casals et al. розробив схему виявлення з використанням біологічного натхнення для виявлення кібератак, спрямованих на повітряні мережі. Однак, подібно до IDS на основі правил, IDS на основі підпису не може виявити невідомі атаки або атаки за допомогою динамічних підписів.

3. Виявлення на основі аномалії. IDS на основі аномалії в домені БПЛА в основному використовується для запобігання атакам заклинювання. У [28] Рані та співавт. представив алгоритм навчання на основі аномалій для захисту вузлів БЛА від DoS та DDoS-атак. У роботі [29] Lu та співавт. представив посилену на основі навчання систему виявлення аномалії температури двигуна для БПЛА, яка запобігає роботі двигунів безпілотника при ненормальних температурах, використовуючи датчики DS18B20 для реєстрації температури та процесор raspberry-pi для обробки. Ця система пропонує можливість уникнути поломки двигуна шляхом посадки безпілотника в разі перегріву; проте це не повністю запобігає проблемі. Експериментальні результати виявляють можливість

безпечного управління безпілотником на основі інформації датчиків. У роботі [30] Condomines et al. представив гібридний IDS на основі спектрального аналізу трафіку та надійний контролер для оцінки аномалії в мережах БЛА в Flying Adhoc Network (FANET). Ця методика була націлена на розподілені атаки DoS, і її ефективність була перевірена на трафіку в режимі реального часу. Результати показали точне виявлення різних типів аномалій. Однак для забезпечення його ефективності все ще потрібні подальші випробування.

У роботі [31] Sedjelmaci et al. представив систему виявлення та реагування на вторгнення (IDRF) для захисту мережі БПЛА від цілісності даних та атак доступності мережі, а також для захисту VANET, що підтримується БЛА, від шкідливих загроз. Автори зазначили, що запропонована структура є унікальною як гібридна техніка виявлення для мереж БПЛА.

У роботі [32] Lauf et al. представив децентралізовану методику виявлення на основі аномалії з використанням методів виявлення максимумів та крос-кореляції. Насправді, системи виявлення Maxima (MDS) забезпечують характеристику одного або нульових підозрілих вузлів, тоді як методи перехресного кореляційного виявлення (CCD) виявляють численні вторгнення. Однак їхній підхід страждає від неточностей щодо хибнопозитивних та помилково негативних показників.

Крім того, Sedjelmaci та співавт. представив ієрархічну схему виявлення та реагування на вторгнення для підвищення безпеки мереж БПЛА від руйнівних кібератак, таких як розповсюдження неправдивої інформації, спуфінг GPS, заміна та атаки чорних дір та сірих дір. Ця схема працює на рівні БПЛА та наземної станції для виявлення шкідливих аномалій мережі. Результати моделювання показали високий коефіцієнт виявлення 93,3% та низький показник хибнопозитивних результатів менше 3% при низьких накладних витратах на зв'язок.

У роботі [33] Мітчелл та ін. представив IDS на основі специфікації для захисту датчиків і виконавчих механізмів, вбудованих в БАС. Для оцінки ефективності їхнього рішення IDS тестували на БПЛА, щоб дослідити вплив поведінки зловмисника. Результати показали, що рішення ефективно торгує

помилково позитивним коефіцієнтом для високої ймовірності виявлення, щоб запропонувати кращий захист для програм UAS.

З огляду на те, що шлюзи безпілотних мереж можуть працювати з деякими обмеженнями (вузли туману), існує потреба в полегшеній техніці виявлення аномалій на основі хоста, яка вимагає міні-обчислювальних ресурсів. Цього можна досягти за допомогою простої техніки машинного навчання або статистичного підходу з мінімально можливою кількістю функцій. Структура стійкого IDS повинна базуватися на гібридному підході, де підходи, що базуються на правилах або підписах, використовуються для відомих атак та підхід на основі аномалії для виявлення аномальної поведінки. Така система залежала б від експертів з машинного навчання та безпеки людини.

2.4.2 Захист зв'язку безпілотників/БПЛА

Через збільшення кількості перехоплення кадру безпілотника/БПЛА були представлені різні рішення для забезпечення зв'язку БПЛА. У роботі [34] Zhang et al. було розглянуто питання безпеки фізичного рівня в системах зв'язку БПЛА та представлено ітераційний алгоритм, заснований на блочному спуску координат та послідовних опуклих методах оптимізації. Результати моделювання показали значне поліпшення щодо рівня секретності систем зв'язку БПЛА.

Автор Zhang et al. застосували ці алгоритми для вирішення проблем трансляції, прямої видимості та бездротових каналів «земля-земля», пов'язаних з бездротовими мережами п'ятого покоління (5G). Результати моделювання показали поліпшення рівня секретності для зв'язку БПЛА на землю (U2G) та наземного зв'язку на БПЛА (G2U).

У роботі [35] Cui та співавт. також розглянули характер трансляції бездротових каналів прямого огляду "повітря-земля" та вирішив її на основі фізичного рівня, використовуючи дизайн траєкторії мобільності БПЛА. Автори представили ітераційний субоптимальний алгоритм, застосувавши метод блочного координатного спуску, S-процедуру та послідовний метод опуклої оптимізації.

Результати моделювання показали значне покращення середнього рівня найгіршої секретності.

У роботі Zhao et al. представив кешовану схему безпечної передачі БПЛА в надщільних базових станціях малих комірок (SBS) на основі вирівнювання перешкод, щоб розвантажити трафік через бездротовий зворотний зв'язок та поліпшити покриття та швидкість за рахунок генерування сигналів перешкод, щоб порушити будь-яку потенційну спробу підслуховування. Результати моделювання показали ефективність їх методів. У роботі Lee et al. дослідив захищений зв’язок, що підтримується БПЛА, із кооперативним глушителем БПЛА та представив ітераційний алгоритм, який забезпечує ефективне рішення для мінімальної задачі максимізації швидкості секретності шляхом спільної оптимізації потужності передачі, траєкторії руху БПЛА та змінних планування користувачем. Чисельні результати показали, що алгоритм перевершує базові методи. У роботі Liu et al. вивчив проблему безпеки в системах зв'язку, що підтримуються БПЛА, і представив схему безпечної передачі каналу прослуховування БПЛА із використанням багатоантенного джерела, яке передає на одну антену БПЛА, у присутності повнодуплексного активного підслуховувача. Багатоантенне джерело передає штучні шумові сигнали разом з інформаційними сигналами, щоб перешкодити повнодуплексному підслуховуванню здатності підслуховувати та заклинювати.

На додаток до методів модуляції, важливим є шифрування зв'язку безпілотників та БПЛА. У цьому контексті нещодавно були представлені різні криптографічні рішення, включаючи шифрування повідомлень та автентифікацію. Оскільки більшість стандартів дронів повинні забезпечувати безпечний зв’язок, основна увага приділялася тому, як розробити легкий алгоритм автентифікації та шифрування повідомлень. Крім того, це можна зробити таким чином, щоб зберегти аутентифікацію джерела на додаток до цілісності та конфіденційності переданих даних. Існуючі криптографічні алгоритми для захисту дронівських комунікацій можуть бути застосовані для забезпечення зв'язку дронів, що використовуються для цивільних застосувань. Більше того, захищений протокол зв'язку (eCLSC-

TKEM) між безпілотниками та розумними об'єктами кращий в 1,3, 1,5 та 2,8 рази за інші протоколи, включаючи протоколи в CLSC-TKEM від Seo, CL-AKA від Sun та CL-AKA від Yang.

Крім того, в роботі [36] Sharma та співавт. представив високозахищену техніку функціонального шифрування (FE), щоб захистити гетерогенну мережу (HetNet), що підтримується БПЛА, у щільних міських районах від шкідливих дій, а також захистити критичними даними користувачів за допомогою шифрування; однак це рішення вимагає подальших удосконалень.

З іншого боку, автор Chen et al. представив схему автентифікації, що простежується та захищає конфіденційність (TPPA) для систем управління зв’язком БПЛА. TPPA інтегрує криптографію кривої еліптичної кривої (ECC), цифровий підпис, хешування та інші механізми криптографії для застосування БПЛА. Це забезпечує конфіденційність, конфіденційність, цілісність, доступність, анонімність та відмову від використання, особливо проти DoS та підміни, з низькими обчислювальними та комунікаційними витратами.

Працюючи на великих відстанях на пристроях з підтримкою акумулятора, безпека дронівського зв’язку вимагає легких криптографічних алгоритмів та протоколів. Нещодавно були представлені нові криптографічні алгоритми з функціями одного раунду або малою кількістю ітерацій. Більше того, існуючі протоколи автентифікації, що зберігають конфіденційність, можуть використовувати такі легкі криптографічні алгоритми для мінімальної затримки. Також параметри фізичного рівня можна використовувати для багатофакторної автентифікації.

2.4.3 Захист даних безпілотників

Всі дані, захоплені безпілотниками, повинні бути зведені, щоб мінімізувати трафік, який постійно надсилається на базову станцію. Однак агрегування зашифрованих даних ставить нові виклики. Відповідно, була представлена робота, в якій описано метод гомоморфного шифрування (HE) та практична схема

агрегування даних, заснована на добавці HE. На жаль, існуючі рішення ВНЗ страждають від проблем безпеки та/або продуктивності.

Симетричні шифри страждають від проблем із безпекою, особливо з точки зору обраних атак на відкритий текст/шифртекст, тоді як асиметричні шифри страждають від великих накладних витрат на обчислення та ресурси, крім пов'язаних із цим накладних витрат на зберігання.

1. Криміналістичні рішення. Цифрові криміналістичні методи широко використовуються в домені БПЛА/безпілотника. Загальна основа для Мережевої криміналістики (NF) включає аналіз мережевих даних, що проходять через брандмауери або системи виявлення вторгнень. Це дозволяє мережевому розслідуванню виявляти та виявляти аномалії трафіку. Метою такої моделі є відстеження джерела нападу за допомогою шестифазного ланцюжка опіки. Інша структура використовує процес цифрового розслідування (DIP) для просування всебічної багаторівневої ієрархічної цифрової моделі розслідування.

Ця структура включає два рівні: перший рівень включає фазу оцінки та реагування на інциденти, фазу збору та аналізу даних, представлення висновків та фазу закриття інциденту, другий рівень включає об'єктну підфазу.

Проте було висвітлино різні проблеми криміналістичної роботи безпілотних літальних апаратів та представлено результати їх цифрового криміналістичного аналізу, проведеного на безпілотнику Parrot AR 2.0. Аналіз включав можливість доступу до медіа-файлової системи за допомогою протоколу передачі файлів (FTP) або послідовних з'єднань для отримання всієї необхідної інформації цифровими криміналістами, включаючи ідентифікатор Android контролера, який використовується для встановлення права власності.

Автор Barton et al. висвітлив використання інструментів криміналістики з відкритим кодом та розробив базові сценарії, які допомагають криміналістичному аналізу DJI Phantom 3 Professional та AR Drone 2 у поліматичному робочому стилі, маючи на меті реконструювати дії, які вчинили ці безпілотники, визначивши операторів безпілотників. та витяг даних із пов’язаних з ними мобільних пристроїв.

Це можна зробити, проаналізувавши журнали польотів та виявивши артефакти та захопивши цифрові носії безпілотників.

У роботі [37] Clark et al. представив інструмент криміналістики з відкритим кодом DRone Open Source Parser (DROP), який аналізує власні файли даних, витягнуті з енергонезалежної внутрішньої пам'яті DJI Phantom III, та текстові файли, розташовані на мобільному пристрої, що керує дроном. Результати показали, що можна ідентифікувати місцезнаходження GPS, акумулятор та час польоту, а також можливість зв’язати даний безпілотник з керуючим мобільним пристроєм на основі його серійного номера. Подальші результати показали, що дані можна отримати на криміналістичній основі шляхом ручного вилучення картки Secure Digital (SD) дрону.

Мантас та співавт. дослідив найбільш часто використовувані криміналістичні платформи, такі як Ardupilot, журнали флеш-даних та телеметрії, перед тим як представити власний інструмент криміналістики з відкритим кодом, Gryphon, який фокусується на журналах польотних даних безпілотника з точки зору наземної станції управління, збирає, вивчає та аналізує судово-медичні артефакти для побудови відповідного строку подій, щоб винні могли бути притягнуті до відповідальності.

Jain et al. представив основу цифрового криміналістичного розслідування на основі події в результаті процесу розслідування на основі місця фізичного злочину. Ця структура допомагає перевіряти та розробляти гіпотезу шляхом реконструкції події на основі зібраних доказів, що проходять після фази готовності та розгортання, фази розслідування місця фізичного злочину, фази розслідування місця цифрового злочину та фази презентації.

Більше того, було представлено процес судового розслідування БПЛА, який пройшов покроковий процес, заснований на трьох основних початкових фазах.

Етап підготовки. Визначити ланцюг командування, оскільки БПЛА буде першим обладнанням, яке буде вилучено після аварії. Це дозволяє проводити звичайну судово-медичну практику для виявлення будь-якої ДНК або відбитків пальців на безпілотнику/БПЛА. Таким чином, цифрові докази можуть

поєднуватися з традиційними доказами, такими як показання свідків. Потім проводиться «аналіз правопорушень» для ідентифікації використовуваного пристрою, визначення поточної дати та часу та ідентифікації поточного оператора БПЛА шляхом відстеження його адреси та вилучення їх пристрою.

Етап обстеження. Базується на виявленні можливостей відео/аудіозапису та зйомки зображень безпілотника. Це робиться шляхом визначення місць зберігання даних, таких як знімні, стаціонарні та флеш-карти пам'яті, а також визначення відкритих портів зв'язку для подальшого перехоплення трафіку. Це вимагає неруйнівних методів, для захисту вихідних даних, використання комерційних або некомерційних інструментів криміналістики, або використання методу руйнівного вилучення.

Етап звітності та аналізу. Базується на первинному огляді вилучених даних, оскільки перші збережені зображення - це власні зображення підозрюваного, включаючи початкове місце зльоту/посадки, наявний персонал, місце розташування, координати району тощо. Таким чином, важливо знати, як працює функція запису, щоб перехопити дані та перевести їх у зручну для читання форму.

Крім того, існує добре підібрана криміналістична модель під назвою «модель водоспаду» у відповідь на значні відмінності між комерційними моделями. Ця модель включає декілька фаз, що дозволяють цифровому досліднику перевірити всі попередні етапи під час процесу розслідування, включаючи фазу підготовки та ідентифікації, фазу вимірювання ваги та перевірки налаштувань, фазу відбитків пальців, фазу карти пам'яті, геолокацію фаза та фаза Wi-Fi та Bluetooth.

Однак нещодавно було розроблено декілька антикриміналістичних методів, які не дозволяють слідчим знаходити та/або збирати докази, що вимагає розробки ефективних контрзаходів для відновлення дійсних доказів. Такі анти-антикриміналістичні рішення повинні бути розроблені таким чином, щоб зберегти основні функціональні можливості безпілотних літальних апаратів, водночас протистоячи анти-криміналістичним методам.

Підсумовуючи, у цьому розділі розглянуто існуючі рішення безпеки для захисту безпілотних систем, включаючи криптографічні та некриптографічні

рішення. Криптографічні рішення по суті спрямовані на захист зв'язку безпілотників та переданих даних, тоді як некриптографічні рішення (IDS) спрямовані на виявлення та відновлення від можливих атак безпеки.

2.4.4 Контрзаходи проти дронів

Оскільки кількість інцидентів між безпілотниками та літаками постійно зростає, стало важливим вирішити питання про порушення безпеки та конфіденційності на найвищому національному рівні.

Це включає прийняття дуже суворих підходів, які обмежують можливість безпілотника збирати зображення та записувати відео людей та майна без чітко дозволеного дозволу. Насправді, оскільки багато людей не читають інструкцію належним чином, вони не здатні належним чином реагувати у випадку несправності.

На рис.2.2 представлено можливі атаки безпілотників та відповідні контрзаходи. Адже основу для захисту різних компонентів системи БПЛА. Існують різні методи злому та/або викрадення безпілотника, або за допомогою традиційних методів (про які йдеться нижче), або за допомогою нової форми, яка називається «рубати і ламати».

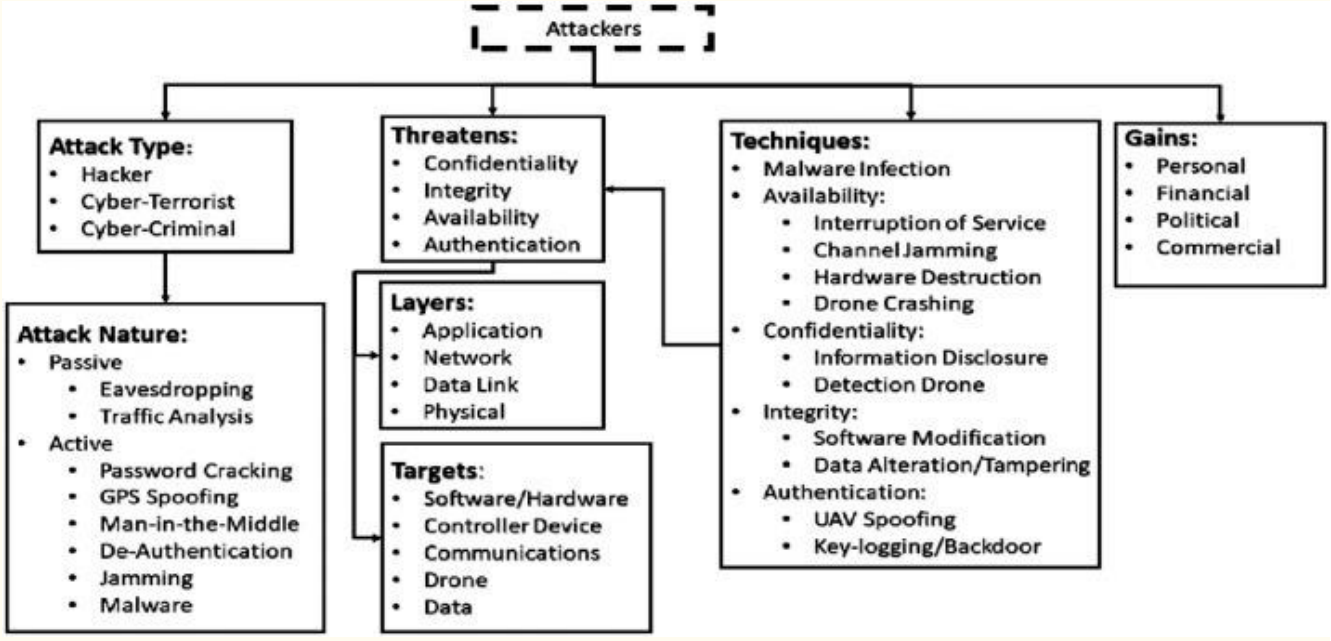


Рис.2.2. Можливі атаки безпілотників та відповідні контрзаходи

Цивільні контрзаходи поділяються на фізичні та логічні контрзаходи.

1. Фізичні контрзаходи. Коли безпілотники стали широко популярними, багато організацій витрачали час та ресурси на пошук способів запобігти їх використанню в обмеженому повітряному просторі та над своїми будівлями.

- Ловці безпілотників - великі безпілотники, обладнані мережами, такі як «робот-сокіл».
- Drone Defenders - захисники безпілотники (Dedrone), які використовуються для скидання безпілотників з неба за допомогою радіохвиль.
- Електрична огорожа - встановлена електрична огорожа, підключена до хмари БСА, для виявлення та запобігання проникненню БАС у заборонені зони, особливо за межі ВЛОС.

2. Логічні контрзаходи. Ці заходи включають використання логічного обладнання, а не дорогого фізичного обладнання. Наприклад, Hooper et al. провели тестування пера на БПЛА Parrot Bebop і виявили, як БПЛА Parrot на базі Wi-Fi схильні до вразливостей нульових днів та різних атак, таких як Протокол дозволу адрес (ARP) та атаки отруєння кешу. Отже, автори представили багаторівневу систему безпеки як поглиблений захист для захисту БПЛА від вразливостей нульових днів. У роботі Birnbaum et al. представив прототип системи моніторингу БПЛА, яка збирає дані польоту та виконує оцінку та відстеження параметрів планера та контролера в реальному часі шляхом їх порівняння з раніше відомими параметрами. Це було зроблено за допомогою методу рекурсивних найменших квадратів (RLSM), який виявляє кібератаки та початкову деградацію апаратного забезпечення та збої. Експериментальні результати показали, що можна автоматично встановлювати параметри польоту БПЛА, одночасно досягаючи ефективного виявлення аномалії в польоті для виявлення значних відхилень.

Однак інші рішення щодо безпеки були представлені для БПЛА, як було представлено далі.

- Перешкоди Wi-Fi. Це перший метод, який застосовується, коли дрони використовують частоту 2,4 ГГц. Це заважає усім бездротовим комунікаціям у

визначеній зоні покриття. Однак здатність перешкод дуже обмежена і не може бути прихована, оскільки її можна легко виявити, і вона заклинює інші сусідні частоти.

- Тристороннє рукостискання. Цей процес заснований на рукостисканні між точкою доступу маршрутизатора та новим інтегрованим неправдивим пристроєм. Це дозволяє зловмисникові скасувати автентифікацію або навіть заблокувати зв'язок між дроном та пристроєм, що ним керує. Більше того, таке рукостискання можна використовувати для запуску атаки злому пароля, особливо якщо дрон надійно захищений.

– Wi-Fi Aircrack. Наприклад, атака Wi-Fi (SkyJet) - дозволяє зловмиснику шукати безпілотники поблизу і викрадати їх, перетворюючи на «зомбі-дронів». SkyJet використовує aircrack-ng для виявлення сусідніх бездротових мереж та клієнтів перед тим, як вимкнути контролер дрону. Це завдання виконується під час підключення зловмисника до безпілотника, що забезпечує повний контроль над безпілотником жертви. Цей тип атак базується на трьох основних фазах: перший модуль - безпроводовий інструмент, такий як «airodump», спрямований на виявлення мереж із підтримкою WEP та WPA-2, а також відкритих мереж. Другий модуль - інструмент для впорскування, такий як «показ повітря», що використовується для збільшення трафіку. Третій модуль - «aircrack-ng», що дозволяє зловмиснику проводити атаку скасування автентифікації. Така атака може порушити з'єднання Wi-Fi, захищене шифруванням WPA2.

- Повторне відтворення. Це DoS-подібна атака, яка перехоплює передані дані, а потім або затримує їх, або повторно передає пізніше. Насправді, повторне відтворення запиту Протоколу роздільної адреси (ARP) також може бути використане для спроби зламу ключів шифрування, особливо якщо зв’язок між дроном та пристроєм надійний.

- Переповнення буфера. Це DoS-подібна атака, яка перехоплює мережевий трафік і заповнює його постійними запитами на порушення з'єднання дрону/пристрою. Ця атака відбувається, коли сценарій JSON робить запит стати контролером з атакуючого комп’ютера для захоплення мережевого трафіку через Wireshark, на додаток до вбудованої статистики з каталогу/proc/stats.

– Відмова в обслуговуванні (DoS). Виконується або шляхом зняття автентичності, або перешкод Wi-Fi, використовуючи «Kali-Linux» як платформу, щоб спричинити збій БПЛА. Процес зняття автентичності може надсилатися періодично або постійно, використовуючи: команду «airodump-ng» для оцінки безпеки мережі дрону, команду «Aireplay-ng» для відключення будь-якого підключеного пристрою, «aircrack-ng», щоб розірвати будь-яке безпечне з'єднання безпілотника/пристрою.

Що стосується перешкод Wi-Fi, то перешкода Wibs Fi Websploit може бути використана як ідентифікатор розширеного набору послуг (ESSID) пристрою (MAC-адреса точки доступу дрону), так і ідентифікатор базового набору послуг (BSSID) (номер каналу дрону/пристрій зв'язку).

- ARP Cache Poison. Це тип атаки «людина посередині» і запускається для переривання, зупинки або зміни мережевого трафіку. Для здійснення цієї атаки використовується комп’ютер, який безперервно виконує шкідливий скрипт під назвою «Scapy» через бібліотеку Python, поки дрон не від’єднається від підключеного пристрою.
- Ін’єкція та модифікація. Також відома як атаки цілісності. Такі атаки засновані на зміні конфіденційної інформації законного повітряного судна шляхом введення неправильних даних. Це дозволяє модифікувати вміст і, можливо, завантажувати заражені дані, щоб забезпечити бэкдор до наземної системи управління.
- Цивільна підробка GPS. Дуже важливо переконатися, що дані GPS є законними, інакше це призводить до помилкової оцінки положення пристрою. Це може призвести до провалу місії та, можливо, втрати активів.
- Атака віддаленого спуфінгу - спуфер знаходиться на незначній відстані з точним вирівнюванням підроблених та автентичних сигналів, що можливо лише при точному запропонованому положенні на рівні метра.

У табл.2.1 представлена класифікація атак БЛА на основі їх класу та того, чи є ціль лише однією чи кількома цілями безпеки.

Таблиця 2.1

Аналітичний огляд методів виявлення безпілотників/БПЛА

Метод	**Operational**		**Опис**			
Тип	**Відстань**	**Поля**	**Характеристики**	**Точність**	**Переваги**	**Обмеження**
На основі аудіо	7-9м	Відкриті поля	Багатонаправлений мікрофонний масив	змінні	Виявляє безпілотники / БПЛА, що дзижчать звуковими хвилями	Близька дальність, шумові перешкоди
На основі відео	105 м	Міські/сільські райони	Зйомка зображення на великій відстані	Помірний/низький	Хороша роздільна здатність захоплення зображення	Висока помилка виявлення, не розрізнення між птахами та трутнями
На основі руху	15-45м	Відкриті поля	Визначення руху та швидкості	Прийнятний	Успішне виявлення безпілотників серед літаючих об'єктів	Близька дальність
На тепловій основі	105 м	Міські/сільські райони, відкриті поля	Виявлення тепла	Високий/низький	Точний при виявленні безпілотників із фіксованим крилом	Неточний при виявленні менших квадрокоптерів
На основі радарів	45-500 м	Міські/сільські райони, відкриті поля	Виявлення тепла, руху та шуму	Високий / помірний	Високоточний при виявленні / пошуку великих / середніх безпілотників / БПЛА	Неточний при виявленні / розташуванні малих / крихітних безпілотників / БПЛА
На основі ВЧ	50–500 м	Міські / сільські райони, відкриті поля	Виявлення / перехоплення радіочастотного сигналу	Високий / помірний	Успішний при виявленні / перехопленні сигналів та пошуку дронів	Схильний до перешкод сигналу, не в змозі виявити більш високі / низькі частоти

3. Військові контрзаходи. Приклади військових методів протидії безпілотним атакам включають використання старого радянського зенітного озброєння (тобто ЗСУ-23-4 Шилка та ракет «земля-повітря» (ЗРК С-300/С-400), ракети).

Недавні дослідження показали, як терористи переходять до нової асиметричної війни, яка називається «війна безпілотників». З цієї причини було запропоновано та реалізовано чотири основні різні військові контрзаходи для подолання загроз безпеці БПЛА.

До найновіших високоточних засобів протидії безпілотникам у режимі реального часу відносять:

- ATHENA: або Advanced Test High Energy Asset - це оновлення системи захисту від боєприпасів (ADAM), яка являє собою систему лазерної зброї потужністю 30 кВт, яка використовує лазер прискореної лазерної демонстрації (ALADIN) потужністю 30 кВт, який поєднує в собі потужність трьох волоконних лазерів потужністю 10 кВт в один промінь. ATHENA також може працювати на рівнях 10 і 20 кВт. Ця система фінансується та тестується Lockheed Martin, і вона може працювати на тисячі метрів.
- Rafael Drone Dome: це протидіюча оперативна мобільна система, що використовується для виявлення, відстеження та усунення ворожих безпілотників (навіть під час маневрування) розміром 0,002 м2 на відстані 3,5 км за допомогою потужного лазерного променя , що дає можливість м’якого та жорсткого вбивства. Результати тестування показують його здатність успішно своєчасно ліквідувати три безпілотники.
- Компактна система лазерної зброї Boeing (CLWS): використовується для відстеження та відключення БПЛА за допомогою системи лазерної зброї для отримання, відстеження та ідентифікації потенційних цілей або навіть їх знищення. Основні його переваги засновані на тому, що він портативний, і його можна зібрати майже за 15 хвилин. Більше того, він може знищити ціль з 22 миль за 10 секунд, використовуючи енергетичний пучок 2, 5 або 10 кВт.
- Система захисту від БПЛА (AUDS): це система проти БПЛА, розроблена британськими оборонними компаніями для вирішення зростаючих

загроз БЛА. Він класифікується як пакет інтелектуальних датчиків та «ефекторів» з можливістю віддаленого виявлення невеликих БПЛА, відстеження та класифікації їх перед наданням можливості порушити їх діяльність. Серед характеристик - містить електронно-скануючий радар, спрямований на виявлення цілей, електрооптичне відео для відстеження і класифікації цілей, а також програмне забезпечення, відоме як «інтелектуальний спрямований інгібітор РЧ». Діапазон його виявлення становить до 10 км при мінімальному розмірі цілі 0,01 м2. Більше того, він здатний працювати в різних погодних умовах і цілодобово.

- Контр-ракета та міномет (CRAM): це ракетна система протиракетної, артилерійської та мінометної оборони, розроблена в рамках технології посиленого захисту та виживання армії США (EAPS), з розширенням, що включає загрози із безпілотних літальних систем або безпілотників. Насправді CRAM є сухопутною версією Phalanx CIWS. Серед його характеристик - використання 20-міліметрової HEIT-SD (сильно вибухонебезпечний запалювальний індикатор, самознищення), 30, 50 або 76-міліметровий боєприпас із зменшеним часом польоту (DART), запустити керовані перехоплювачі з використанням точного радіолокаційного інтерферометра у якості датчика, комп'ютера управління вогнем (CC), а також радіочастотного приймача для запуску снаряда в «кошик» залучення. Потім обчислення проводяться на місцях, і інформація передається назад до ЦК.
- Некінетичні методи: інші контрзаходи включають некінетичні методи, такі як використання радіохвиль для зриву польоту безпілотників. Однак через класифікацію правил бойових дій важко сказати, за якими варіантами та зброєю може застосовуватись армія.
- Цапери проти БПЛА. Цапер відповідав за збиття понад 500 безпілотників

2.5 Методи виявлення безпілотників

Зростання БПЛА/безпілотників призвело до того, що було розроблено багато методів виявлення, які використовуються як ранні попереджувальні знаки.

Насправді, деякі з цих методів були представлені та класифіковані в [38], включаючи також їх переваги, недоліки та рівні точності. Тим не менше, у цьому пункті представлені найбільш відомі методи виявлення безпілотників таким чином:

1. Виявлення звуку. Це метод акустичного виявлення, який фіксує навколишній звук за допомогою багатонаправленої мікрофонної решітки, яка виявляє будь-який звук в діапазоні від 25 до 30 футів. Потім звукові хвилі фільтруються для аналізу частоти цілі. Це можливо, оскільки дрони шумлять; їх поворотний пристрій включає щонайменше 8 бритв, які звучать голосніше, коли вони наближаються. Однак цей метод забезпечує високий рівень точності в тихих районах і не підходить у галасливих умовах.

2. Виявлення відео. Був класифікований як обмежений метод виявлення; механізм виявлення включає можливість знімати зображення літаючих безпілотників навіть на великих відстанях (100м) з прийнятною роздільною здатністю. Однак основною проблемою є його нездатність розрізнити птахів та трутнів, що призводить до високого рівня невдачі виявлення, незважаючи на використання комп’ютерних алгоритмів, таких як схеми польоту.

3. Виявлення руху. У поєднанні з алгоритмом Speed Up Robust Features (SURF) він може успішно виявляти безпілотники, маючи поблизу інші літаючі об'єкти (на відстані 15-45 м), а також малює шлях дрона.

4. Теплова детекція. Є більш точним при виявленні безпілотних літальних апаратів на відстані до 100м. Автор Столкін заявив, що турбовентилятор або турбореактивні двигуни легше виявити через утворення гарячих газів з їх вихлопних газів. Однак, схоже, цей метод не підходить і не надійний для пластикових квадрокоптерів з електродвигунами. Отже, Ganti припустив, що краще поєднувати цей метод з іншими методами. У будь-якому випадку, вартість його реалізації висока, при низькій швидкості виявлення на обмеженій відстані.

5. Радіолокаційне виявлення. Дуже корисний при виявленні великих літальних апаратів на великі відстані (45-500 м), але не малих. Це пов’язано з тим, що дрони меншого розміру видають менше шуму і мають меншу передачу сигналу.

6. Виявлення ВЧ. Радіочастотне виявлення дуже ефективне для безпілотних літальних апаратів на великі відстані, оскільки радіочастотні сигнали можуть бути виявлені з більшої відстані (від 50 м до 450 м). Дуже важко виявити безпілотник, який уникне радіочастотного виявлення, особливо коли дрони передають зображення на Наземну станцію управління (GCS) за допомогою радіочастотного сигналу. Однак для забезпечення успішної швидкості виявлення спочатку потрібно оцінити та підтримувати потужність передавача та чутливість приймача.

Висновки до другого розділу

Розглянуто основні проблеми конфіденційності, безпеки та безпеки, які можуть бути порушені порушенням безпеки.

Зазначено, що ключові проблеми слід вирішити якомога швидше, інакше їх незаконне використання буде постійно зростати, особливо за відсутності чітких законів, правових обмежень та санкцій. Представлено основні вразливі пункти безпеки та загрози, які можна використати, щоб поставити під загрозу безпеку безпілотників.

Проаналізовано існуючі рішення безпеки для захисту безпілотних систем, включаючи криптографічні та некриптографічні рішення. Криптографічні рішення по суті спрямовані на захист зв'язку безпілотників та переданих даних, тоді як некриптографічні рішення (IDS) спрямовані на виявлення та відновлення від можливих атак безпеки.

Досліджено можливі заходи безпеки безпілотника/БПЛА та протидію/БПЛА, на додаток до методів запобігання, та рішення, пов’язані з безпекою зв’язку та мереж безпілотників/БПЛА, які є важливими для збройних сил та рятувальні роботи.

3 АНАЛІЗ МЕТОДІВ ЗАХИСТУ ЗВ'ЯЗКУ БЛА ПРОТИ АТАК З ВИКОРИСТАННЯМ РАДІОЗАСОБІВ

Як частина вищезазначеної сфери електронної війни, сучасні радіостанції активно впроваджують два механізми, визначені в галузі електронного захисту, тобто затвердіння та контроль викидів електронної війни. Ці механізми призначені для захисту радіостанцій від наслідків такого використання частотного спектру, який погіршує, нейтралізує або повністю блокує їх працездатність. Заходи електронного захисту мінімізують здатність противника виявляти, відстежувати і перехоплювати (підтримка електронної війни) та здатність ефективно виконувати електронну атаку.

Механізм управління спектром реалізований поза радіостанціями і спрямований на координацію та усунення конфліктів використання частотного спектру як власними силами, так і опонентами [39

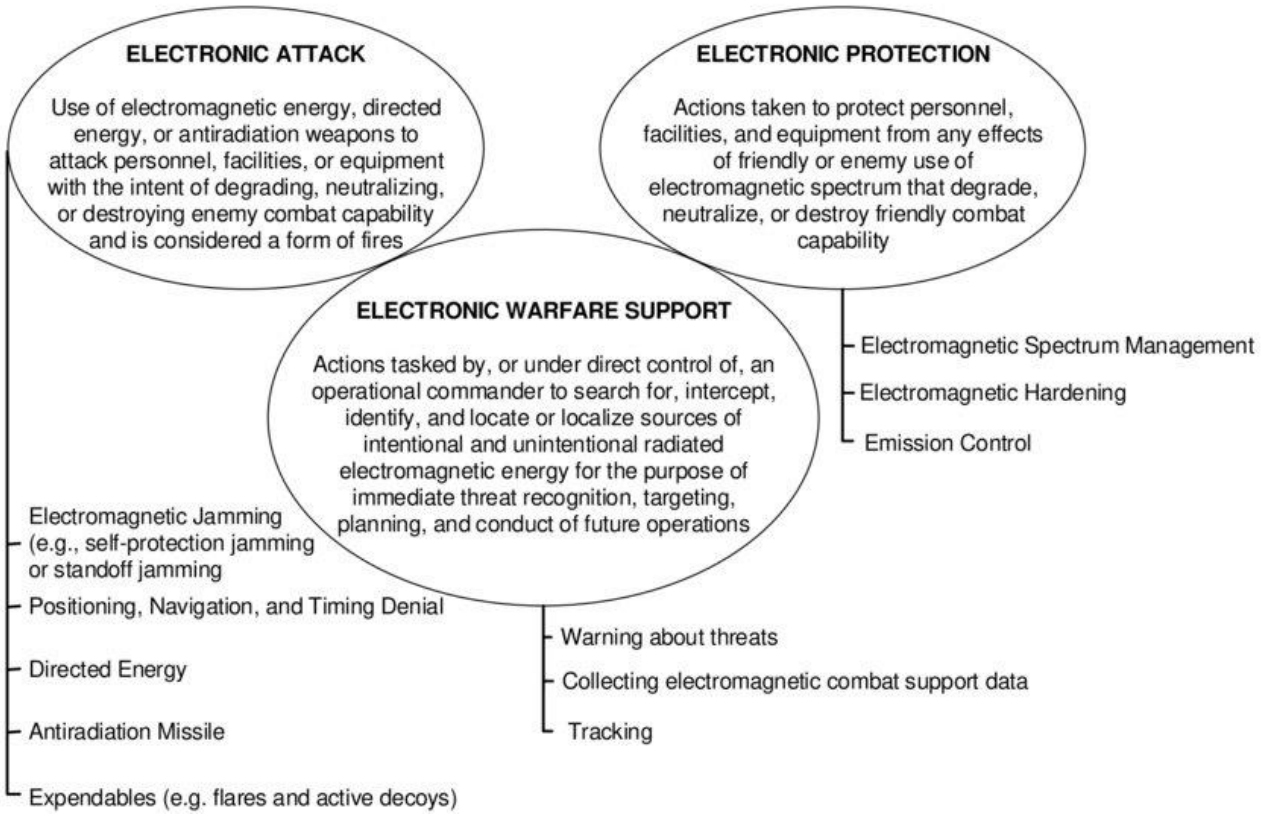


Рис.3.1.Сфера діяльності електронної війни (РЕБ) [1].

2.4 Класифікація механізмів, що імунізують радіостанції на навмисні перешкоди

Класифікація механізмів, що імунізують радіостанції для навмисних перешкод (Загартовування РЕ, Техніка протидії перешкодам, Електронні контрзаходи, Електронні запобіжні заходи), представлена на рис.3.2.

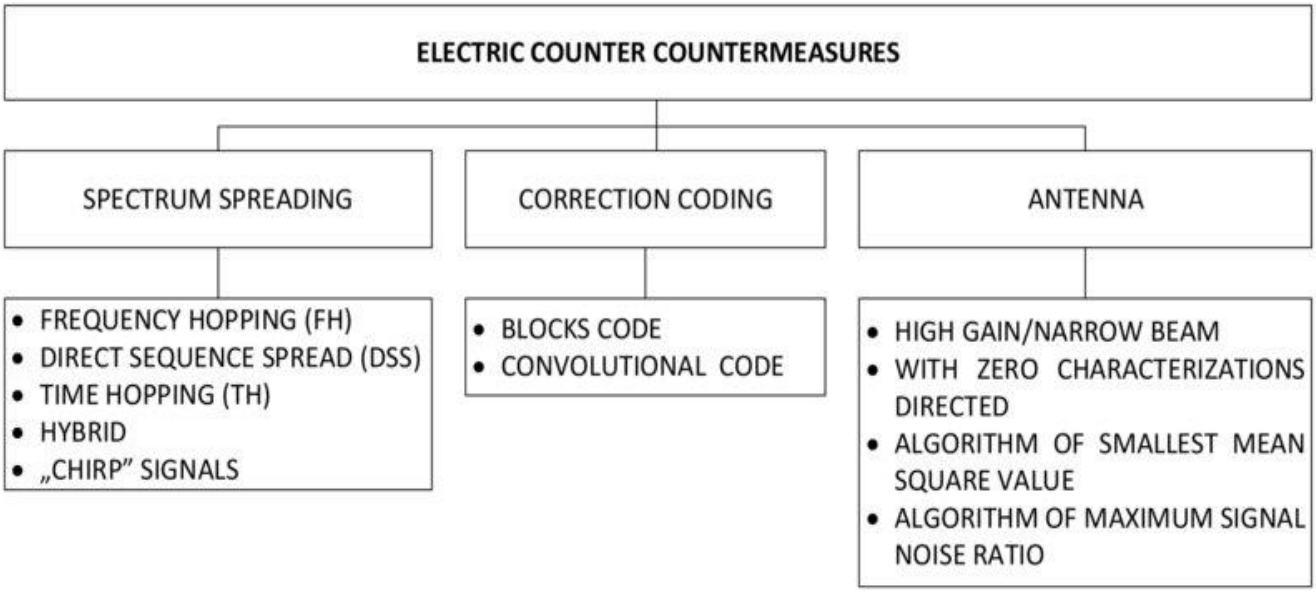


Рис.3.2.Класифікація механізмів, що імунізують радіостанції на навмисні перешкоди

У діапазоні частот VHF/UHF практично застосовуються механізми кодування SST (Техніка розширеного спектра, Прямий розподіл послідовності) та ECC, FEC (Кодування контролю помилок, Кодування помилок вперед).

Механізми проти завад, пов'язані з антенами, в цьому місці не мають практичного застосування. Метою зазначених вище механізмів є примусити систему порушити розпорошення своїх ресурсів у галузі частоти, часу та простору, тим самим знизивши її ефективність.

Система DSSS (Direct Sequence Spread Spectrum) має відносну простоту через відсутність вимоги до синтезатора швидких частот. Переданий сигнал множиться на псевдовипадкову послідовність з високою бітовою швидкістю, що призводить до розширення спектру сигналу та зменшення його спектральної щільності.

Переданий сигнал набуває шумоподібної форми, що ускладнює виявлення LPD (низька ймовірність виявлення) і важче перехоплює LPI (низька ймовірність перехоплення) щодо сигналу без розсіювання [40]

У системі з частотним стрибком FH (Frequency Hopping) частота несучої сигналу змінюється псевдовипадковим чином у широкому діапазоні. Хоча потенційний опонент може виявити сигнал, його не можна захопити (низька ймовірність перехоплення).

Системи, в яких на задану несучу частоту припадає більше одного символу, називаються системами з частотою повільного стрибка LFH (низькочастотний стрибок). В іншому випадку ми маємо справу з системою із швидким стрибком частоти FFH (Fast Frequency Hopping).

Системи CSS (Chirp Spread Spectrum) - це системи, які використовують імпульси з монотонно змінюваною частотою від мінімальної частоти f1 до максимальної частоти f2 або навпаки.

Різниця в цих частотах є хорошою оцінкою діапазону сигналів. Високий опір сигналу отримується, коли добуток смуги сигналів чирпіння та тривалість його імпульсу набагато більше одиниці (це супроводжується постійною спектральною щільністю потужності сигналу).

Системи CSS особливо корисні, коли пропускна здатність сигналу набагато вища, ніж двійкова швидкість передачі даних (надширокосмугові системи). Системи Chirp Spread Spectrum належать до класу LPI.

Методи кодування ECC (FEC) дозволяють передавати відформатовану інформацію, щоб протистояти шуму та перешкодам. Цей процес пов'язаний з введенням контрольованої надмірності в переданий потік даних з метою виявлення та виправлення помилок в приймачі.

Кодування характеризується так званою ефективністю кодування R, яка є відношенням кількості переданих символів даних до загальної кількості переданих символів коду.

3.2 Розробка концепції архітектури комунікаційної системи для БЛА, імунізованої для атак радіозначенням

Концепція архітектури системи радіозв'язку для БЛА, несприйнятливого до радіоатак, базується на пристроях, виготовлених компанією Transbit. Запропоноване радіотехнічне рішення працює у військовому діапазоні 4,4-5 ГГц та 235-380 МГц і призначене для розвідувальних безпілотних літальних апаратів.

Для встановлення зв'язку між наземною базовою станцією (NSB) та БПЛА була використана літакова радіолінія (SLR).

Дзеркальна камера складається з таких пристроїв:

- Радіомодуль літака - SMR;
- Базовий радіомодуль - BMR;
- Набір антен.

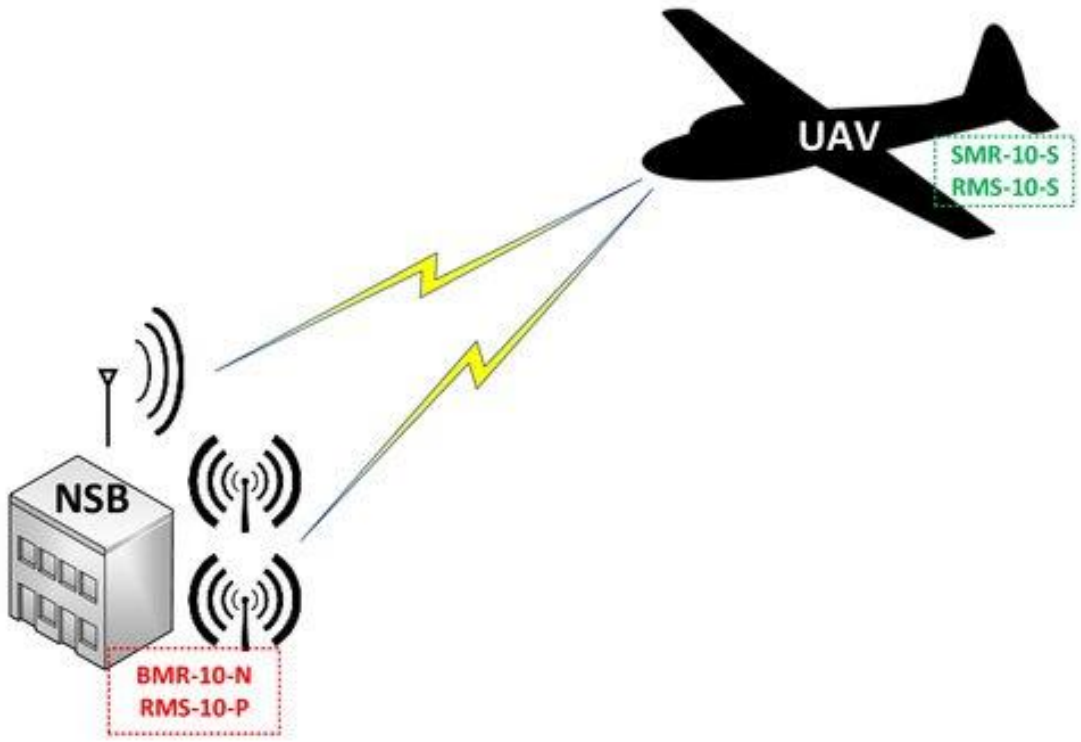


Рис.3.3. Концепція радіозв’язку БПЛА з NSB за допомогою літакової радіолінії

Набір вищезгаданих радіопристроїв (SMR та BMR) забезпечує двонаправлену передачу даних телеметрії та управління БПЛА, а також різних інших типів даних (наприклад, відеопотік) від БПЛА до наземної базової станції.

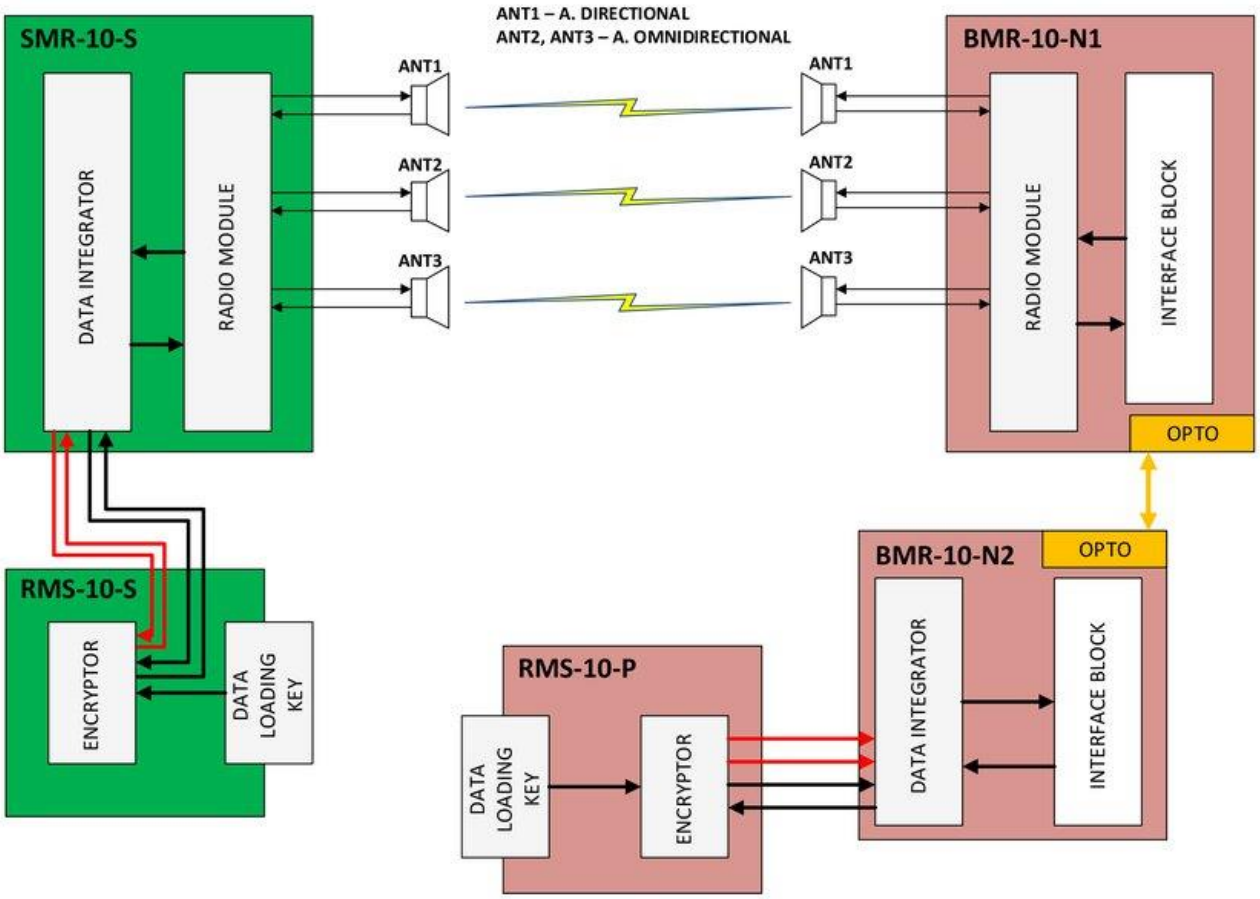


Рис.3.4. Блок-схема системи радіозв’язку

Радіомодуль літака (SMR-10-S) використовується для реалізації радіозв'язку між БПЛА та NSB. Це вдосконалений радіомодуль, розроблений в технології SDR, що дозволяє програмно реалізовувати різні схеми роботи, адаптовані до вимог співпраці з даним безпілотним літальним апаратом. Вибір програмного забезпечення операційної схеми SMR-10-S дозволяє підтримувати сумісність з багатьма типами систем БПЛА без необхідності заміни обладнання. SMR-10-S може використовуватися для передачі різних типів даних у каналі передачі з заданою програмою швидкістю передачі даних.

Це забезпечує двосторонній зв'язок із системними об'єктами. Радіомодуль літака працює з набором двох всеспрямованих антен та однієї спрямованої антени. Використання двох всеспрямованих антен призначене для усунення явища згасання (втрати сигналу внаслідок багатопроменевості) шляхом здійснення колективного прийому.

Метод вибору антен - комбіноване співвідношення - ефективно запобігає атрофії глибини, дозволяючи досягти зв'язку без збільшення потужності випромінювання передавача NSB. Використовуючи цей модуль, можна досягти ефективного радіозв'язку на відстані від 0 до 100 км, зберігаючи пряму видимість LoS (Line of Sight).

Базовий радіомодуль BMR-10-N є еквівалентом авіаційного радіомодуля з розгалуженою архітектурою завдяки встановленню пристрою. Він складається з двох модулів BMR-10-N1 та BMR-10-N2. Перший (BMR-10-N1) відповідає за виконання радіофункцій, ідентичних модулю SMR-10-S. Модуль BMR-10-N1 виготовлений з наборів трансиверів - підсилювача потужності, смугового фільтра, наборів підсилювачів LNA.

Блок BMR-10-N1 виконує операції вибору радіоканалу, процеси модуляції та демодуляції, кодування радіосигналів та функцій, що забезпечують низьку ймовірність виявлення - LPD, низьку ймовірність перехоплення - LPI та стійкість до перешкод (Anti-Jamming) - AJ. Всі ці функціональні можливості реалізуються програмно. BMR-10-N1 призначений для установки з направленою антеною.

Модуль BMR-10-N2 відповідає за побудову радіоканалів, придатних для властивостей даних, що надходять на інтерфейс Ethernet. Він також відповідає за обробку даних, що надходять на приймальні канали, опосередковує схеми управління роботою системи зв'язку, а також встановлюючи RMS-10-P шифрує та розшифровує дані, що передаються/приймаються модулем WMD-10-N1. Зв'язок між модулями BMR-10-N1 та BMR-10-N2 відбувається через оптичний інтерфейс.

Модулі RMS-10-S та RMS-10-P радіошифрування є окремими апаратними модулями. Вони оснащені роз'ємами, що дозволяють передавати дані за двома окремими двосторонніми каналами (шифрування/розшифрування не залежить від кожного напрямку) та роз'ємом, що дозволяє з'єднувати несучу з ключовою інформацією, що відповідає стандарту USB на логічному рівні. Їх головне завдання - забезпечити конфіденційність переданої інформації та достовірність походження даних. Він має алгоритм AES, реалізований відповідно до FIPS 197 (з параметрами: блок - 128 біт, кількість раундів - 14, довжина ключа - 256 біт), працює в режимі

лічильника (CTR, сумісний з NIST: SP800-38A) та в Галуа Режим лічильника (GCM - NIST: SP800-38D).

Для роботи модуля потрібні ключові матеріали, надані на криптографічному носії інформації - NIK. Цей матеріал повинен мати спільні ключі (PPK/PSK) відповідно до структури DS-100-1, описаної в EKMS308f.

З метою досягнення високого рівня стійкості до навмисного втручання та запобігання отриманню конфіденційних даних противником у пропонованому рішенні вживаються такі заходи:

- Кодування каналів - для увімкнення виправлення помилок під час передачі даних у втручаному середовищі;
- Спектр частотного стрибка;
- Реалізація підключень NSB до БПЛА та БПЛА до NSB на інших піддіапазонах для маскування каналів передачі;
- Використання діапазону радіозв'язку 4,4-5 ГГц лише через більшу ослабленість поширення радіохвиль порівняно із смугами, що працюють на нижчих частотах, та відсутністю грунтової хвилі;
- Застосування техніки DSSS для вузькосмугових каналів;
- Шифрування переданих даних;
- Реалізація радіолінії за допомогою спрямованої антени;
- Адаптивне управління потужністю;
- Можливість використовувати резервний канал.

3.3 Розробка рекомендацій щодо підвищення безпеки безпілотників/БПЛА

Після обговорення основних загроз безпеці та конфіденційності, атак та відповідних рішень, пропонуються наступні рекомендації щодо підвищення безпеки безпілотників/БПЛА:

1. Ліцензування безпілотних літальних апаратів. Користувачі безпілотних літальних апаратів повинні їх законно зареєструвати та отримати дозвіл на керування ними.

2. Жорсткіші обмеження. Необхідно брати до уваги, особливо проти незаконного використання безпілотників та БПЛА, та безвідповідального використання безпілотників поблизу життєво важливих районів, таких як аеропорти та військові об'єкти.

3. Посилений нагляд. За імпортом безпілотників, особливо підроблених, та відстеженням історії їх закупівлі, особливо коли безпілотники мають можливість піднімати та перевозити вагу на великій висоті з покращеним зворотним зв’язком із відео.

4. Подальша освіта. Необхідна, особливо для того, щоб користувачі безпілотних літальних апаратів могли розуміти їх загрози, а також навчати, як ними користуватися.

5. Більш жорсткі закони. Мають бути прийняті для запобігання несанкціонованому/неліцензійному використанню безпілотників/БПЛА, а нелегальні оператори повинні нести відповідальність згідно із законом.

6. Зони обмеженого та обмеженого користування. Безпілотні літальні апарати та БПЛА повинні уникати польоту над зонами обмеженого користування і повинні здійснювати польоти лише над певними обмеженими та відведеними зонами, щоб запобігти будь-якій близькій зустрічі, яка може призвести до пошкодження майна, поранення або загибелі людей.

7. Національні/міжнародні зусилля з боротьби з тероризмом. Їх слід застосовувати та підтримувати, щоб обмежити використання безпілотників/БПЛА в терористичних операціях, а також відслідковувати та зупиняти ринки незаконних безпілотників/БПЛА та торгівлю ними.

8. Спеціалізовані нелетальні заходи безпеки. Їх також слід розглядати як ідеальне рішення для протидії загрозам БПЛА, що не дозволяють літати цивільним районам, щоб запобігти пошкодженню та травмуванню.

9. Покращені методи виявлення безпілотників/БПЛА. Пропонують кращий тривожний підхід до будь-якого вхідного безпілотника/БПЛА та забезпечують достатньо часу для нейтралізації загрози на відстані.

10. Визначте новий полегшений хост/мережу IDS/IPS. Без ефективної системи IDS безпілотні літальні апарати можуть бути серйозно скомпрометовані та використані для здійснення кібер- чи фізичних атак на людей та майно. Тому розробляти полегшений IDS, що використовує гібридні методи виявлення (тобто методи виявлення на основі підписів, на основі специфікацій та на основі аномалій), рекомендується для швидкого прийняття рішень у середовищі, обмеженому ресурсами безпілотника, або додатках у режимі реального часу.

11. Легка багатофакторна схема автентифікації. Використання лише одного фактора (криптографічного) недостатньо, оскільки будь-яка слабкість у схемах ідентифікації/автентифікації може скомпрометувати безпілотник для використання у зловмисних цілях, що потенційно може призвести до різких наслідків. Для вирішення цих проблем слід поєднувати легкі криптографічні та некриптографічні рішення, щоб зменшити ймовірність незаконного доступу.

12. Легкі динамічні криптографічні алгоритми. Розробка легких динамічних криптографічних алгоритмів може забезпечити безпілотний зв’язок, забезпечуючи вищий рівень конфіденційності при низькій затримці та витратах ресурсів. Це випадок підходу, який використовує функцію одного раунду, спираючись на загальні параметри каналу як коефіцієнт «ти знаєш», а секретний ключ як фактор «ти маєш» для створення динамічного ключа оскільки параметри бездротового каналу змінюються випадковим чином. Тому динамічний криптографічний підхід забезпечує правильний баланс між рівнем безпеки та продуктивності.

13. Основною складовою в організації зв’язку системи керування БПЛА є радіоканал передачі даних в якому відбуваються процеси прийому та передачі їх. Однією з загроз, пов’язаних з перехопленням управління БПЛА є вплив на систему прийому та передачі інформації, яка здійснюється між оператором і БПЛА. Це призводить до повного контролю над БПЛА з боку протидіючої сторони. Отже, для

запобігання цьому, необхідно здійснювати керування радіосигналом з метою недопущення його перехоплення. Одним з таких можливих керувань є керування фазоюсигналу.

Задача керування фазою сигналу полягає в наступному: необхідно визначити фазу φ сигналу, який передається по закону синуса в момент часу $t = k$, безпілотному літальному апарату, який в момент часу $t = k$ своєчасно отримує правильну команду, при умові, що в лінії передачі присутні перешкоди, які носять випадковий характер. Інакше кажучи, при здійснені частотної, або амплітудно-частотної модуляції сигналу проводиться маніпуляція його фазою.

Розглянемо сигнал керування, який передається безпілотному літальному апарату, в якому зосереджена антена, яка має M решіток

$$X(k) = A\sin(\pi k\omega_0 + \varphi) + W(k),\ k = 0,1,2,...,M, \qquad (3.1)$$

де $W(k)$ – перешкода, яку розглядаємо як гаусовий білий шум з нульовим математичним сподіванням і невідомим середнім квадратичним відхиленням σ. При цьому параметри A і ω_0 відомі. Маючи оцінку параметра φ можна задавати різні значення його при передачі команд. При кожній передачі команди відбувається зміна фази за певним законом, що дає можливість захистити відповідну інформацію від перехоплення. Для здійснення оцінки фази сигнали застосуємо метод максимальної правдоподібності, який полягає в максимізації функції правдоподібності

$$H(X,\varphi) = \frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{1}{2\sigma^2}\sum_{k=0}^{M}\left(X(k) - A\sin\left(\pi\omega_0 k + \varphi\right)\right)\right). \qquad (3.2)$$

Функція (2) приймає максимальне значення, при мінімумі показника експоненти. Це означає, що максимізувати $H(X,\varphi)$ еквівалентно мінімізувати функцію

$$\Phi(\varphi) = \sum_{k=0}^{M}\left(X(k) - A\sin\left(\pi k\omega_0 + \varphi\right)\right)^2. \qquad (3.3)$$

Після диференціювання функції (3) по φ, маємо

$$\frac{d\Phi}{d\varphi} = 2\sum_{k=0}^{M}\left(X(k) - A\sin\left(\pi k\omega_0 + \varphi\right)\right)A\cos\left(\pi k\omega_0 + \varphi\right). \qquad (3.4)$$

Прирівнявши похідну (4) до нуля, отримаємо рівність

$$\sum_{k=0}^{M} X(k)\cos\left(\pi k\omega_0+\varphi\right)=A\sum_{k=0}^{M}\sin\left(\pi k\omega_0+\varphi\right)\cos\left(\pi k\omega_0+\varphi\right). \qquad (3.5)$$

Праву частину рівності (5) можна записати у вигляді

$$\frac{A}{2}\sum_{k=0}^{M}\sin\left(2\pi k\omega_0+2\varphi\right)=\frac{A}{2}\cdot\frac{\sin\left(\pi\left(M+1\right)\omega_0\right)\cos\left(\pi M\omega_0+\varphi\right)}{\sin\left(\pi\omega_0\right)}. \qquad (3.6)$$

Права частина (6) дає можливість визначити, при яких значеннях фази φ вона дорівнює 0. Ця умова визначається з рівності

$\cos\left(\pi M\omega_0+\varphi\right)=0$, звідки

$$\varphi=\frac{\pi}{2}-\pi M\omega_0. \qquad (3.7)$$

Рівність (7) визначає середнє значення фази для побудови асимптотичної щільності розподілу ймовірності оцінки фази. З іншого боку, прирівнявши ліву частину рівності (5) до нуля, маємо

$$\sum_{k=0}^{M} X(k)\cos\left(\pi k\omega_0\right)\cos\varphi-\sum_{k=0}^{M} X(k)\sin\left(\pi k\omega_0\right)\sin\varphi=0,$$

Звідки

$$\varphi=arctg\frac{\sum_{k=0}^{M} X(k)\cos\left(\pi k\omega_0\right)}{\sum_{k=0}^{M} X(k)\sin\left(\pi k\omega_0\right)}. \qquad (3.8)$$

Підставівши в (8) представлення (1), маємо

$$\varphi=arctg\frac{\sum_{k=0}^{M}\left(A\sin\left(\pi k\omega_0+\varphi\right)+W(k)\right)\cos\left(\pi k\omega_0\right)}{\sum_{k=0}^{M}\left(A\sin\left(\pi k\omega_0+\varphi\right)+W(k)\right)\sin\left(\pi k\omega_0\right)}. \qquad (3.9)$$

За допомогою рівності (9) визначимо яка повинна бути мінімальна кількість решіток антени прийому в БПЛА M, щоб досягти точне значення асимптотичної оцінки фази та її дисперсії. Так як асимптотична щільність розподілу оцінки фази має нормальний закон розподілу, то

$$D(\varphi)=\frac{2\sigma^2}{MA^2}. \qquad (3.10)$$

В таблиці 1 приведені результати імітаційного моделювання в результаті чого отримані середня оцінка $E(\varphi)$ та дисперсія $D\left(\varphi\right)=E\left(\varphi\right)-\left(E\left(\varphi\right)\right)^2$, де φ - визначається рівністю (9). Розрахунки здійснювались при $A=1$, $\omega_0=0,08$, $\sigma^2=0,02$.

В таблиці 1 приведені результати імітаційного моделювання в результаті чого отримані середня оцінка $E(\varphi)$ та дисперсія $D\left(\varphi\right)=E\left(\varphi\right)-\left(E\left(\varphi\right)\right)^2$, де φ - визначається рівністю (9). Розрахунки здійснювались при $A=1$, $\omega_0=0,08$, $\sigma^2=0,02$.

Таблиця 1. Результати розрахунку середнього значення оцінки фази і дисперсії

M	φ	$E(\varphi)$	$D\left(\varphi\right)=E\left(\varphi\right)-\left(E\left(\varphi\right)\right)^2$	$D(\varphi)=\frac{2\sigma^2}{MA^2}$
10	0	0,00001	0,0005	0,004
20	$-1,57$	-1,456	0,0016	0,002
30	$-3,14$	-2,897	0,0006	0,0013
40	$-4,71$	-3,987	0,00095	0,001
50	$-6,28$	-5,754	0,00059	0,0008
60	$-7,85$	-8,012	0,000556	0,000667
70	$-9,42$	-8,568	0,000612	0,000571
80	$-10,99$	-11,123	0,00046	0,0005
90	$-12,56$	-13,002	0,000356	0,000444
100	$-14,13$	-13,78	0,0004	0,0004

Як видно з таблиці 1 асимптотичне середнє значення фази і дисперсія оцінки φ досягає точних значень при $M=100$. Якщо $M<100$, то оцінка φ значно зсувна.

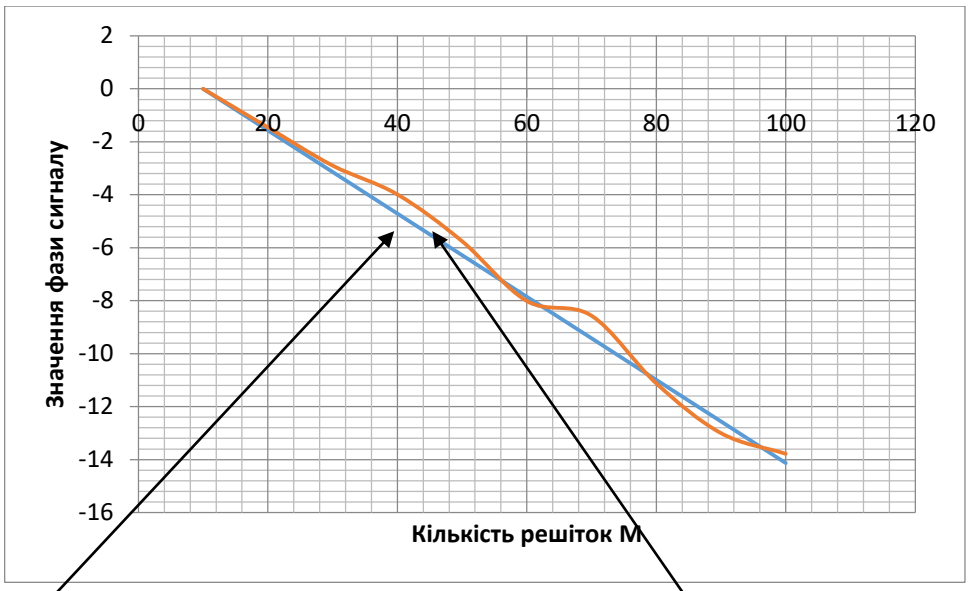


Рис.1. Порівняльні залежності заданої частоти і розрахункової методом максимальної правдоподібності.

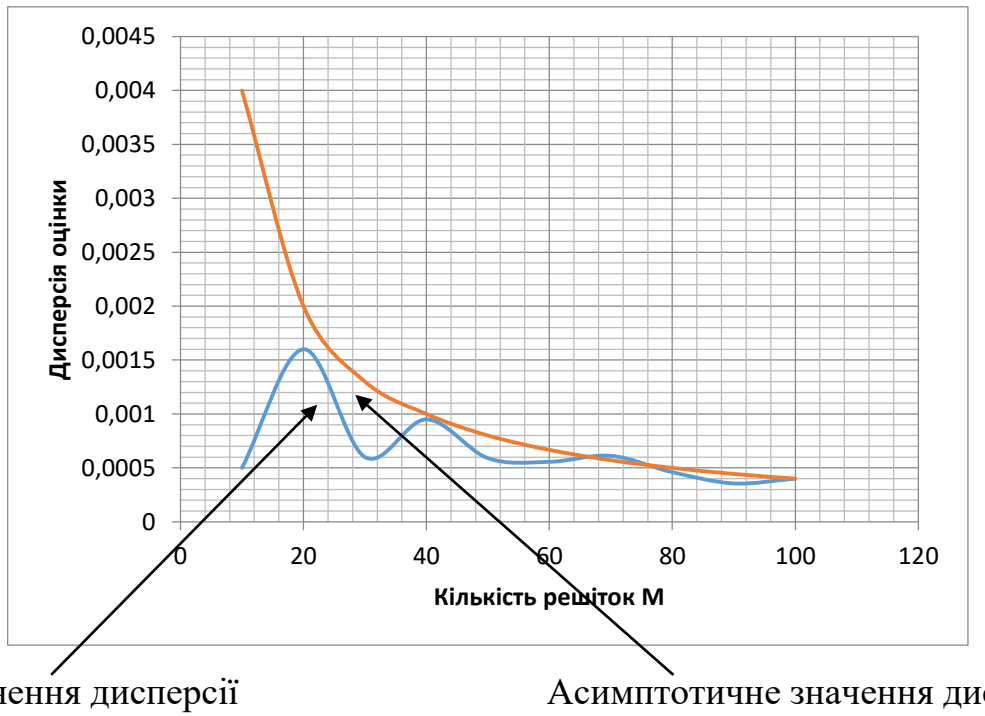


Рис.2. Порівняльні залежності заданої оцінки і розрахункової методом максимальної правдоподібності.

Рисунки 1 і 2 показують, що запропонований метод максимальної правдоподібності оцінки фази сигналу, який моделюється гармонічним коливанням при наявному шумі, функція розподілу ймовірності якого підпорядкована нормальному закону, дає точну оцінку при достатньо великій кількості решіток приймальної антени, яка вмонтовується в БПЛА для керування їм.

Висновки до третього розділу

Представлено аналіз некінетичних методів боротьби з БПЛА для цивільного та військового використання.

Описано фізичні рішення, які базуються на кінетичних та некінетичних методах боротьби з безпілотними літальними апаратами. Всі описані методи використовуються в даний час, часто приносячи позитивні ефекти в дії.

Проведено аналіз розчинів, які імунізують радіопередачу БПЛА оператором або наземною базовою станцією.

Враховуючи результати аналізів, проведених та використовуючи радіопристрої, що випускаються компанією Transbit, було внесено пропозиції щодо концепції радіозв'язку для БПЛА військового призначення для проведення розвідувальних місій.

Обговорено найважливіші функціональні можливості окремих елементів запропонованої архітектури. Використання описаних методів в апаратній реалізації ефективно зменшує ризик перешкод або переривань радіозв'язку між БПЛА та NSB.

Розроблено рекомендації щодо підвищення безпеки безпілотників/БПЛА з урахуванням обговорення основних загроз безпеці та конфіденційності, атак та відповідних технічних рішень.

А также для забезпечення захисту радіосигналу керування БПЛА необхідно проектувати антену прийому команд з достатньо великою кількістю решіток. Кількість таких решіток повинна бути не менше 100. Метод максимальної правдоподібності дає можливість здійснювати аналіз параметрів радіосигналу таких як амплітуда, частота і фаза при великій кількості решіток антени системи «оператор-БПЛА». Крім того, кількість даних решіток впливає на степінь скритності БПЛА при виконання керованих дій.

4 ВДОСКОНАЛЕННЯ МЕТОДИКИ ЗАХИСТУ РАДІОКАНАЛІВ УПРАВЛІННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Завдання виявлення розпізнавання виду і класу радіосигналів, що необхідні для ідентифікації типу об’єктів вирішувались вже багато років. При цьому головна увага була зосереджена на одиночних умовах при заздалегідь відомих параметрах сигналу та його внутрішній структурі [41].

У більшості відомих алгоритмів послідовної чи одночасної перевірки множинних умов не враховується структурна складова сигналу. Крім того, загальним недоліком, що притаманний більшості відомих алгоритмів, є розрізненість результатів, що ускладнює практичну (програмну) реалізацію та зменшує їх ефективність.

Виявленням сигналів систем керування БПЛА називаються встановленням факту належності прийнятого радіовипромінювання до класу сигналів систем керування БПЛА.

Номенклатура наявних на світовому ринку систем дистанційного радіокерування моделями технічних засобів (автомобілів, суден, літаків тощо) надзвичайно велика, а детальна інформація про використовувані види сигналів, режими та протоколи є комерційною таємницею підприємств-виробників та відсутня для вільного доступу [42]. За результатами проведеного аналізу встановлено, що системи керування БПЛА умовно поділяються на дві групи:

- системи, що працюють на фіксованих частотах у діапазонах метрових хвиль, використовують сигнали з частотною або амплітудною маніпуляцією та порівняно нескладні протоколи пакетної передачі команд управління;
- системи, що використовують режими адаптивного перестроювання робочої частоти у діапазоні 2400...2483,5 МГц, сигнали з гауссівською частотною, фазовою або квадратурною амплітудною маніпуляціями, а також різноманітні алгоритми розширення спектра.

За результатами аналізу ринку систем дистанційного радіокерування встановлено, що кількісне співвідношення між наявними зразками, що відносяться до визначених вище груп, приблизно рівне. Натомість, ринкова вартість систем другої групи приблизно на порядок вища, ніж першої. Незважаючи на те, що модельний ряд зразків обох груп має приблизно рівне кількісне співвідношення, популярність їх зразків співвідноситься приблизно як 80% на 20%. Саме тому для подальших досліджень обрано саме першу групу систем керування БПЛА.

4.1 Аналіз особливостей формування сигналів у системах дистанційного управління безпілотниками

До найбільш широкорозповсюдженим протоколам передачі команд управління від оператора до безпілотника відносяться імпульсно-позиційна та імпульсно-кодова модуляції. При цьому важливо відмітити, що сигнал формується при передачі Формування сигналу на передавальній стороні з використанням модуляції ІПМ, та передбачає наступні кроки:

- додавання синхронізаційного інтервалу;
- створення послідовності поодиноких імпульсів (з врахуванням кількості каналів). Позиція кожного повинна чітко відповідати значенню керуючої величини;
- маніпуляція несучої (піднесучої) частоти передавача отриманим пакетом імпульсів.

Тривалість поодинокого імпульсу дорівнює $\tau_s = 0.3 - 0.5$ мс, а синхронізаційного $\tau_c -$ до 22мс. При цьому зміна показників частоти F_M становить від 3 до 10 кГц. Враховуючи те, що середня тривалість пакета імпульсів рівна приблизно 0,08–0,2, відбувається асиметрична частотна маніпуляція, якій відповідає така ж асиметрична форма амплітудно-частотного спектра, як це показано на рис.4.1 для випадку модуляції піднесучої. При цьому замість центральної частоти спектра має місце так звана домінантна частота f_D, яка для сигналу, що розглядається на рис.4.1 становить 1100 Гц.

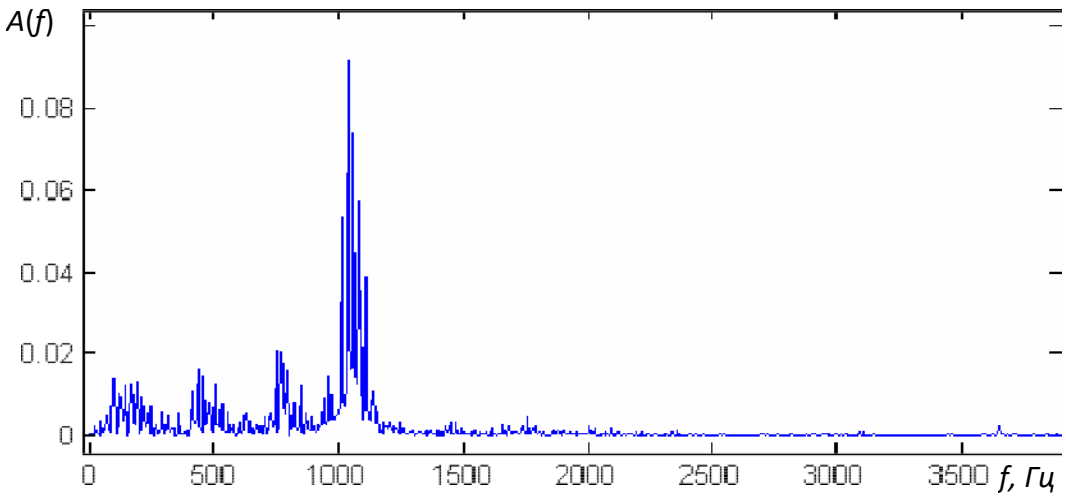


Рис.4.1. Типовий амплітудно-частотний спектр сигналу з імпульсно-позиційною модуляцією

Сигнали з імпульсно-кодовою модуляцією (ІКМ) формуються шляхом двопозиційної частотної маніпуляції бітових послідовностей, до яких входять восьмирозрядні кодові слова (байти) у такій типовій послідовності: преамбула (6 – 12 байтів), інформаційні канали (4 – 8 каналів по 2 байти), контрольна сума (2 або 4 байти). На відміну від ІПМ, відбувається звичайна симетрична частотна маніпуляція. Типовий амплітудно-частотний спектр такого сигналу наведено на рис.4.2.

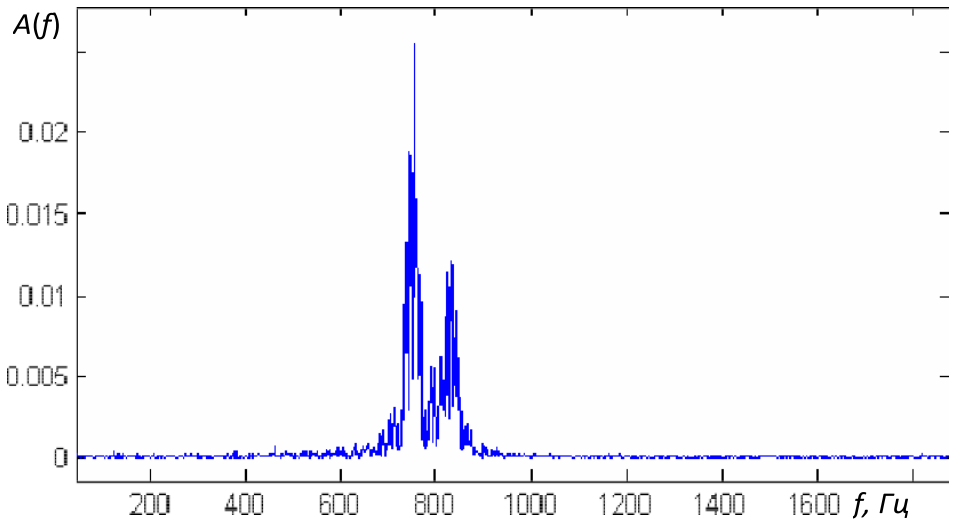


Рис.4.2. Типовий амплітудно-частотний спектр сигналу з імпульсно-кодовою модуляцією

Умовами виявлення сигналів систем керування БПЛА є [43]:

- енергетична (електромагнітна) доступність джерела радіовипромінювання; знаходження амплітудно-частотного спектра сигналу в межах смуги пропускання
- радіоприймального пристрою (РПрП) протягом часу, що виділений для аналізу; знаходження у вимкненому стані систем автоматичного підстроювання частоти та
- автоматичного регулювання підсилення РПрП;
- робота РПрП у режимі перенесення сигналу на низькочастотну піднесучу (USB або LSB), або перетворення на квадратурні складові.

4.2 Виокремлення системи ознак та критеріїв для розпізнавання сигналів

Відповідно до класичної теорії виявлення сигналів з частково відомими параметрами модуляції першою ознакою S_1 для нашого випадку є енергетична, згідно з якою енергія сигналу:

$$E(t) = \frac{1}{t}\int_0^t U^2(\tau)d\tau. \quad (4.1)$$

Протягом певного інтервалу часу t, обмеженої часом початку t_s та завершення t_f аналізу, повинна перевищує порогове значення E_0:

$$S_1 = \begin{Bmatrix} E(t) > E_0 \\ t \in (t_s, t_j) \end{Bmatrix}, \quad (4.2)$$

де $U^2(\tau)$ −дійсний сигнал, що аналізується. Порогове значення E_0 встановлюється за результатами аналізу фонової електромагнітної обстановки за умови роботи радіоелектронних засобів, що не становлять небезпеки.

У більш загальному випадку виявлення повинне здійснюватись у певному діапазоні частот, тому E_0 повинне бути функцією від частоти, дискретні значення якої взяті з кроком, що дорівнює типовій ширині спектра сигналу.

Наступною ознакою є модуляційна, яка вказує на належність сигналу, що підлягає аналізу, до класу сигналів із частотною маніпуляцією. Сама ознака S_2 описується сукупністю часткових ознак за виразом:

$$S_2 = \{S_{2.1} \cap S_{2.2} \cap S_{2.3}\}, \tag{4.3}$$

де часткова ознака розраховується:

$$S_{2.1} = \left\{\max_i(F_i) << 2\pi \frac{1}{N_s}\sum_{i=0}^{N_s-1}|F_i|\right\}. \tag{4.4}$$

де $F_i, i = 0, \dots N_s - 1 -$ дискретне перетворення Фур'є розмірністю N_s від вхідного сигналу, відповідає за його належність до класу сигналів із постійною амплітудою;

$$S_{2.2} = \left\{\frac{1}{N_s-1}\sum_{i=0}^{N_s-1}(\theta_i)^2 > \frac{\pi^2}{16}\right\}. \tag{4.5}$$

Вираз, в якому $\theta_i = arctg(Q_i/I_i)$– відліки абсолютної фази сигналу; I_i та $Q_i, i = 0, \dots N_s - 1 -$квадратурні складові сигналу, отримані за допомогою перетворення Гілберта, свідчать про належність сигналу до класу сигналів із кутовою модуляцією.

$$S_{3.2} = \left\{\sum_{i=1}^{N_s/2-l}(f_i - f_D)^2 \neq \sum_{i=N_s/2}^{N_s-1}(f_i - f_D)^2\right\}. \tag{4.6}$$

Вираз вказує на те, що модулююча функція (миттєва частота сигналу) $f_i = (\theta_i + \theta_{i-1}) * F_s$,де F_s −частота дискретизації, має імпульсний характер. Домінантна частота f_D у спектрі сигналу обчислюється ітераційно за виразом:

$$f_D = k\frac{1}{N_s}f_i + (1-k)f'_D, \tag{4.7}$$

де f_D – значення, обчислене за попередньою ітерацією; k – безрозмірний ваговий коефіцієнт, що обирається в діапазоні 0,05 – 0,1.

Завершальною ознакою є наявність у модулюючій функції сигналу $F(t)$, що підлягає аналізу, інформації про команди керування (структурна ознака). Тобто сама модулююча функція повинна мати структуру та вигляд, подібний до тієї, що формується на передавальній стороні. Аналітично ознаку S_3 записується у такому вигляді:

$$S_3 = \left\{\left[\frac{|\widehat{\tau_c}-\tau_c|}{\tau_c} < D_1\right] \cap \left[\frac{|\widehat{F_M}-F_M|}{F_M} < D_2\right] \cap \left[\frac{1}{T}\int_0^T F(t)dt < D_3\right]\right\}. \tag{4.8}$$

Де $\widehat{\tau_c}$ та $\widehat{F_M}$ −виміряні значення тривалості синхроімпульсу і девіації частоти відповідно, безрозмірні порогові значення D_1, D_2та D_3 встановлюються експериментальним шляхом залежно від необхідних значень імовірностей правильного виявлення та хибної тривоги.

4.3 Удосконалення алгоритму виявлення сигналів систем управління БПЛА

Базується на послідовних перевірках ознак (4.2), (4.3), (4.8), яким передують необхідні розрахунки. Вхідними даними для роботи алгоритму є масив відліків $r(k), k = 0..K-1,$ отриманих після дискретизації у часі з частотою F_s, та квантування за рівнем сигнальної суміші $r(t)$ з виходу радіоприймального пристрою:

$$r(t,U) = s(t,U) + n(t), \tag{4.9}$$

$s(t,U)$ −корисна складова; $n(t)$– шум; $U = [a, f, \theta, T]$ – вектор параметрів сигналу; a – амплітуда сигналу; f – центральна частота спектра; θ – інваріантна в часі фаза несучої частоти; T – символьний період.

Значення частоти дискретизації F_s та кількості рівнів квантування повинні відповідати вимогам для подальшого правильного відтворення сигналу. Результатом роботи алгоритму має бути рішення S про наявність ($S = True$) чи відсутність ($S = False$) сигналу систем управління БПЛА у прийнятій сигнальній суміші. Схема розробленого алгоритму наведена на рис.4.3.

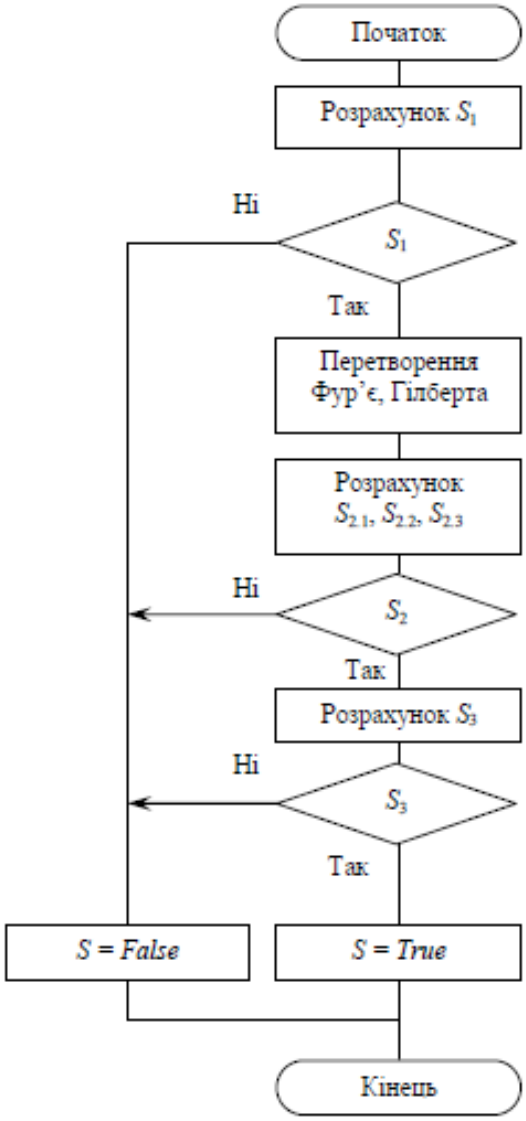


Рис.4.3. Схема алгоритму виявлення сигналів систем управління БПЛА

Першим етапом роботи алгоритму є перевірка енергетичної ознаки S_1. Перевірка інших ознак здійснюється лише при $S_1 = True$, тобто наявності будь-якого сигналу, енергія якого достатня для подальшого аналізу. Інакше приймається рішення про відсутність будь-якого сигналу (у тому числі сигналу систем управління БПЛА) й алгоритм завершує свою роботу. Додатково за цією ознакою може здійснюватись перестроювання радіоприймального пристрою для аналізу іншої ділянки частотного діапазону.

Другим етапом роботи алгоритму є перевірка модуляційної ознаки S_2, якій передують проміжні розрахунки: перетворення Фур'є та Гілберта, виділення модулюючої функції (вектора миттєвої частоти сигналу), фільтрація та автоматичне налаштування на домінуючу частоту сигналу. При $S_2 = True$ маємо випадок сигналу, що за видом модуляції відповідає сигналу систем управління БПЛА.

Третім етапом роботи алгоритму є перевірка структурної ознаки S_3. При її виконанні приймається остаточне рішення про наявність ($S = True$) чи відсутність ($S = False$) сигналу систем управління БПЛА у прийнятій сигнальній суміші.

Практична реалізація розробленого алгоритму виявлення сигналів систем управління БПЛА здійснена у програмному засобі, головне вікно якого наведено на рис.4.4.

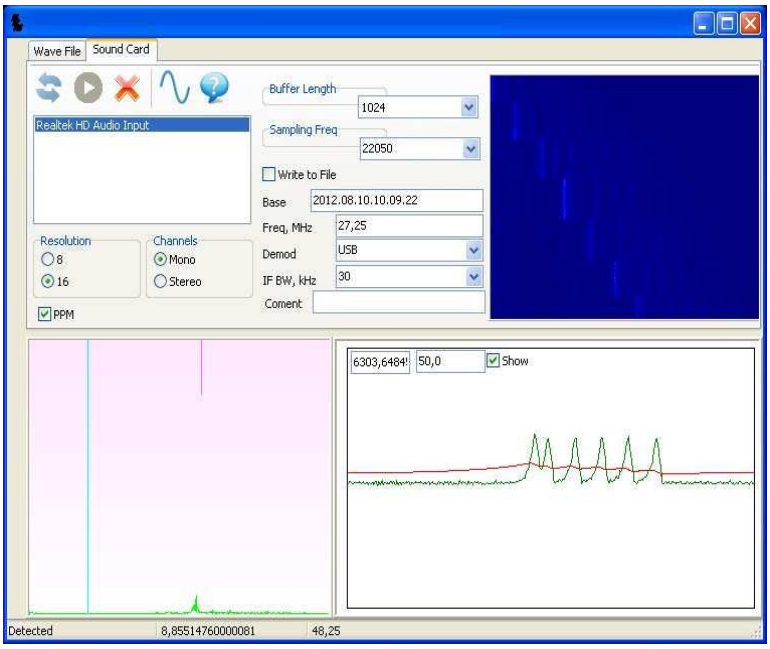


Рис.4.4. Програмна реалізація розробленого алгоритму

Програмний засіб орієнтований на використання у середовищі Windows 7 та вище. Він забезпечує обробку звукових файлів із записом сигналу у форматі WAW або безпосередньо потоку відліків з аудіоадаптера електронно-обчислювальної машини у реальному масштабі часу. Аналіз сигналу з автоматичним настроюванням на центральну (домінантну) частоту здійснюється у смузі пропускання аудіоадаптера, яка може становити до 96 кГц. Під час роботи відображаються основні етапи обробки: осцилограма, миттєвий спектр та сонограма сигналу, графік модулюючої функції. Для виявлення сигналу систем управління БПЛА потрібно в середньому 0,5 – 1,2 с. У разі такого виявлення передбачено звукову та візуальну індикацію [44].

4.4 Пропозиції щодо розробки прототипу БПЛА із захищенним каналом зв'язку

Головний мікрокомп'ютер. Для подальшої розробки та дослідження було запропоновано мікрокомп'ютер (Raspberry Pi 3 Model B). Як показують резульати світових дослідників, RPi 3 здатен виконати всі ті функції та вимоги, які до нього формуютья. Тобто RPi 3 може виступати достатньо потужною платформою для реалізації можливостей прототипу БПЛА із захищенним каналом зв'язку.

Основними критеріями при виборі мікрокомп'ютера були наявність великої кількості портів, достатня потужність для виконання шифрування потоку і інших, менш затратних процесів одночасно, а корисними особливостями вважалися вбудований WiFi модуль і наявність GPU. RPi 3 повністю відповідає критеріям вибору: кількості портів достатньо для підключення всіх необхідних апаратних компонент (DVB-T модем, video capture device, порт телеметрії та порт керування для пілотного контролера, RTC, GPIO індикатор та інші ситуативні), процесор справляється з навантаженням від всіх процесів у режимі повного функціонування, наявні вбудований WiFi модуль і VideoCore IV 3D.

2. Відео система. Для реалізації відеозйомки може бути запропонована камера FPV Sony super HAD color CCD з максимальною розподільною здатністю

752 x 582 (PAL). Вона здатна цілком задовольнити вимог до роздільної здатності того відео трафіку, який необхідно фіксувати та аналізувати. Відеотрафік генеруватиметься за рахунок фреймворка GStreamer, який складається із плагінів.

Досить велика кількість плагінів забезпечує варіативність можливих варіантів побудови трафіку та дозволяє підлаштовувати кінцевий результат використовуючи різні додаткові можливості кастомізації. Крім того, вихідний код плагінів є відкритим, тому можна модифікувати плагіни під конкретні рішення, якщо базова версія не має необхідного функціоналу.

Для прикладу, можна порівняти завантаженість процесору під час використання стандартного плагіну для кодування відео у формат H.264 (рис.4.5) і плагіну OMX (рис.4.6).

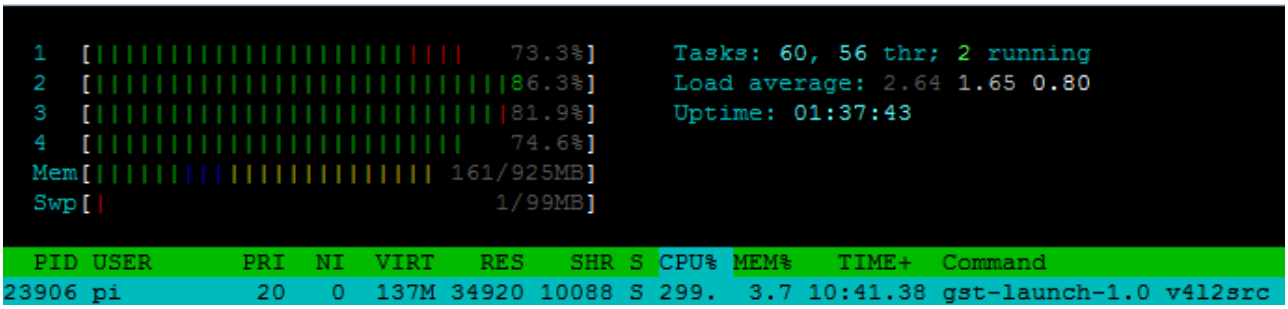


Рис.4.5. Завантаженість процесора при використанні плагіну x264

Після аналізу, можна зробити висновок, що для першого варіанту використання відео у форматі 576i є неможливим.

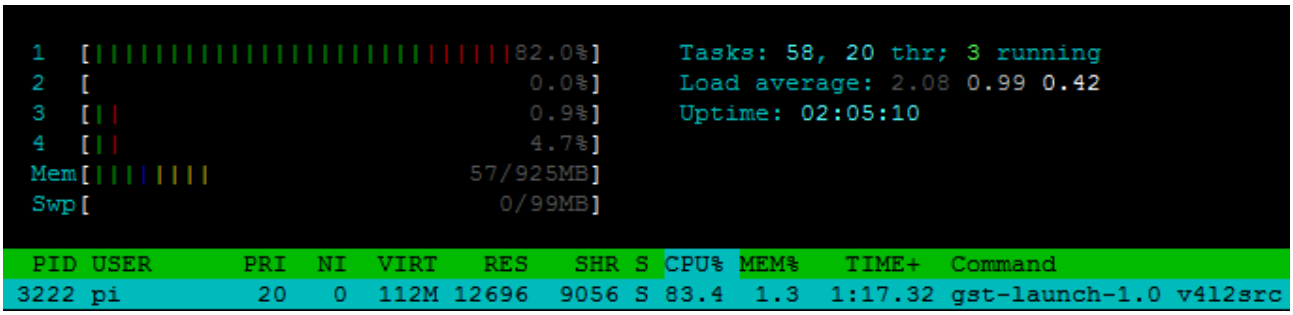


Рис.4.6. Завантаженість процесора при використанні плагіну OMX

В той же час, при другому варіанті звільнюється значна частина головного процесору за рахунок використання VideoCore IV 3D. Тому і середнє значення

завантаженості процесора при використані x264 близько 300%, а при використанні плагіну OMX – 80%.

3. Лінія зв’язку. Для передачі даних між наземним і повітряним модулями було обрано європейський стандарт наземного цифрового мовлення - DVB-T. DVB-T призначений для передачі єдиного транспортного потоку MPEG-TS з цифровими сервісами (мультиплексу), використовуючи модуляцію COFDM, зі швидкістю до 31 Мбіт/с. Було обрано компактний повно дуплексний DVB-T передавач, параметри якого задовольняють умовам використання лінії зв’язку (необхідно мати можливість рознести частоти приймачів на наземному і повітряному модулі БПЛА, а також мати значну кількість частот, на які можна налаштувати приймачі, для реалізації алгоритму протидії РЕБ).

Таблиця 4.1

Характеристики DVB-T модему

Параметр	**Значення**	
Полоса пропускання	Передавач	2/3/4/5/6/7/8 MHz
	Приймач	5/6/7/8 MHz
Frequency range	Передавач	50~950 MHz та 1200~1350 MHz з кроком 1KHz
	Приймач	50~950 MHz з кроком 1KHz
Вихідний рівень RF	0 dBm (108 dBuV)	
Цифрове підсилення	Діапазон: +6/-25 dB , з кроком 1 dB	

Програмна частина лінії зв’язку є основною і найбільш складною складовою проекту: вона включає в себе мультиплексування/ демультиплексування потоку, фільтрацію пакетів, інтерфейси для взаємодії із драйвером радіо передавача/приймача, збору статистики та інших компонент.

За допомогою бібліотеки MavLink виконується обмін повідомленнями і сигналами керування між польотним контролером та наземною станцією керування. Всі дані включаючи сигнали керування, телеметрії, відео потік та інші інформаційні об’єднуються у єдиний MPEG-TS потік, також до пакетів

прикріплюються додаткові дані для контролю над пакетами, що забезпечує більший захист інформації.

Локальні повідомлення в межах кожного з модулів передаються за допомогою бібліотеки LCM, що забезпечує дуже швидкий обмін даними і, як наслідок малі затримки.

4. Захист лінії зв’язку Оскільки алгоритм AES є стандартом шифрування у наш час, для реалізації шифрування даних у проекті використовується вже реалізований алгоритм AES-128 із однієї з багатьох бібліотек шифрування. Реалізація алгоритмів протидії РЕБ і захисту від підміни пакетів є однією з головних ідей проекту, тому є строго конфіденційними і не можуть бути описані в цій роботі.

Проте, значну частину досліджень становив аналіз і розробка алгоритму синхронізації часу у розподіленій системі, а саме між наземним та повітряним модулем зв’язку з БПЛА. Синхронний годинник на даний момент необхідно використовувати у двох основних напрямах: синхронне логування та синхронна зміна радіочастот у алгоритмі протидії РЕБ

Для логування необхідно встановити час що відповідає реальному з точністю до однієї секунди. Для ефективного функціонування алгоритму зміни частот необхідно значно більша точність - до 20 мсек або краще. Також, треба зазначити, що система зв'язку базується на використанні радіо модемів і має затримку на прийом даних до 50 мсек (затримка є нерівномірною і може відрізнятися від затримку у протилежну сторону).

На основі аналізу алгоритмів синхронізації, вимог до алгоритму та апаратних обмежень побудуємо власний алгоритм, що максимально задовольняє умовам його використання.

По-перше, будемо синхронізувати час на наземному модулі використовуючи протокол NTP. Наземний модуль, на відміну від повітряного, має можливість підключення до мережі у перед польотному режимі. Альтернативним джерелом синхронізації часу, у разі відсутності мережі, до наземного модуля підключено

RTC, але RTC має меншу точність синхронізації і повинен перевірятися і налаштовуватися час від часу.

Таким чином, маємо еталонне джерело часу на наземному модулі. Тепер необхідно синхронізувати повітряний модуль з наземним.

За основу алгоритму синхронізації було обрано алгоритм Крістіана оскільки він простий у реалізації і має високу ефективність в невеликих мережах і мережах з малим завантаженням. Недоліки алгоритму нівелюються наступним чином:

1. Вимагає зовнішнього джерела точного часу – як зазначено вище, наземний модуль буде використовуватись як джерело еталонного часу.

2. Не має вбудованої захисту від переведення годинників у зворотну сторону – будемо проводити синхронізацію годинників один раз перед початком польоту. У цей час ключові системи що залежать від синхронності часу не будуть запущені і переведення годинників у зворотну сторону не спровокує неоднозначності у роботі алгоритмів.

3. Не дозволяє коректно встановлювати час в разі, якщо запит і відповідь передаються по різних маршрутах (потрібен різний час для передачі даних повідомлень) – будемо встановлювати початковий час як половина часу повного кола передачі усередненого за декілька ітерацій. Для уточнення часу при різному часі при передачі у різні сторони будемо корегувати час шляхом відправки поточного еталонного часу на повітряний модуль і перевірки розрахованого часу затримки з затримкою при передачі еталонного часу.

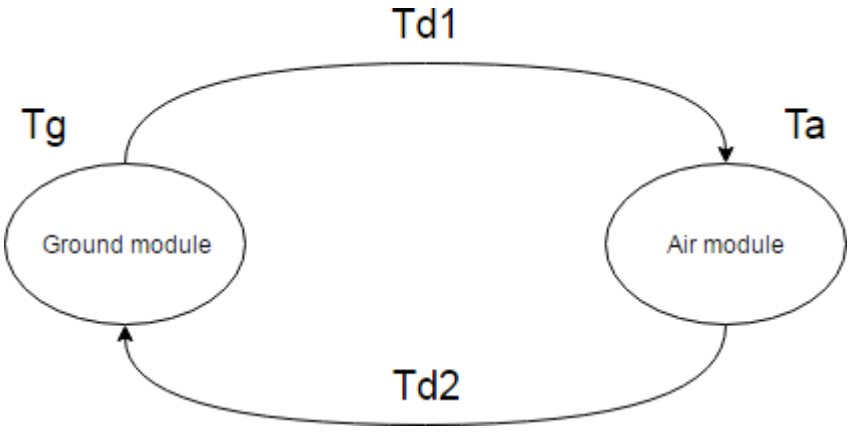


Рис.4.7. Зміщення часу

Затримка при передачі даних з наземного на повітряний модуль ($Td1$) та з повітряного на наземний ($Td2$) є невідомими і можуть відрізнятися (рис.4.7). Проте, можливо визначити затримку повного кола ($Td1 + Td2$) і спираючись на алгоритм Крістіана апроксимувати $Td1 = Td2 = (Td1 + Td2)/2$.

Для більшої точності виконується декілька (на даний момент 10) обчислень затримки повного кола. З 10 обчислених затримок обираємо найменшу, як найбільш точну. Після обчислення затримки змінюємо час на повітряному модулі $Ta = Tg + (Td1 + Td2)/2$.

Наступний крок – коректування обраної на першому кроці затримки. Коректування відбувається шляхом передачі таймстампів з наземного модуля на повітряний. На повітряному модулі, як і на першому кроці знаходимо найменшу затримку при передачі таймстампу. Ця затримка порівнюється із поточним часовим зміщенням (на першому кроці $(Td1 + Td2)/2$) на наземній станції, якщо затримка має похибку що потрапляє у заду дельту точності синхронізації, то годинники вважаються синхронізованими, в іншому випадку часове зміщення задається корегується на половину різниці поточних затримок на повітряному і наземному модулі.

Таким чином, маємо годинники синхронізовані з точністю до половини затримки повного кола, що теоретично становить приблизно 30 мсек, проте фактично, як показали практичні результати використання, завдяки відносній рівномірності розподілу значень затримок у дві сторони, маємо похибку приблизно у 5 мсек, що є цілком прийнятним результатом для подальшого використання даного алгоритму.

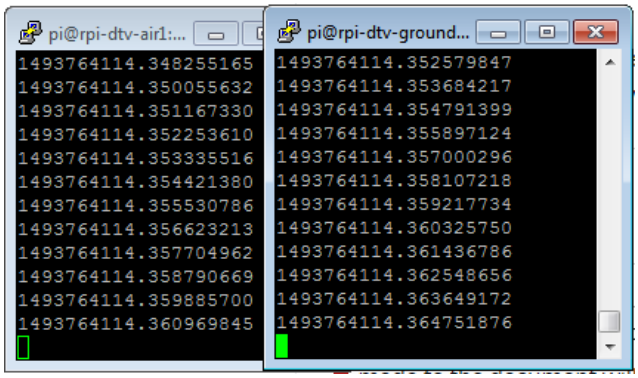


Рис.4.8. Порівняння часу після синхронізації

Висновки до четвертого розділу

Розроблено алгоритм, який забезпечує встановлення факту належності прийнятого радіовипромінювання до класу радіосигналів систем дистанційного керування БПЛА з імпульсно-позиційною та імпульсно-кодовою модуляціями.

Зазначено, що алгоритм базується на послідовних перевірках енергетичної, модуляційної та структурної ознак сигналу, передбачає можливість автоматичного виявлення сигналу супроводження його за частотою.

Запропоновано конкретні апаратні та програмні рішення для побудови прототипу БПЛА. Наведено результати практичного тестування можливих рішень задач на готовому прототипі і наведено результати функціонування розроблених компонентів зв'язку.

ВИСНОВКИ

В магістерській кваліфікаційній роботі було:

- описано архітектуру безпілотника, типи зв'язку та типи БПЛА. Також різниця між безпілотниками, БПЛА та БПЛА.
- зауважено те, що все ще необхідні більш жорсткі правила, щоб забезпечити більш безпечне використання БПЛА та БПЛА, особливо внаслідок нещодавніх зустрічей між безпілотниками/БПЛА та іншими літаками.
- зазначено неохідність виокремлення безпеки основних програм БПЛА та розглянуто основні проблеми конфіденційності, безпеки та безпеки, які можуть бути порушені порушенням безпеки.
- представлено основні вразливі пункти безпеки та загрози, які можна використати, щоб поставити під загрозу безпеку безпілотників.
- проаналізовано існуючі рішення безпеки для захисту безпілотних систем, включаючи криптографічні та некриптографічні рішення. Криптографічні рішення по суті спрямовані на захист зв'язку безпілотників та переданих даних, тоді як некриптографічні рішення (IDS) спрямовані на виявлення та відновлення від можливих атак безпеки.
- досліджено можливі заходи безпеки безпілотника/БПЛА та протидію/БПЛА, на додаток до методів запобігання, та рішення, пов’язані з безпекою зв’язку та мереж безпілотників/БПЛА, які є важливими для збройних сил та рятувальні роботи.
- описано фізичні рішення, які базуються на кінетичних та некінетичних методах боротьби з безпілотними літальними апаратами. Всі описані методи використовуються в даний час, часто приносячи позитивні ефекти в дії.
- проведено аналіз розчинів, які імунізують радіопередачу БПЛА оператором або наземною базовою станцією.
- обговорено найважливіші функціональні можливості окремих елементів запропонованої архітектури. Використання описаних методів в

апаратній реалізації ефективно зменшує ризик перешкод або переривань радіозв'язку між БПЛА та NSB.

- розроблено рекомендації щодо підвищення безпеки безпілотників/БПЛА з урахуванням обговорення основних загроз безпеці та конфіденційності, атак та відповідних технічних рішень.
- розроблено алгоритм, який забезпечує встановлення факту належності прийнятого радіовипромінювання до класу радіосигналів систем дистанційного керування БПЛА з імпульсно-позиційною та імпульсно-кодовою модуляціями.
- зазначено, що алгоритм базується на послідовних перевірках енергетичної, модуляційної та структурної ознак сигналу, передбачає можливість автоматичного виявлення сигналу супроводження його за частотою.
- запропоновано конкретні апаратні та програмні рішення для побудови прототипу БПЛА. Наведено результати практичного тестування можливих рішень задач на готовому прототипі і наведено результати функціонування розроблених компонентів зв'язку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Atherton K.D. The faa says there will be 7 million drones flying over america by 2020. Popular Sci. 2016 [Google Scholar]

2. Vattapparamban E., Güvenç İ., Yurekli A.İ., Akkaya K., Uluağaç S. Wireless Communications and Mobile computing Conference (IWCMC), 2016 International. IEEE; 2016. Drones for smart cities: issues in cybersecurity, privacy, and public safety; pp. 216–221. [Google Scholar]

3. Dalamagkidis K., Valavanis K.P., Piegl L.A. On integrating unmanned aircraft systems into the national airspace system. Springer; 2012. Aviation history and unmanned flight; pp. 11–42. [Google Scholar]

4. Altawy R., Youssef A.M. Security, privacy, and safety aspects of civilian drones: a survey. ACM Trans. Cyber-Phys. Syst. 2017;1(2):7. [Google Scholar]

5. Marshall D.M., Barnhart R.K., Hottman S.B., Shappee E., Most M.T. Crc Press; 2016. Introduction to unmanned aircraft systems. [Google Scholar]

6. Chen M., Challita U., Saad W., Yin C., Debbah M. Machine learning for wireless networks with artificial intelligence: a tutorial on neural networks. arXiv Preprint arXiv:1710.02913. 2017 [Google Scholar]

7. Dinger J., Hartenstein H. Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on. IEEE; 2006. Defending the sybil attack in p2p networks: taxonomy, challenges, and a proposal for self-registration; pp. 8–pp. [Google Scholar]

8. Fotouhi A., Qiang H., Ding M., Hassan M., Giordano L.G., Garcia-Rodriguez A., Yuan J. Survey on uav cellular communications: practical aspects, standardization advancements, regulation, and security challenges. arXiv Preprint arXiv:1809.01752. 2018 [Google Scholar]

9. Uragun B. Machine Learning and Applications and Workshops (ICMLA), 2011 10th International Conference on. Vol. 2. IEEE; 2011. Energy efficiency for unmanned aerial vehicles; pp. 316–320. [Google Scholar]

10. Irizarry J., Gheisari M., Walker B.N. Usability assessment of drone technology as safety inspection tools. J. Inf. Technol. Construct. (ITcon) 2012;17(12):194–212. [Google Scholar]

11. Abid M.E., Austin T., Fox D., Hussain S.S. Drones, uavs, and rpas: an analysis of a modern technology. Worcester Polytech. Inst., Worcester, Massachusetts. 2014 [Google Scholar]

12. Kopardekar P.H. 2014. Unmanned aerial system (uas) traffic management (utm): Enabling low-altitude airspace and uas operations. [Google Scholar]

13. Motlagh N.H., Taleb T., Arouk O. Low-altitude unmanned aerial vehicles-based internet of things services: comprehensive survey and future perspectives. IEEE Internet Things J. 2016;3(6):899–922. [Google Scholar]

14. Yang L., Qi J., Xiao J., Yong X. Intelligent Control and Automation (WCICA), 2014 11th World Congress on. IEEE; 2014. A literature review of uav 3d path planning; pp. 2376–2381. [Google Scholar]

15. Ueno S., Higuchi T. Numerical Analysis-Theory and Application. InTech; 2011. Collision avoidance law using information amount. [Google Scholar]

16. Brandt A.M., Colton M.B. Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on. IEEE; 2010. Haptic collision avoidance for a remotely operated quadrotor uav in indoor environments; pp. 2724–2731. [Google Scholar]

17. Hernandez-Hernandez L., Tsourdos A., Shin H.-S., Waldock A. Unmanned Aircraft Systems (ICUAS), 2014 International Conference on. IEEE; 2014. Multi-objective uav routing; pp. 534–542. [Google Scholar]

18. Lipsitch M., Swerdlow D.L., Finelli L. Defining the epidemiology of covid-19-studies needed. N. Engl. J. Med. 2020 [PubMed] [Google Scholar]

19. . Mansfield K., Eveleigh T., Holzer T.H., Sarkani S. Technologies for Homeland Security (HST), 2013 IEEE International Conference on. IEEE; 2013. Unmanned aerial vehicle smart device ground control station cyber security threat model; pp. 722–728. [Google Scholar]

20. Jones A., Kovacich G.L. Auerbach Publications; 2015. Global Information Warfare: The New Digital Battlefield. [Google Scholar]

21. Carr E.B. Unmanned aerial vehicles: examining the safety, security, privacy and regulatory issues of integration into us airspace. Natl. Centre Policy Anal. (NCPA). Retriev. September. 2013;23:2014. [Google Scholar]

22. Kerns A.J., Shepard D.P., Bhatti J.A., Humphreys T.E. Unmanned aircraft capture and control via gps spoofing. J. Field Rob. 2014;31(4):617–636. [Google Scholar]

23. Kovar D. 2016. Uavs, Iot, and Cybersecurity. [Google Scholar]

24. Mitchell R., Chen R. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. IEEE Trans. Syst. Man Cybernet. 2014;44(5):593–604. [Google Scholar]

25. Mitchell R., Chen R. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. IEEE Trans. Syst. Man Cybernet. 2013;44(5):593–604. [Google Scholar]

26. Kacem T., Wijesekera D., Costa P., Barreto A. Trustcom/BigDataSE/ISPA, 2016 IEEE. IEEE; 2016. An ads-b intrusion detection system; pp. 544–551. [Google Scholar]

27. Casals S.G., Owezarski P., Descargues G. Digital Avionics Systems Conference (DASC), 2013 IEEE/AIAA 32nd. IEEE; 2013. Generic and autonomous system for airborne networks cyber-threat detection; pp. 4A4–1. [Google Scholar]

28. Rani C., Modares H., Sriram R., Mikulski D., Lewis F.L. Security of unmanned aerial vehicle systems against cyber-physical attacks. J. Defense Model. Simul. 2016;13(3):331–342. [Google Scholar]

29. Lu H., Li Y., Mu S., Wang D., Kim H., Serikawa S. Motor anomaly detection for unmanned aerial vehicles using reinforcement learning. IEEE Internet Things J. 2017;5(4):2315–2322. [Google Scholar]

30. Condomines J.-P., Zhang R., Larrieu N. Network intrusion detection system for uav ad-hoc communication: from methodology design to real test validation. Ad Hoc Netw. 2019;90:101759. [Google Scholar]

31. Sedjelmaci H., Senouci S.M., Ansari N. A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks. IEEE Trans. Syst. Man Cybernet. 2017;48(9):1594–1606. [Google Scholar]

32. Lauf A.P., Peters R.A., Robinson W.H. A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. Ad Hoc Netw. 2010;8(3):253–266. [Google Scholar]

33. Mitchell R., Chen I.-R. Proceedings of the first ACM MobiHoc workshop on Airborne Networks and Communications. ACM; 2012. Specification based intrusion detection for unmanned aircraft systems; pp. 31–36. [Google Scholar]

34. Zhang G., Wu Q., Cui M., Zhang R. GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE; 2017. Securing uav communications via trajectory optimization; pp. 1–6. [Google Scholar]

35. Cui M., Zhang G., Wu Q., Ng D.W.K. Robust trajectory and transmit power design for secure uav communications. IEEE Trans. Veh. Technol. 2018;67(9):9042–9046. [Google Scholar]

36. Sharma D., Rashid A., Gupta S., Gupta S.K. A functional encryption technique in uav integrated hetnet: a proposed model. Int. J. Simul.–Syst. Sci. Technol. 2019;20 [Google Scholar]

37. Clark D.R., Meffert C., Baggili I., Breitinger F. Drop (drone open source parser) your drone: forensic analysis of the dji phantom iii. Digital Invest. 2017;22:S3–S14. [Google Scholar]

38. Ganti S.R., Kim Y. Unmanned Aircraft Systems (ICUAS), 2016 International Conference on. IEEE; 2016. Implementation of detection and tracking mechanism for small uas; pp. 1254–1260. [Google Scholar]

39. Kosmowski K., Matyszkiel R., “Verification of the criterion and measures of interferences used in radio planning systems,” in Proc. SPIE 11055, XII Conference on Reconnaissance and Electronic Warfare Systems, 110550J (2019). Google Scholar

40. Sliwa J., Matyszkiel R., Jach J., “Efficient Methods of Radio Channel Access Using Dynamic Spectrum Access That Influences SOA Services Realization - Experimental Results,” in 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), (2015). https://doi.org/10.1109/VTCSpring.2015.7145801 Google Scholar

41. Болховская О. В. Характеристики обнаружения пространственных сигналов для статистик обобщенного отношения правдоподобия в случае

коротких выборок / О. В. Болховская. А. А. Мальцев, К. В. Родюшкин // Изв. вузов. Радиофизика – 2007. – Т. 48. – № 5. – С. 446–453.

42. Кобилянський К. Є. Безпілотні літальні апарати. Сучасний стан та перспективи розвитку / К. Є. Кобилянський. – К. : Військова освіта. – 2012. – С. 328.

43. Otnes R. Improved receivers for digital High Frequency communications: Iterative channel estimation, equalization, and decoding (adaptive turbo equalization) / Roald Otnes // Department of Telecommunications. Faculty of Information Technology, Mathematics and Electrical Engineering. Norwegian University of Science and Technology. – Trondheim. – 2002. – 201 p.

44. Ю. Г. Даник, О. В. Манько, В. В. Павлюк. Алгоритм виявлення радіосигналів систем дистанційного керування безпілотними літальними апаратами / Даник Ю. Г., Манько О. В., Павлюк В. В. // Збірник наукових праць, ЖВІ НАУ. – вип.7. – 2013.

45. В.И. Тихонов, Б.И. Шахтарин, В.В. Сизых, «Случайные процессы, примеры и задачи», Том.5 Оценка сигналов, их параметров и спектров. Основы теории информации, Горячая линия – Телеком, Москва, 2009.- с.400.

46. Д.А. Навроцкий, «Система защиты радиоканалов БПЛА от несанкционированного вмешательства», Национальная ассоциация учёных (НАУ) #*III*(8), г. Киев, сс. 95-99, 2015 / Технические науки.

47. Р.В. Иванов, «Предложения по разработке математической модели воздействия имитационных помех на каналы управления БПЛА в режиме «Ожидания»», Science &ASC, pp. 45-49, 2016.

48. Р.В. Иванов, «Предложения по разработке математической модели воздействия имитационных помех на каналы управления БПЛА в режиме «Ожидания»», Science &ASC, pp. 45-49, 2016.

49. В.В. Гордійчук, «Методика підвищення скритності в системах радіозв’язку з ортогональним частотним мультиплексуванням за рахунок використання таймерних сигнальних конструкцій», Сучасні інформаційні системи, Том.2, №4, сс. 108-113, 2018.

50. О.В. Яровий, «Системи управління безпілотними літальними апаратами для здійснення моніторингу наземних об’єктів», Системи управління, навігації та зв’язку, випуск 3(49), сс. 33-38, 2018.

51. Qasim Abbood Mahdi, «The method of increasing the immunity of communication systems», Advanced Information Systems, Vol.3, №1, pp.126-130, 2019.

52. А.В.Науменко, Г.В. Шуклін, Барабаш О.В. « Проблема інформаційного захисту командної телеметрії безпілотних літальних апаратів» , Сучасний захист інформації. Київ: ДУТ, №4, сс.40-44, 2019.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

МЕТОДИКА ПІДВИЩЕННЯ ЗАХИСТУ РАДІОКАНАЛУ УПРАВЛІННЯ ВІД ПЕРЕХОПЛЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

СТУДЕНТ: Ганусяк Степан Ігорович
КЕРІВНИК: Шуклін Герман Вікторович

Мета роботи - підвищення точності розрахунку функції надійності захисту радіоканалу управління при передачі інформації від безпілотних літальних апаратів. **2**

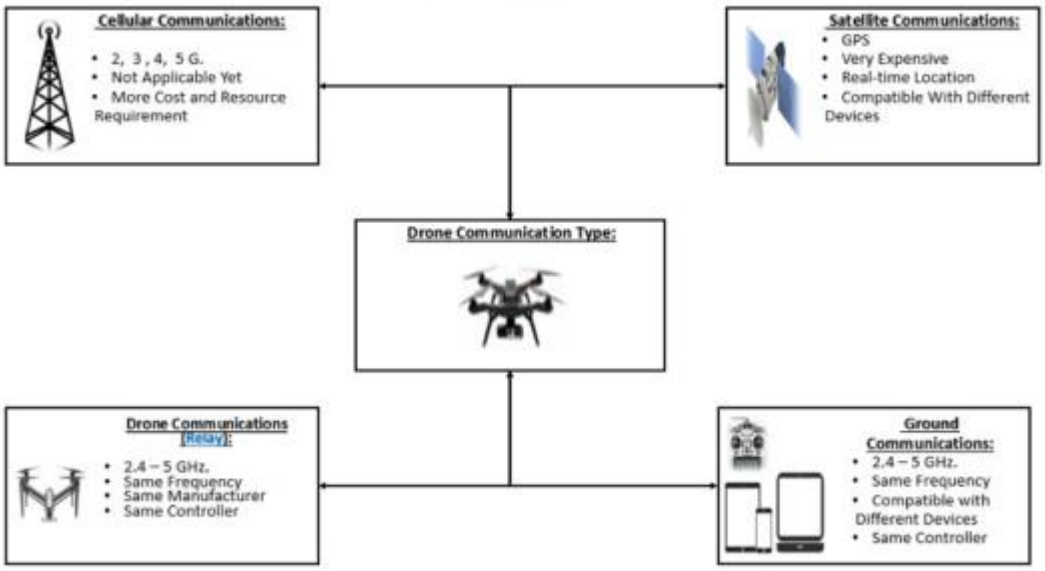
Об'єкт дослідження - безпілотні літальні апарати.

Предметом дослідження є методика захисту радіоканалів управління безпілотними літальними апаратами.

Завдання

- аналіз особливостей функціонування безпілотних літальних апаратів;
- дослідження проблеми безпеки безпілотників;
- аналіз існуючих методів захисту безпілотних літальних апаратів проти атак з використанням радіозасобів;
- розробка рекомендацій щодо підвищення безпеки безпілотників та безпілотних літальних апаратів;
- вдосконалення методики захисту радіоканалів управління безпілотними літальними апаратами.

СТРУКТУРА СПІЛКУВАННЯ МІЖ БПЛА 3



Атака	Ціль			Заходи безпеки	
Тип	**Конфіденційність даних**	**Доступність**	**Аутентифікація**	**Некриптографічний**	**Криптографічний**
Зловмисне програмне забезпечення	✓	✓	✓	Гібридна IDS	Контролюйте доступ, рішення щодо цілісності системи та багатофакторну автентифікацію
Соціальна інженерія	✓	X	✓	Підвищення обізнаності, навчання операторів	Н/д
Ін'єкція / модифікація	X	X	X	Гібридні IDS машинного навчання, позначки часу	Аутентифікація повідомлення або цифровий підпис
Scanning	✓	X	X	Гібридна легка IDS або Honeypot	Зашифрований трафік / потік
Man-in-the-Middle	✓	X	X	Гібридна IDS	Багатофакторна автентифікація та легкий потужний протокол криптографічної автентифікації
Злом паролю	X	X	✓	Лайт IDS	Міцні періодичні паролі, надійне шифрування
Wi-Fi Aircrack	X	X	✓	Легкі IDS на фізичному рівні	Сильні та періодичні паролі, потужний алгоритм шифрування
Перешкоди Wi-Fi	X	X	✓	Перехід частоти, зміна діапазону частот	Н/д
Переповнення буфера	X	X	✓	Перехід частоти, зміна діапазону частот	Н/д
Denial of Service	X	X	✓	Перехід частоти, зміна діапазону частот	Н/д
ARP Cache Poison	X	X	✓	Перехід частоти, зміна діапазону частот	Н/д
GPS Spoofing	X	X	✓	Повернення до бази, зміна діапазону частот	Н/д

4

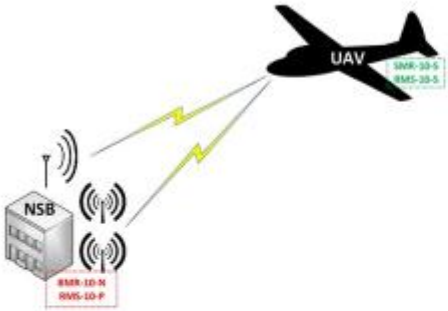


Рис.1. Концепція радіозв'язку БПЛА з NSB за допомогою літакової радіолінії

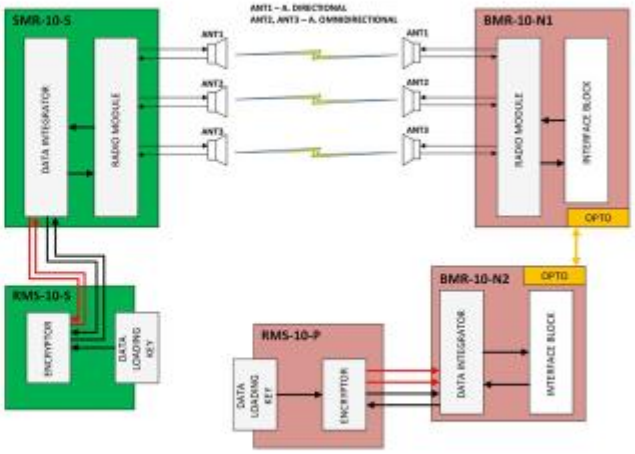


Рис.2. Блок-схема системи радіозв'язку

СХЕМА АЛГОРИТМУ ВИЯВЛЕННЯ СИГНАЛІВ СИСТЕМ УПРАВЛІННЯ БПЛА 6

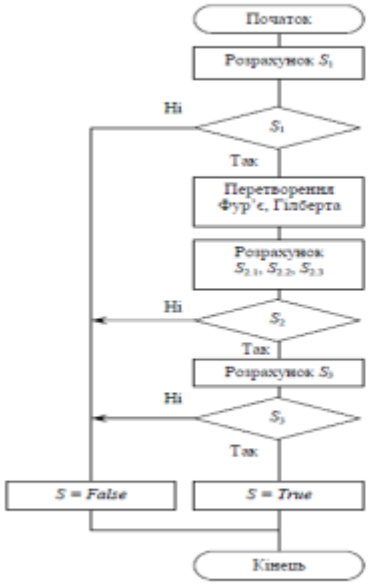


Рис.1. Алгоритму виявлення сигналів систем управління БПЛА

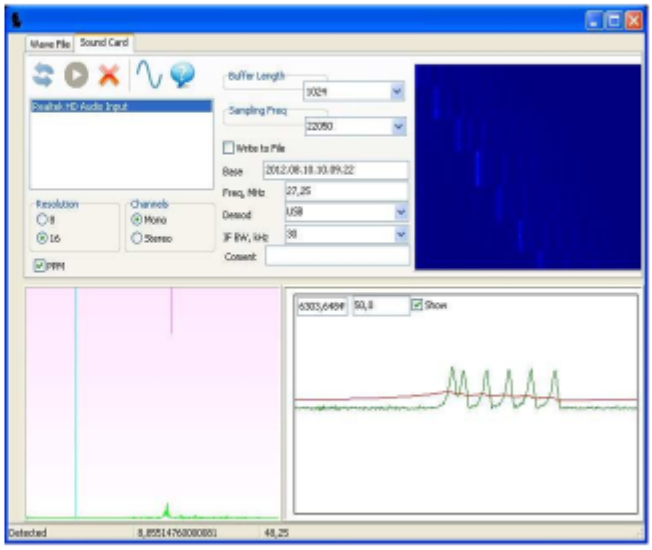


Рис.2.Практична реалізація розробленого алгоритму виявлення сигналів систем управління БПЛА здійснена у програмному засобі

ПРОПОЗИЦІЇ ЩОДО РОЗРОБКИ ПРОТОТИПУ БПЛА ІЗ ЗАХИЩЕННИМ КАНАЛОМ ЗВ'ЯЗКУ 7

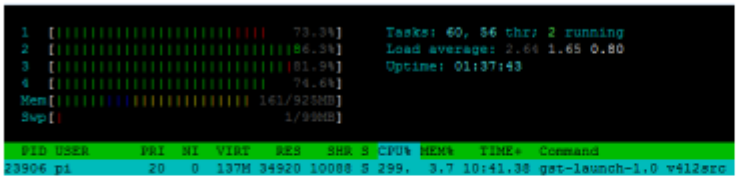


Рис.1. Завантаженість процесора при використанні плагіну x264

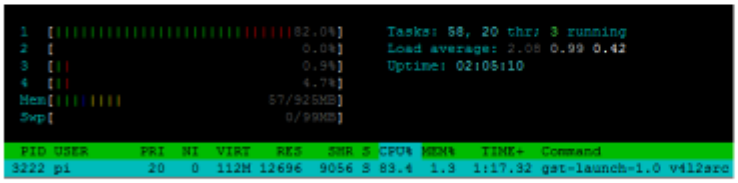


Рис.2. Завантаженість процесора при використанні плагіну OMX

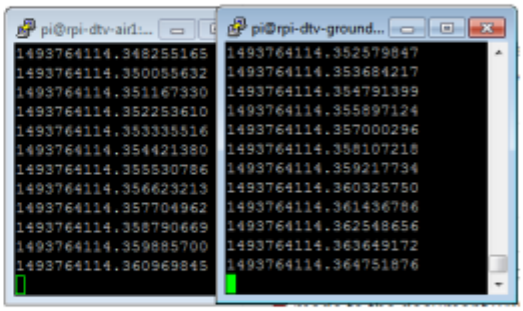


Рис.3. Порівняння часу після синхронізації

ВИСНОВКИ

В магістерській кваліфікаційній роботі було:

- описано архітектуру безпілотника, типи зв'язку та типи БПЛА. Також різниця між безпілотниками, БПЛА та БПЛА.
- представлено основні вразливі пункти безпеки та загрози, які можна використати, щоб поставити під загрозу безпеку безпілотників.
- досліджено можливі заходи безпеки безпілотника/БПЛА та протидію/БПЛА, на додаток до методів запобігання, та рішення, пов'язані з безпекою зв'язку та мереж безпілотників/БПЛА, які є важливими для збройних сил та рятувальні роботи.
- описано фізичні рішення, які базуються на кінетичних та некінетичних методах боротьби з безпілотними літальними апаратами. Всі описані методи використовуються в даний час, часто приносячи позитивні ефекти в дії.
- обговорено найважливіші функціональні можливості окремих елементів запропонованої архітектури. Використання описаних методів в апаратній реалізації ефективно зменшує ризик перешкод або переривань радіозв'язку між БПЛА та NSB.
- розроблено рекомендації щодо підвищення безпеки безпілотників/БПЛА з урахуванням обговорення основних загроз безпеці та конфіденційності, атак та відповідних технічних рішень.
- розроблено алгоритм, який забезпечує встановлення факту належності прийнятого радіовипромінювання до класу радіосигналів систем дистанційного керування БПЛА з імпульсно-позиційною та імпульсно-кодовою модуляціями. Зазначено, що алгоритм базується на послідовних перевірках енергетичної, модуляційної та структурної ознак сигналу, передбачає можливість автоматичного виявлення сигналу супроводження його за частотою.
- запропоновано конкретні апаратні та програмні рішення для побудови прототипу БПЛА. Наведено результати практичного тестування можливих рішень задач на готовому прототипі і наведено результати функціонування розроблених компонентів зв'язку.

Дякую за увагу!