**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»**
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

**КВАЛІФІКАЦІЙНА РОБОТА**

на тему:

# «ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КАНАЛУ ЗВ'ЯЗКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
**Стаднік Богдан Сергійович**

Керівник: к.ф-м.н., доцент
**Чепурна Олена Євгенівна**

Рецензент: д.ф.-м.н., професор
**Василенко Микола Дмитрович**

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека та захист інформації**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____»_____ 20__ року

**З А В Д А Н Н Я**
**на кваліфікаційну (бакалаврську) роботу**
**здобувачу Стадніку Богдану Сергійовичу**

1. Тема роботи: «Забезпечення захисту каналу зв'язку безпілотних літальних апаратів»
Керівник роботи: к. ф.-м. н., доцент **Чепурна О.Є.**

затверджені наказом НУ ОЮА від *«_____»_____№ _____*

2. Строк подання здобувачем роботи *«____» _____ 2024 року*

3. Дата видачі завдання *«_____» _____ 2024 року*

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів магістерської роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Видача завдання | 15.09.2024 | |
| 2 | Аналіз теоритичних відомостей | 24.02.2024-30.02.2024 | |
| 3 | Збирання інформації про зв'язок | 10.03.2024-22.03.2024<br>1.03.2024-7.03.2024 | |
| 4 | Написання першої частини | 10.03.2024-22.03.2024 | |
| 5 | Пошук інформації про заглушку зв'язк | 24.03.2024-27.03.2024 | |
| 6 | Написання другої частини | 28.03.2024-04.04.2024 | |
| 7 | Аналіз методів захисту зв'язку | 07.04.2024-16.04.2024 | |
| 8 | Написання третьої частини | 20.04.2024-02.05.2024 | |
| 9 | Здача роботи | 20.05.2024 | |

**Здобувач** _____
( підпис ) (прізвище та ініціали)

**Керівник роботи** _____
( підпис ) (прізвище та ініціали)

# АНОТАЦІЯ

Кваліфікаційна робота на тему «Забезпечення захисту каналу зв’язку безпілотних літальних апаратів» на здобуття бакалаварського рівня вищої освіти за спеціальності 125 «Кібербезпека».

Містить 28 рисунків, 1 таблиці, 38 літературних джерел за переліком посилань. Робота виконана на 46 сторінках загального тексту і 42 сторінках основного тексту.

Метою даної роботи є огляд та аналіз захисту зв'язку управління БПЛА, їх ролі та методи забезпечення безпеки дронів з конфінденційною інформаціює.

У роботі розглядаються теоретичні основи криптографічні алгоритми, їх принципи, недоліки та переваги. Проаналізовано ефективність методів захисту від кібератак та запобігання втрати важливої інформації. Також будуть розглянутий метод частотної модуляції. Проаналізовано ефективність роботи методу цього захисту. Рекомендації щодо подальшого захисту, щоб уникнути кібератак

БЕЗПІЛОТНИЙ ЛІТАЛЬНИЙ АПАРАТ, ЗАХИСТ, ЗВ’ЯЗОК, КРИПТОГРАФІЧНІ АЛГОРИТМИ

# ABSTRACT

Qualification work on the topic “Protection of the control channel of unmanned aerial vehicles from unauthorized access” for the bachelor's degree in higher education in the specialty 125 “Cybersecurity”.

Contains 28 figures, 1 table, 38 references according to the list of references. The work is executed on 46 pages of general text and 42 pages of the main text.

The purpose of this work is to review and analyze the protection of UAV control communications, their role and methods of ensuring the security of drones with confidential information.

The paper discusses the theoretical foundations of cryptographic algorithms, their principles, disadvantages and advantages. The effectiveness of methods for protecting against cyberattacks and preventing the loss of important information is analyzed.

The frequency modulation method will also be considered. The effectiveness of this protection method is analyzed Recommendations for further protection to avoid cyberattacks

UNMANNED AERIAL VEHICLE, PROTECTION, COMMUNICATION, CRYPTOGRAPHIC ALGORITHMS

ЗМІСТ

# ВСТУП

Захист каналу зв'язку безпілотних літальних апаратів (БПЛА) є критично важливою задачею для забезпечення їхньої безпеки та ефективності в умовах, коли може існувати загроза кібератак, перешкод або перехоплення зв'язку. Аналізуючи досвід у боротьбі з агресором показує, що за останній час використовують дуже інтенсивно безпілотну авіацію для успішного виконання бойових завдань, тому можливо назвати цю війну - “війна дронів”. З часом з’явились різні види дронів та їх використання. Дрони можливо використовувати у розвітці для подальшого аналізу стратегії, наведення артилерії і побудування тактики. Також активно використовують ударні дрони для знищення різної техніки та особового складу ворога, їх часто називають “дрони-камікадзе”.

Безпілотний літальний апарат має дуже широку сферу застосування. Це можуть бути завдання розвідки, рятувальні опеації, знищення ворожої техніки, спостереження та збирання інформації та багато інших застосувань. Застосування дронів значно спрощує роботу на фронті та збільшує безпеку для людей, також збереження житів особового складу, що приймають участь у різноманітних операціях. Система керування має бути на самперед ефективною. Тому при проектуванні системи керування використовувались модулі та блоки широко представлені на ринку, що мають необхідні параметри при не високій ціні.

Через зростаючу кількістю різних типів БпЛА, радіоелектронна протидії та хакерські атаки для досягнення доступу управління є найважливішим метою забезпечення захисту інформаційної системи. Необхідність про методів забезпечення захисту каналу зв'язку для БПЛА, такі як : Частотна модуляція, антиспуфінг, шифрування каналу зв’язку. Не можливо уникнути такі фактори коли мова йде про безпеку зв’язку управління БПЛА.

В більшості випадків дрони вразливі до багатьох атак. Ці атаки завдають шкоди безпілотникам, також і операторам дронів. У цій ситуації потрібне розуміння того, як хакери виконують свої атаки та викрадають дрон, щоб перехопити або навіть зруйнувати його. Насправді, зловмисники також можуть використовувати

безпілотники. Таким чином, їх потрібно знайти та пошкодити. Мало людей знають, як будуються радіоканали управління безпілотними літальними апаратами і як підвищити їх захист.

Об’єкт дослідження - канал управління БПЛА

Предметом дослідження є захист канал управління безпілотними літальними апаратами .

Мета роботи - визначити можливі методи захисту каналу управління при передачі даних.

Методи дослідження - для рішення використовуються криптографічні методи та частотні модуляції.

# 1 БУДОВА ОБЛАДНАННЯ БПЛА ТА ЇХ ВИДИ

## 1.1 Будова FPV дрона.

Будова FPV дрона представлена таким чином(рисунок 1.1).

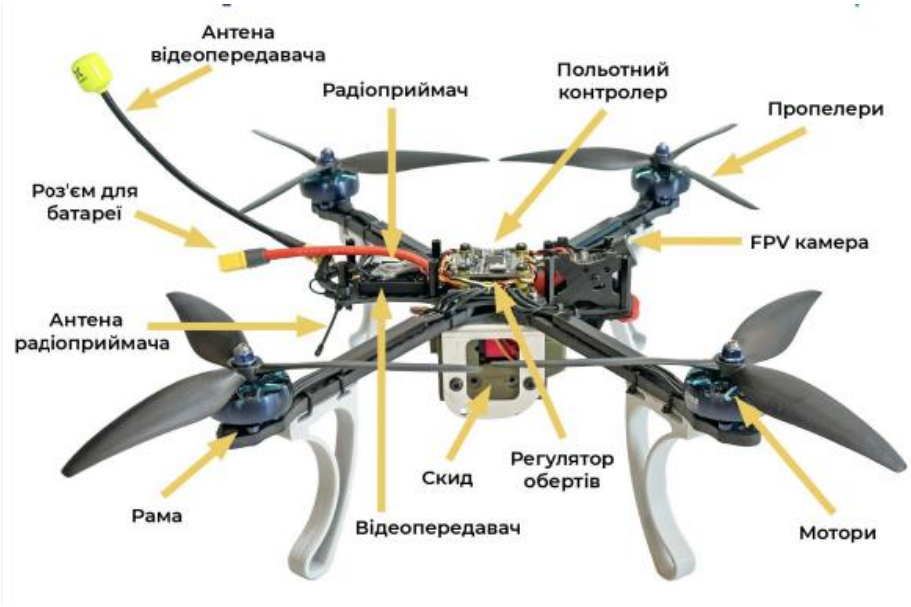


Рис.1.1 - Будова FPV дрона

Пульт, радіопередавач / Radio Transmitter, TX

Основним компонентом для FPV дронів: пульт, радіопередавач, TX Пульт (TX) - це портативний пристрій, за допомогою якого пілот керує дроном. Після того, як пульт передає радіосигнал на приймач (RX) дрона, польотний контролер (FC) перетворює ці сигнали на рух дрона. Щоб прилади могли з’єднатися, частоти пульта та радіоприймача дрона мають співпадати, а протоколи мають бути сумісними(рисунок 1.2)[32].


Рис. 1.2 - Радіопередавач

FPV окуляри / FPV Goggles

Основне обладнання для роботи з FPV дроном: FPV-окуляри приймають відеосигнал від передавача дрона (VTX) і дозволяють пілоту бачити картинку з FPV-камери дрона. Окуляри можуть бути цифровими або аналоговими. Існують аналогові адаптери для цифрових окулярів, які дозволяють приймати сигнал з аналогових VTX. Окуляри зазвичай включають вбудований відеоприймач (VRX) на 5.8 ГГц. Приймачі різноманітності мають два виходи антени, що дозволяє пристрою вибирати більш потужний сигнал. Аналоговий сигнал не є зашифрованим, тому відео з аналогового VTX може приймати будь-який відеоприймач, який знаходиться в зоні випромінювання антени. Цифровий сигнал шифрується, і якість цифрового відео значно вища, ніж аналогового. Але аналоговий сигнал може забезпечити дальність польоту в десятки кілометрів, на відміну від цифрового. Наразі фронт використовує переважно аналогові FPV-системи(рисунок 1.3) [32].


Рис. 1.3 - Основні компоненти

Рама

Розміри рами визначаються в дюймах відповідно до розмірів пропелерів, для яких вона розроблена, наприклад, 5 дюймів, 7 дюймів, 10 дюймів тощо.

Hybrid X, TrueX, Deadcat, H і Square (Box) - це типи рам за формою (рисунок 1.4). Популярним матеріалом є легкий і міцний карбон. Важливо пам’ятати, що карбон є електропровідним. Промені 7” дрона повинні бути не менше 5 мм[32].

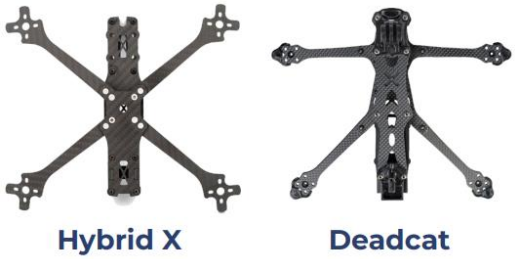


Рис. 1.4. - Рама

Гвинти та пропеллери (рисунок 1.5)

Пропелери можна маркувати в двох різних форматах: *ДДКК х Л або Д х К х Л*, де *Д* — довжина у дюймах. Можна визначити як відстань у дюймах, яку проходить пропелер за один оберт, називається К. Кількість лопатей називається Л. За годинниковою стрілкою напрямок обертів позначається CW або CCW проти неї.

Рис. 1.5. - Пропелери

Мотори

Дрони FPV використовують безколекторні двигуни (рисунок1.6). Маркування статора показує діаметр і висоту. Кількість обертів двигуна на 1 вольт напруги називається KV. Дрони мають навантаження на мотори 900-1500 KV. Характеристики 4s-6s вказують на кількість послідовно з’єднаних елементів батареї, які можуть забезпечити живлення мотору [32].


Рис. 1.6 - Мотори

Контролер руху FC - це плата керування дроном, яка обробляє сигнали власних сенсорів, таких як акселерометр, гироскоп і інші, а також команди пілота та визначає швидкість, яку потрібно надати моторам (рисунок 1.7).

FC має інтерфейси, такі як UART, I2C, PWM тощо, які можна використовувати для підключення ESC, VTX, RX, камер, GPS, сервомоторів та інших пристроїв. В даний час FC працюють на процесорах F4, F7 і H7. Програми BetaFlight, INAV і Ardupilot доступні FC.

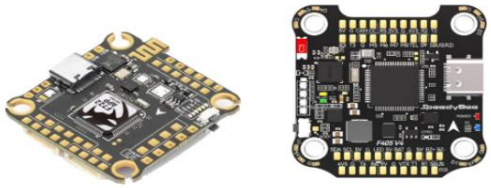

Рис. 1.7 - Польотний контролер

Регулятор обертів

За допомогою польотного контролера регулятор обертів регулює швидкість моторів дрона. ESC можуть бути 4 в 1 - для чотирьох моторів і окремі. При підборі моторів слід враховувати постійний і піковий струм ESC. Нова прошивка BLHeli_32 ESC підтримує протокол двонаправленого DShot. Це дозволяє ESC відстежувати швидкість обертання моторів і передавати польотному контролеру RPM-телеметрію, що покращує керованість дрона(рисунок1.8). Необхідно перепрошити софт Bluejay, щоб увімкнути телеметрію моторів ESC на BLHeli_S[32].


Рис. 1.8 - Регулятори обертів

Відеопередавач

VTX передає відеосигнал на окуляри пілота з камери(рисунок 1.9). VTX можуть передавати цифрові та аналогові сигнали. Незважаючи на те, що аналоговий сигнал має більшу стійкість і забезпечує більшу дальність, трансляцію можуть побачити будь-хто. На даний момент частоти аналогового відео 1,2 ГГц і 5,8 ГГц є найпоширенішими, а цифрового відео - 5,8 ГГц. 8 дронів можуть одночасно літати на аналоговій частоті 5,8 ГГц. Рекомендується використовувати потужні VTX на 1.6 Ватт або більше. Щоб керувати VTX, FC може використовувати протоколи IRC Tramp або SmartAudio [32].

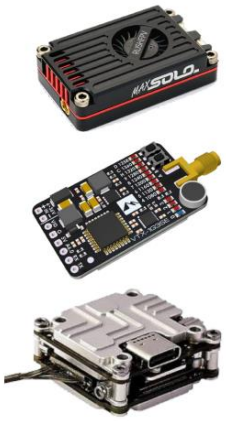

Рис. 1.9 - Відеопередавач

Курсова камера

Курсова камера для аналогових і цифрових FPV-систем не сумісні(рисунок1.10). Розміри камер Mini (21x21 мм), Micro (19x19 мм) і Nano (17x17 мм). Розподільна здатність аналогової камери вимірюється за допомогою

телевізійних ліній, також відомих як TVL. Що більше, то краще [32]. Він має перебувати в діапазоні від 1000 до 1500 TVL.


Рис. 1.10 - Курсова камера

Радіоприймач

Дрон отримує сигнали з пульта керування, а потім передає їх FC. TBS Crossfire або ExpressLRS, які працюють на протоколі CRSF, є найпоширенішими приймачами.

Для тренувань на невеликій відстані частоти 868/915 МГц і 2,4 ГГц є основними. Приймачі різноманітності з двома антенами забезпечують більш стійкий зв’язок (рисунок 1.11).


Рис. 1.11 - Радіоприймач

Антени

В FPV дронах є як мінімум дві антени:  Антена радіоприймача для отримання сигналів з пульта керування, які зазвичай працюють на частотах 868/915 МГц або 2,4 ГГц (рисунок1.12). Передача сигналу з дрона на очі пілота на частотах 5,8 або 1,2 ГГц. Антени можуть бути всеспрямованими або спрямованими, лінійними або

круговими. Антени цифрового лівої поляризації (LHCP) використовуються для передачі цифрового відео.


Рис. 1.12. - Антени

Батареї та стрепи

Літій-полімерні (LiPo) та літій-іонні (Li-Ion) батареї використовуються для стрепів і батарей FPV. LiPo мають кращу струмовіддачу, тоді як Li-Ion дешевші та мають більшу ємність при тій же вазі(рисунок 1.13).

Напругу збірки визначає кількість послідовно з’єднаних елементів у батареї. Три секунди, чотири секунди та шість секунд мають відповідні маркування. Батарея 6s2p складається з двох паралельно з’єднаних збірок 6s. Дрон кріпить батареї за допомогою пари стрепів.

Рис. 1.13. - Батереї та стрепи

FPV-дрони на війні: переваги та недоліки

Застосування FPV-дрону гарантує високу точність, швидкість та маневреність. Через ці якості дрони можуть знищувати ворожу військову техніку та особистий склад ворога, що збільшує шанси на успішне виконання завдання бійців.

Одною із важливих переваг використання FPV це його ціна, тому що для збірки потребується не велика сума відносно яку витрачають на озброєння. Один

FPV дрон обійдеться приблизно 500 доларів. Але при цьому він здатний знищувати на багато дорожщі в декілька пару сотих разів зразки озброєнь та військової техніки. FPV-дрони унікальні тим що вони управляються вручну, тому це великий плюс, тому що вони не пов'язані із супутниковою системою GPS, таким чином утворюється перевага в тому що вони не сприйнятливі до дії засобів радіоелектронної боротьби[15].

Існують інші певні недоліки:

1)Доводиться ставити легкі акумулятори і як правило вони можуть працювати лише кілька хвилин. Ставлять легкі акумулятори тому що потрібно підвісити потужну вибухову гранату для ураження, тому доводиться використовувати тільки цей варіант;

2)Існують недоліки яких називають ворожі "глушилки", тому що є ймовірність шо вони можуть заглушити глушити частоту яку використовує дрон при польоті. Існує метод захисту, який може це запобігти, а саме частотна модуляція[15].

## 1.2 Будова розвідного дрона

DJI Mavic 3 - це передовий квадрокоптер, який має багато функцій і здатний знімати високоякісні зображення та відео з повітря. Він вважається одним із найкращих сучасних квадрокоптерів[6]. Цей дрон легко транспортувати завдяки своїм невеликим розмірам і здатності згортатися. DJI Mavic Pro має чудові камери та тривалий час польоту. Квадрокоптер також має додаткову систему безпеки, включаючи автоматичне уникнення перешкод. Цей квадрокоптер також має покращений час польоту до 46 хв, що дає йому можливість перебувати тривалий час в повітрі. DJI Mavic 3 може знімати якісні зображення в форматі HDR. Крім того, він має інші функції, такі як: система навігації та вбудований GPS[6]. Також, Mavic 3 має аксесуар 4G, який можна під’єднати до дрона за допомогою USB-C і використовувати мобільну мережу для ефективного керування дроном. DJI Mavic 3 може бути корисним у війні з кількох причин:

1)Розвідка - дрон може знайти ворожі військові позиції;

2)Підтримка бойових дій - дрон може допомогти в бойових діях. Наприклад, він може надсилати військовим важливі дані;

3)Знищення ворожих цілей - це метод, за допомогою якого можна передати точні координати для наведення артилерії.

Коли почалася російсько-українська війна, цивільні дрони DJI Mavic були одними з найпоширеніших засобів розвідки для армії. Дрони використовувалися для:

1)розвідування території;

2)корегування роботи артилерії;

3)скидання саморобних боєприпасів[6].

Технічні характеристики:

1)Вага порожнього дрона DJI Mavic становить 895 грам;

2)Тривалий час польоту без вітру;

3)Максимальний час зависання без вітру — сорок хвилин;

4)Максимальна висота становить 6 000 метрів;

5)Довжина 380,1 мм;

6)Швидкість польоту на рівні моря без вітру становить до 21 м/с;

7)Максимальна дальність польоту  - тридцять кілометрів;

8)Внутрішня пам'ять 8 ГБ;

9)Температура місця роботи становить від -10° до +40°C;

10)Максимальна відстань передачі зображення — 15 км або 8 км, якщо використовується контролер CE;

11)Час автономної роботи 6 годин без зарядки мобільного пристрою[6].

Дизайн та будова зображено на рисунку 1.14

Рис.1.14 - Дизайн DJI Mavic 3

Пульт дистанційного керування входить в комплект та має такий вигляд як на рисунку 1.15 Пульт дистанційного керування Mavic 3 є повноцінним центром керування дроном. Процес польоту комфортний завдяки ергономічному дизайну та зручному інтерфейсу.

Рис.1.15 - Пульт дистанційного керування

Якість зображення та відео відеокамери Mavic 3 відтворює зображення з високою роздільною здатністю та деталізацією(рисунок1.16).

Рис.1.16 - Камера Mavic 3

Корпус

Зазвичай корпус складається з легких, але міцних матеріалів, таких як карбонові волокна або алюміній. Всі необхідні компоненти, включаючи електроніку, акумулятор, камеру та інші датчики, містяться в корпусі (рисунок 1.17).


Рис.1.17 - Корпус Mavic 3

DJI Mavic 3 має чотири ротори та пропелери. Вони відповідають за підйом і рух дрона в небі. У процесі транспортування ротори можуть бути складними (рисунок 1.18).

Рис.1.18 - Пропелери Mavic 3

Безплатформенний стабілізатор

DJI Mavic 3 оснащений передовими системами стабілізації, навіть у сильних вітрах або рухах безплатформенний стабілізатор DJI Mavic 3 має потужні функції стабілізації (рисунок 1.19) [13].


Рис.1.19 - Стабілізатор

Плюси використання :

1)Висока якість зображень і відео: Основна камера з 4/3-дюймовим сенсором від Hasselblad дозволяє отримувати детальні зображення та відео, що може бути критично важливим для розвідки;

2)Довгий час польоту: До 46 хвилин польоту на одному заряді дозволяє здійснювати тривалі місії без необхідності частого повернення для підзарядки;

3)Покращена система уникнення перешкод: Сенсори в усіх напрямках зменшують ризик зіткнення з перешкодами, що є важливим у складних умовах бойових дій;

4)Дальність польоту та передача відео: Система передачі відео O3+ забезпечує надійну трансляцію відео на відстані до 15 км, що дозволяє операторам працювати з безпечної відстані;

5)Інтелектуальні режими зйомки: Автоматичні режими зйомки, такі як ActiveTrack, можуть бути корисними для автоматичного стеження за об'єктами;

6)Компактність і портативність: Відносно невеликий розмір і вага дозволяють легко транспортувати дрон у польових умовах[13].

Мінуси використання:

1)Вразливість до електронних атак - електронні засоби протидії, такі як глушіння або злом сигналів, можуть атакувати дрони;

2)Розмір і вага можуть бути незручними для тривалих подорожей, де кожен грам важливий. Це може обмежити його використання в екстремальних умовах або в ситуаціях, коли потрібна висока мобільність;

3)Регулярне калібрування та оновлення програмного забезпечення може бути незручним але необхідним;

4)Залежність від погоди Mavic 3, як і більшість дронів, не водонепроникний і чутливий до сильного вітру. Це обмежує його використання в поганих погодних умовах, що може бути проблемою для зйомок у непередбачуваних кліматичних зонах [13].

## 1.3 Антена для керування дронами та БПЛА

Для надійного керування дронами та БПЛА з будь-якого укриття професійна виносна антена Profi Long Range ідеальна. Ця антена забезпечує фантастичний діапазон приймання та передавання відеосигналу на частоті 5.8 ГГц. Антена, яка поставляється з кабелем завдовжки 20 метрів, дозволяє легко під’єднуватися до джерела сигналу, що робить її надзвичайно гнучкими та зручними у використанні. Можливість передавати сигнал на монітори або відеоокуляри дозволяє оператору повністю контролювати процес спостереження. У діапазонах частот 868 МГц / 915 МГц антена забезпечує високу чутливість приймання на рівні 15 дБ і відеосигнал на рівні -98 дБм. Її спрямована діаграма антени з коефіцієнтом посилення до 22 дБ гарантує, що якість сигналу залишається високою, а втрати даних мінімальні. Антенна Profi Long Range з кутом відеоогляду 40 градусів і кутом каналу управління 50 градусів забезпечує широке охоплення та точне позиціювання, необхідні для виконання найскладніших завдань. Крім того, коефіцієнт передачі КВС не менше 1,25 гарантує довговічність і ефективне використання ресурсів (рисунок 1.20).

Максимізувати продуктивність і ефективність своєї роботи з дронами та БПЛА, антена Profi Long Range є незамінним інструментом [33]. Головні переваги:

1)Розширений діапазон дії - через широкий діапазон приймання та передавання відеосигналу антена дозволяє керувати дронами, коли вони перебувають в укритті;

2)Гнучкість підключення - Антена оснащена кабелем завдовжки 20 метрів, що дозволяє оператору самостійно вибрати найкраще місце для підключення до джерела сигналу;

3)Множинні виходи сигналу - здатність виводити сигнал на два приймачі для відеоокулярів або монітори;

4)Надійна робота в різних умовах - навіть у сильних перешкодах антена забезпечує високу чутливість приймання та стабільну якість сигналу;

5)Широке охоплення та точне позиціювання - Кути каналу керування та відеоогляду дозволяють забезпечує широке охоплення та точне позиціювання;

6)Ефективне використання ресурсів - антена Profi Long Range має коефіцієнт передавання КВС не менше 1,25 [33].

Рис. 1.20 - Виносна антена для керування дронами та БПЛА з укриття Profi long range

Специфікації винисної антени Profi Long Range:

1)Відеосигнал приймається з частотою 5.8 ГГц;

2)Вхідні порти: два виходи з пульта на монітори або відеоокуляри;

3)Напруга: 14–25 В;

4)Спрямованість антени є дві спрямовані антени мають коефіцієнт посилення 3 дБ, а одна спрямована до 22 дБ;

5)Сигнал управління має частоту 868 МГц / 915 МГц;

6)Чутливість приймання становить 15 дБ;

7)Рівень відеосигналу становить -98 дБм;

8)Огляд відео: 40 градусів;

9)Кут керуючого каналу: 50 градусів;

10)Коефіцієнт передавання КВС повинен перевищувати 1,25 [33].

# 2 ВИДИ РАДІОПРОТИДІЇ НОРМАЛЬНОМУ ФУНКЦІНУВАННЮ БПЛА

## 2.1 Радіоелектронна боротьба

РЕБ, також відомий як радіоелектронна боротьба, - це комплекс заходів, спрямованих на запобігання радіоелектронним засобам ворога та ускладнення роботи систем зв’язку ворога (рисунок 2.1). Завданням РЕБ є виявлення засобів спостереження противника, дезорієнтація їх і захист радіоелектронних систем від ворожого впливу. Основними цілями РЕБ є дезорганізація командування ворога[35]. Основними компонентами РЕБ є комплекси радіоелектронного придушення та захисту:

1) Радіоелектронне заглушення активно використовує електромагнітний перешкоди;

2) Електронні заходи підтримки підлягають у пасивному використанні електромагнітних хвиль. Воно допомагає отримати дані про противника, які можливо використовувати для виконання тактичних цілей. Наприклад, може бути користною інформація для застосування артилерійського вогню[4].

Рис. 2.1 - Українська система РЕБ “Буковель”

Засоби РЕБ, які працюють на суші, на морі або в повітрі, можуть передавати інформацію про розташування об’єктів, системи управління військами, зброю та техніку противника. РЕБ є тактичними і оперативно-тактичними[16].

Вплив радіоелектронної боротьби на хід бойових дій

Радиоелектронна боротьба може значно змінити хід битви. У ході бойових дій вона може використовуватися для вирішення наступних завдань: порушення роботи систем зв’язку та управління противника може ускладнити або унеможливити управління військами та бойовими діями, що може призвести до дезорієнтування противника та його поразки. Придушення роботи радарних систем противника може ускладнити або унеможливити використання авіації та протиповітряної оборони інших систем противника, що може призвести до переваги союзників. Введення противника в оману може призвести до помилкового рішення. РЕБ є складним і багатогранним процесом. Її продуктивність постійно зростає.[16].

## 2.2 Пристрої заглушка дронів

Відсутність стабільного сигналу є однією з проблем, яка турбує власників дронів з самого початку. Не тільки низька якість приймачів і передавачів безпілотників, але й глушилки викликають проблеми. Щоб забезпечити безпеку, ці пристрої встановлюють у різних місцях, особливо поруч із важливими цивільними та військовими об’єктами, але їх можна знайти навіть у сільських районах. Хоча FPV дрони мають багато переваг, вони все ж мають потенціал для збоїв. Наприклад, вони краще захищені від глушилок. Розглянемо «засліплюючі» пристрої та те, наскільки вони впливають на дрони нового покоління. Крім того, ми розглянемо способи захисту моделей First Person View[10].

Що таке глушилка для дронів?

Роботу коптера можуть передавати зображення або відео з камери пілота за допомогою різних бездротових технологій. Глушилка дронів - це спеціальний пристрій, який генерує та передає радіошум на певну відстань (рисунок 2.2). При попаданні безпілотника в його радіус дії відбувається наступне:

1)нездатний ідентифікувати та виконувати команди;

2)не може правильно посадити;

3)може впасти або врізатися  у будь-який момент;

4)вже не може використовуватися для військових чи інших завдань.

Конструкція глушилки дронів досить проста. Вона складається з корпусу з гніздами, кількох антен і кнопки керування, які можуть змінювати потужність або робочі частоти. Всередині є спеціальні плати, які служать для глушіння або зміни сигналу. Радіус впливу залежить від потужності, також принцип роботи, розміри та тип техніки відрізняються від один одного. Крім того, виділяються модифікації для цивільних і військових цілей[10].

Рис.2.2 Глушилка дронів

Робота глушилки дронів

Глушилки повинні надсилають більш потужний сигнал, ніж сигнал дистанційного керування, щоб успішно придушити придушити зв’язок з дроном. Таким чином, можна впливати не лише на команди управління, але й на передачу даних, трансляцію відео і GPS. Основне їхнє завдання - обірвати або пошкодити сигнал. Пристрої можуть відрізнятись принципами роботи (рисунок 2.3). Наступні варіанти:

1)Моделі, які приглушують всі сигнали;

2)Пристрої, спрямовані на заглушку зв’язку з системою глобального позиціонування;

3)Моделі, які можуть замінювати координати GPS;

4)Генератори електромагнітних імпульсів[10].

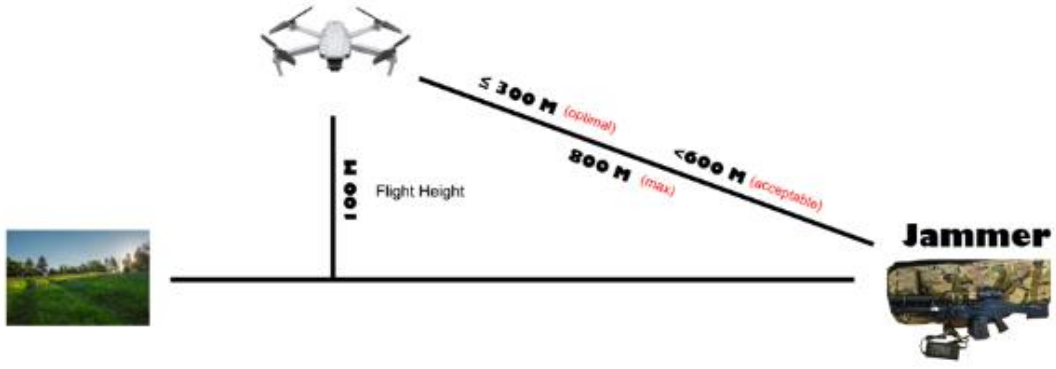


Рис.2.3 - Принцип роботи глушилки дронів

Чи можна заглушити FPV квадрокоптер

Вважається, що сучасні коптери, що передають відео в режимі онлайн, найбільш захищені від глушилок, зокрема від впливу на зв'язок з GPS. Тип і призначення безпілотника визначають багато речей. Для початківців FPV дрон навряд чи витримає потужний подавляч, але військовий безпілотник може продовжувати політ і надсилати сигнал. Потрібно створити модель, здатну протистояти квадрокоптерам, якщо передбачається, що вони будуть використані поблизу глушилок[10]. Сьогодні ще не існує дронів, які повністю захищені від зовнішніх факторів, тому FPV квадрокоптер потрібно захистити, якщо це можливо. Зробити це можна таким чином:

1)Уникати попадання в радіус дії глушилок;

2)Відстежувати зміни поведінки дрона та його реакцію на команди;

3)Заздалегідь підкоригувати налаштування, щоб апарат міг робити посадку в разі втрати сигналу;

4)Придбати безпілотник, який має можливість автоматично повертатися додому;

5)Використовуйте поточну прошивку;

6)Використовувати конструкції та речі, щоб перешкоджати сигналу глушилки[10]

Пристрій протидії БПЛА направленої дії Antidrone jammer DJ-04-70

Пристрій протидії БПЛА Antidrone jammer DJ-04-70 - портативний переносний пристрій для створення радіоелектронних завад. Призначений для запобігання несанкціонованому підльоту (прольоту, стеженню, зависанню) безпілотних літальних апараті (рисунок 2.2). В основі Антидрон DJ-04-70 - генераторна частина зі спрямованими антеннами, які випромінюють радіочастотний білий шум, що в свою чергу, запобігає передаванню радіосигналів керування, позіціонування та відеозвязку БПЛА.

Характеристики глушилки дронів Антидрон DJ-04-70:

1)Тип випромінювання: білий шум;

2)Загальна потужність випромінення: 70 Вт;

3)Напрямок випромінення: 30-35 градусів;

4)Кількість частот глушіння: 4[11];

5)Живлення: вбудований акумулятор 24 В, 7000 А/год;

6)Додатковий зовнішній акумулятор 24 В, 10500 А/год (в комплект не входить);

7)Час безперервної роботи від вбудованого акумулятора: 50-75 хв;

8)Загальний час роботи з комплектом зовнішнього акумулятора (в комплект не входить): близько 2 годин;

9)Тип охолодження: пасивне;

10)Ступінь захисту: IP66;

11)Вага пристрою з вбудованим АКБ: 4,2 кг;

12)Вага зовнішнього АКБ: 2 кг.

Частотні діапазони, потужність та призначення:

1)855–925 МГц, 20 Вт, 43 дБм (канал керування та передавання відеозв’язку FPV дрони);

2)1550–1620 МГц, 10 Вт, 40 дБм (супутникова навігація GLONASS, GPS, Beidou, Galileo);

3)2400–2500 МГц, 20 Вт, 43 дБм, (канал керування та передавання відеозв’язку);

4)5700–5900 МГц, 30 Вт, 43 дБм (канал керування та передавання відеозв’язку).

При наведені пристрою у бік підльоту БПЛА відбувається повне блокування сигналів керування, передачі відеозвязку та супутникового позіціонування БПЛА (рисунок 2.4). Дрон немає змоги повернутися, передати інформацію або ж здійснити інші маніпуляції (включаючи активацію системи скидання предметів) та поводить себе за одним з прогнозованих сценаріїв:

1)Аварійна посадка (в більшості випадків), що дозволяе вам заволодіти БПЛА;

2)Зависання до повного розряду акумуляторної батареї, що в кінцевому результаті призводить до посадки;

3)Зависання з подальшим дрейфуванням за напрямком вітру, з кінцевим падінням в результаті зачеплення за зелені насадження;

4)Неконтрольоване падіння (програмуется в деяких БПЛА);

5)Габаритні розміри 700х270х50 мм[11].

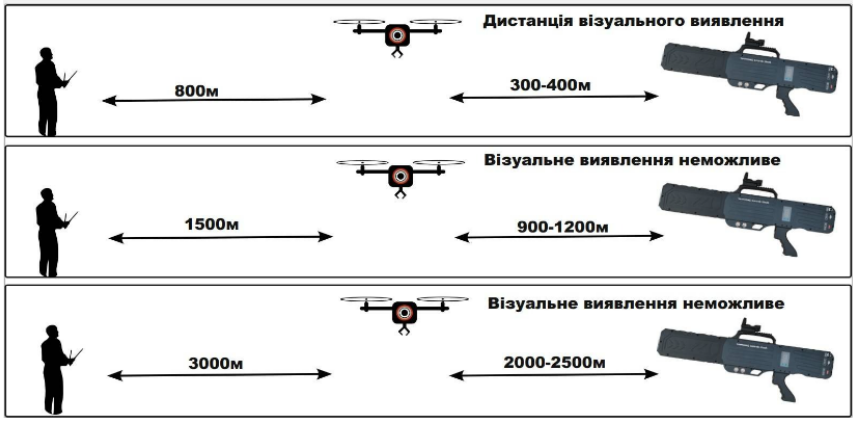


Рис.2.4 - Структура виявлення

Таблиця 2.1 - Харектиристика глушилок

| Вид | Глушилка дронів |
|---|---|
| Загальна потужність | 80 Вт |
| Маса комплекта, кг | 4,2 |
| Радіус дії | 2000 м |
| Розміри | 700х270х50 мм |
| Час автономної роботи | 120 хвилин |
| Пригнічувані частоти | 845-965 МГц;1550-1620 МГц;2400-2500 МГц;5500-5945 МГц |

## 2.3 Кібератаки на канали управління БПЛА

Кібератаки - це дії, які здійснюються в кіберпросторі за допомогою електронних комунікацій і спрямовані на досягнення одного або кількох цілей: порушення конфіденційності, цілісності або доступності електронних

інформаційних ресурсів, що обробляються в комунікаційних та технологічних системах.[18].

Кіберпростір - це віртуальний простір у якому люди можуть спілкуватися та створювати суспільні відносини за допомогою сумісних комунікаційних систем і електронних мереж передачі даних, таких як Інтернет.[18]. Кіберпростір дозволяє людям обмінюватися, ділитися та взаємодіяти з інформацією у віртуальній мережі. Майже щороку в сучасному світі Інтернету з'являються нові загрози для національної та міжнародної безпеки. Наразі хакерські угрупування здійснюють кібератаки через кіберпростір з різними цілями, наприклад: пошкодження ІКС та системи зв'язку за допомогою вірусного програмного забезпечення, спам; несанкціонований доступ до конфіденційних даних з метою їх публікації або спотворення; атаки DDoS, які блокують веб-ресурси, які є важливими для уряду та держави.

Коли зловмисник маскується, щоб отримати доступ до даних або інформації, це називається кібератакою. Зловживання може відбуватися через телефонні дзвінки, електронні листи, веб-сайти, текстові повідомлення, IP-адреси та сервери[36]. Спуфінг може використовуватися за допомогою кількох різних каналів зв'язку та вимагає різних рівнів технічного знання. Атака спуфінгу повинна включати певний рівень соціальної інженерії, щоб вона була успішною. Це означає, що шахраї можуть успішно обманювати своїх жертв, даючи їм особисту інформацію. Шахраї використовують соціальну інженерію, щоб зіграти на страх, жадібність і наївність[19]. Спуфінг має чотири основні види, які він може використовувати в мережі Інтернет: spoofing MAC-адреси, spoofing ARP, spoofing IP, spoofing DNS і spoofing GPS.

Підробка GPS змінює сигнали або дані, пов'язані з системою глобального позиціонування, щоб надати іншу інформацію про місцезнаходження, навігацію чи час (PNT). Це метод, який змусить GPS-приймач і програми, запущені на ньому, вважати, що ви перебуваєте в іншому місці чи в інший час[37]. Такий тип спуфінг-атаки починається з широкомовного передавання сигналу, що вказує правильну позицію. Потім атакуючий поступово змінює позицію, оскільки надмірно швидке

переміщення призведе до втрати сигнального блокування, і атакуючий буде сприйматися одержувачем лише як передавач перешкод [20].

Spoofing MAC-адреси - це техніка зміни призначеної на заводі адреси керування доступом до медіа (MAC) мережевого інтерфейсу на мережевому пристрої. MAC-адресу, жорстко закодовану на контролері мережевого інтерфейсу (NIC), не можна змінити. Однак багато драйверів дозволяють змінювати MAC-адресу. Крім того, існують інструменти, які можуть змусити операційну систему повірити, що мережевий адаптер має MAC-адресу за вибором користувача. Процес маскування MAC-адреси відомий як MAC-спуфінг. По суті, підробка MAC-адрес передбачає зміну ідентичності комп'ютера з будь-якої причини[21].

Spoofing ARP- це форма спуфінгу , яку хакери використовують для перехоплення даних. Хакер здійснює атаку ARP-спуфінгу, обманом змусивши один пристрій надіслати повідомлення хакеру замість передбачуваного одержувача. Таким чином хакер отримує доступ до комунікацій вашого пристрою, включаючи конфіденційні дані, такі як паролі та дані кредитних карток. На щастя, захистити себе від цих атак можна кількома способами. Атака ARP spoof може мати кілька цілей. Зловмисники можуть використовувати ARP-спуфінг для шпигунства, атак типу "людина посередині" або для додаткових кібератак, наприклад атак типу "відмова в обслуговуванні". Хакери використовують ARP-спуфінг з 1980-х років. Атаки хакерів можуть бути спланованими або випадковими. Заплановані атаки включають атаки на відмову в обслуговуванні, тоді як викрадення інформації з загальнодоступної мережі WI-FI було б прикладом опортунізму. Хоча цим атакам можна запобігти, вони все ще часто використовуються, оскільки їх легко здійснити як з фінансової, так і з технічної точки зору. Досить простим способом захисту від ARP-спуфінгу є використання брандмауерів із фільтрацією пакетів. Брандмауери з фільтрацією пакетів позначають пакети даних з адреси, яка двічі знайдена в мережі, оскільки це дублювання передбачає присутність когось, що маскується під інший хост[22].

IP-спуфінг - це створення пакетів Інтернет-протоколу (IP), які мають змінену адресу джерела, щоб або приховати особу відправника, або видати іншу

комп’ютерну систему, або і те, і інше. Це техніка, яку часто використовують зловмисники, щоб викликати DDoS-атаки на цільовий пристрій або навколишню інфраструктуру. Хоча IP - спуфінгу неможливо запобігти, можна вжити заходів, щоб зупинити проникнення підроблених пакетів у мережу. Дуже поширеним захистом від спуфінгу є вхідна фільтрація, описана в BCP38 (документ із найкращої загальної практики). Вхідна фільтрація - це форма фільтрації пакетів, яка зазвичай реалізується на крайньому пристрої мережі, який перевіряє вхідні IP-пакети та переглядає їх вихідні заголовки. Якщо вихідні заголовки в цих пакетах не збігаються з їхнім джерелом або з іншого боку виглядають підозріло, пакети відхиляються. Деякі мережі також реалізують вихідну фільтрацію, яка переглядає IP-пакети, що виходять з мережі, гарантуючи, що ці пакети мають законні вихідні заголовки, щоб запобігти запуску вихідної зловмисної атаки за допомогою IP-спуфінгу [23].

DNS-спуфінг - це використання DNS-протоколів, хоча принцип ідентичний IP-спуфингу.

Взлом БПЛА та методи захисту

Дрон можна взламати різними способами. Це технічно не складно, і багато власників не дуже дбають про захист. Кіберзлочинець може контролювати безпілотник або перехоплювати відео та зображення, які дрон передає на базову станцію. Зловмисники можуть замінити сигнал GPS. Після отримання додаткових координат дрон скасує свій перший маршрут і полетить туди, куди накаже новий господар. Крім того, він має здатність посадити дрон і викрасти його і всі файли на карті пам'яті.

Аналізатор трафіку, також відомий як сніфер - це програма або програмно-апаратний пристрій, призначений для перехоплення трафіку для подальшого аналізу або просто для аналізу трафіку мережі, який надходить до інших вузлів. Перехоплення трафіку може відбуватися в таких випадках:

1)Звичайне використання мережевого інтерфейсу;

2)Встановлення сніфера в розриві між каналами;

3)Відгалуженням трафіку, який може бути апаратним або програмним і передавати копію його на сніфер;

4)Через аналіз побічних електромагнітних випромінювань і збір трафіку;

5)Вони перенаправляють трафік жертви або весь трафік сегмента на сніфер після атаки на канальний або мережевий. Після цього трафік повертається до належної адреси;

Зловмисники можуть легко отримати незашифровані дані, оскільки звичайні дрони, які продаються в магазинах, часто не захищаються шифруванням [23]. Тому існують певні методи захисту дрона, щоб запобігти невдачі:

1)Потрібно встановити надійний пароль для базової станції. Складна комбінація зменшує шанси зловмиснику;

2)У дрона має бути увімкнено функцію повернення додому. Так можливо зберегти дрон і повернути його у разі втрати або заглушки сигналу;

3)Обов’язково онова прошивку дрона. З появою нових загроз основні виробники дронів випускають виправлення; регулярне оновлення допоможе вам уникнути їх;

4)Встановлення віртуальної мережі. VPN - це засіб, який шифрує ваш інтернет-трафік і приховує IP - адресу для безпеки й конфіденційності вашого підключення до Інтернету. Таке шифрування робить вашу інформацію закодованою, що захищає вас від відстеження та збору даних про ваші онлайн-дії третіми особами[24].

# 3 РЕКОМЕНДАЦІЇ ЗАХИСТУ КАНАЛУ ЗВ’ЯЗКУ БПЛА

## 3.1 Криптологічний метод

З вибору криптоалгоритму для забезпечення безпечного передавання зв’язку я розглянув декілька варіантів алгоритму з симетричним ключем AES, Blowfish та алгоритм з асиметричним ключем ECC.

Симетричний блоковий криптоалгоритм AES

Для блокового шифрування Advanced Encryption Standard використовує симетричний алгоритм, який може працювати з блоками 128 біт і ключами 128, 192 або 256 біт. AES працює з масивом 4 на 4 байти, відомим як стан; версії алгоритму з більшим розміром блоку мають додаткові колонки (рисунок 3.1). Алгоритм для 128-bit ключа має десять раундів, протягом яких виконуються наступні операції: SubBytes, ShiftRows, MixColumns та AddRoundKey[25].

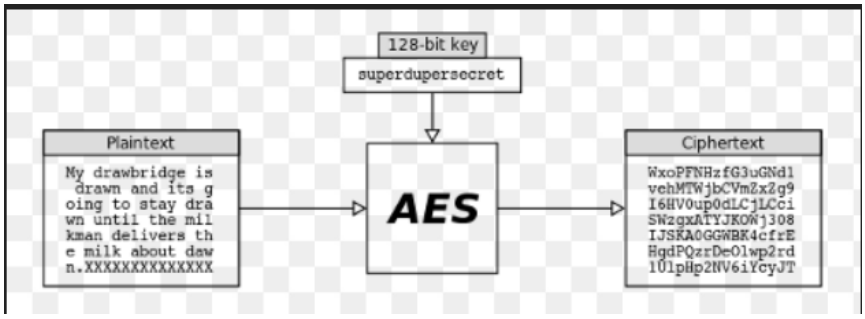


Рис.3.1 - Структура алгоритму AES

Насправді алгоритм AES і запропонований Рейменом і Дейцменом не схожі. Алгоритм Рейндол підтримує різні розміри блоків і ключів. Ключ AES може мати довжину 128 біт, але він також може мати довжину ключа 128, 192 або 256 біт.

Симетричний блоковий криптоалгоритм Blowfish

Алгоритм Blowfish - це блоковий шифр із симетричним ключем, призначений для безпечного шифрування та дешифрування даних. Він був розроблений Брюсом Шнайером у 1993 році як альтернатива існуючим алгоритмам шифрування, забезпечуючи високий рівень безпеки та ефективності. Blowfish працює з блоками

даних фіксованого розміру та використовує ключ змінної довжини для виконання операцій шифрування та дешифруванню.

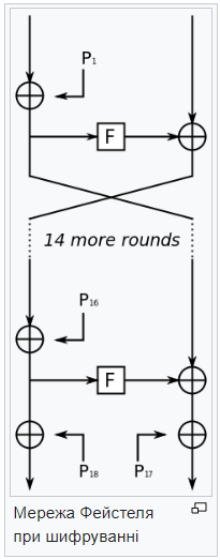


Рис.3.2 - Структура алгоритму Blowfish

Blowfish розділено на дві частини:

1)перша частина - алгоритм починається з секретного ключа шифрування, який створює кілька підключів. Генерація підключів Blowfish є складним і безпечним процесом.

2)друга частина - утворюються масиви P і S за допомогою секретного ключа; створення P1-P18 фіксованим рядком, що складається з 16 бітів.

Операція XOR виконується над P1 з першими 32 бітами ключа K, над P2 з другими 32 бітами та так далі. Ключ K накладається циклічно.

Алгоритм шифрування 64-бітного блоку використовує початкові ключі і таблицю замін для шифрування нульового рядка з 64 бітами (0x0000000000000000). Наступим кроком є отримання результату, після чого шифрування завершується, коли змінились всі ключі і таблиці замін.

Шифрування тексту за допомогою ключів і функції F, після чого його було розділено на блоки по 64 біти. Якщо початковий текст неможливо розбити точно на 64 біти, повідомлення створюється з цілого числа блоків за допомогою різних режимів шифрування. Необхідна загальна кількість пам’яті 4168 байт.

Фіксовані рядки використовується у зворотному порядку під час розшифрування, яке відбувається аналогічно [26].

Асиметричне шифрування ECC

Еліптична криптографія - це метод криптографії з відкритим ключем. Щоб забезпечити еквівалентну безпеку, ECC дозволяє використовувати менші ключі порівняно з криптографією, що не відповідає стандартам EC (рисунок 3.3)[31].

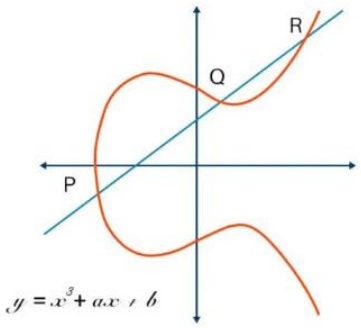


Рис.3.3 - Структура алгоритму ECC

Еліптичні криві можна використовувати для узгодження цифрових підписів, псевдовипадкових генераторів, ключів тощо. Коли узгодженість ключів поєднується з симетричною схемою шифрування, їх можна використовувати непрямо для шифрування. Багато алгоритмів цілочисельної факторизації, які використовуються в криптографії, використовують їх, наприклад факторизацію за еліптичною кривою Ленстри. У 1985 році математики Віктор Міллер і Ніл Кобліц запропонували використовувати еліптичні криві для криптографії. Алгоритм Elliptic Curve Cryptography почали використовувати в 2004-2005 році, майже через два десятиліття після їх розробки. Еліптична крива, створена під час процесу шифрування ECC, представляє набір точок, які відповідають математичному рівнянню *(y 2 = x 3 + ax + b)*[31].

ECC надає потужну безпеку від сучасних методів злому, незважаючи на те, що його довжина ключа коротша, ніж у RSA. Якщо використовувати короткі ключі у алгоритмі ECC, то він навіть може забезпечує кращу продуктивність. Одним із самих головних факторів є менше навантаження мережевого та обчислювальної

потужності, тому вони ідеально підходять для пристроїв, які мають мало місця для зберігання та обробки даних, таких як БПЛА.

Алгоритм ECC в сертифікатах SSL/TLS значно скорочує час шифрування та дешифрування. Програми для шифрування, цифрових підписів і псевдовипадкових генераторів використовують алгоритм ECC. Але велика проблема з широким використанням ECC полягає в тому, що багато серверних програм і панелей управління ще не підтримують сертифікати ECC SSL/TLS. Незважаючи на те, що це може змінитися в недалекому майбутньому, RSA все ще залишається найпоширенішим алгоритмом асиметричного шифрування[30].

## 3.2 Протоколи захисту

Вони забезпечують більш нові методи захисту, протоколи захисту WPA2 та 802.1X. Оскільки більшість сучасних дронів були виготовлені після 2007 року, вони швидше за все підтримують протоколи захисту WPA2 та 802.1X. Система шифрування WPA2 базується на останній редакції стандарту IEEE 802.11i. Алгоритм шифрування базується на блочному шифрі Advanced Encryption Standard (AES). Він використовує протокол Counter-Mode CBC MAC Protocol (CCMP). Основна відмінність між протоколами CCMP і TKIP полягає в тому, як вони шифрують і дешифрують дані: TKIP використовує чотири тимчасових ключі шифрування, тоді як AES використовує три. В обох випадках механізм керування ключами ідентичний. Основним недоліком системи є те, що для підвищення рівня мережі необхідно придбати нове обладнання, що підтримує алгоритм шифрування AES, оскільки центральний процесор змушений нести значну кількість алгоритму[1].

Протокол захисту RADIUS

Remote Authentication Dial-In User Server (RADIUS) Багато мереж використовують його. Протокол безпеки використовує модель клієнт-сервер для ідентифікації віддалених користувачів. Він реалізується як набір запитів і відповідей, які клієнт передає кінцевому користувачу від сервера доступу до мережі

(NAS). Протокол RADIUS був розроблений для забезпечення ідентифікації, авторизації та реєстрації дій користувачів, які потребують доступу до різних обчислюваних ресурсів.

Шифровка каналу зв'язку БПЛА є життєво важливим для забезпечення конфіденційності, цілісності та захищеності переданих даних. Одним із різновидів шифрування є віртуальна приватна мережа. Використання віртуальної приватної мережі (VPN) дозволяє створювати зашифровані тунелі між різними вузлами мережі, такими як БПЛА та земною станцією або контрольним центром [1].

## 3.3 Частотна модуляція БПЛА.

Частотна модуля́ція - модуляціяза допомогою якого частота вихідного сигналу змінюється у часі, таким чином інформаційний сигнал керує частотою опорного сигналу (рисунок 3.4).Частотна модуляція використовує миттєву амплітуду модулюючого сигналу, щоб безпосередньо змінювати частоту несучого сигналу. Індекс модуляції, використовується для опису відношення максимального відхилення частоти несучої до максимального відхилення частоти модулюючого сигналу. Використання широкого спектру частот або частотної модуляції, що ускладнює перехоплення сигналу та сприяє стійкості до перешкод [5].

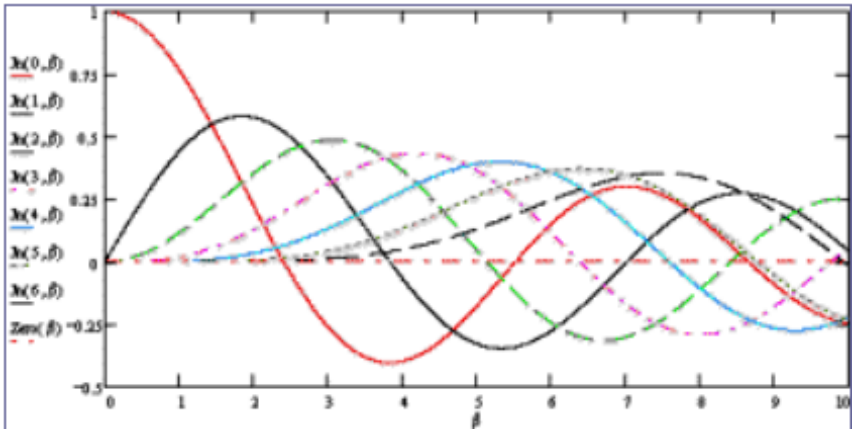

Рис.3.4 Частотна модуляція

Одними з найбільш потужних засобів захисту зв’язку є методи на основі зміни робочої частоти і вони зараз є одними з найбільш досліджених і стрімко розвиваються у галузі захисту зв’язку. Так, у статті [26] описано сучасну систему зв’язку з псевдовипадковим переналаштуванням робочої частоти, яка забезпечує високу стійкість системи до електромагнітного придушення, засобів РЕБ і засобів РЕР. Дзяйло В.В., інший дослідник, у своїй роботі [27] розглянув основні характеристики каналів зв’язку з частотним мультиплексуванням, принципом захисту. Він також розповів про методи та методи покращення характеристик захисту та стабільності роботи каналів зв’язку. Передача інформації на різних частотах є основною перевагою цього методу захисту каналу зв’язку. Це дозволяє, навіть у випадку електромагнітного зашумлення каналу, перейти на іншу незайняту частоту для продовження роботи. Це підвищує стійкість системи зв’язку в умовах активного протиборства. Другим важливим елементом захисту за допомогою зміни частоти є те, що постійна зміна частоти значно ускладнює перехоплення чи придушення сигналу зловмисником, а також виявлення сигналу. Так, у роботі, яку написали Бігун Наталія та Грозовський Роман [28], автори дослідили, як зміна частоти впливає на захищеність каналів зв’язку до засобів радіоелектронної розвідки та радіопеленгації. Вони виявили, що зі збільшенням швидкості переналаштування захищеність каналу зв’язку до виявлення зростає. Сигнал на певній частоті з’являється і зникає швидше, ніж сканер може його побачити, оскільки ймовірність виявлення прямує до нуля, коли швидкість переналаштування частоти засобу зв’язку наближається до швидкості радіопеленгації або до її перевищенням.

Основна мета каналів полягає в тому, що передавачі призначені для особистого використання. Тому діапазони частот, які можуть використовувати особисті користувачі каналів у різних регіонах або країнах, строго регулюються та регулюються законом. Виробники пристроїв беруть це до уваги, щоб захистити операторів від ненавмисного порушення законодавства. Така визначеність має небезпечний наслідок: оскільки це відкрита інформація, ворог також знає про неї. Смуга частот стандартного набору каналів становить від 5705 МГц до 5945 МГц,

якщо ми дозволимо оператору перемикатися між каналами на пульті керування БПЛА, щоб виконати частотне переналаштування. Крім того, ці набори каналів мають заздалегідь визначені значення.Це дозволило створити більш компактні засоби РЕБ для локального використання, які працюють у вищезазначеному частотному діапазоні. Ці пристрої зазвичай виконують електромагнітне зашумлення певного неперервного діапазону, відоме як «білий» шум. Це може звести нанівець переваги перемикання каналів, оскільки засіб РЕБ може заглушити всі доступні канали [29].

## 3.4 Вторинні способи захисту каналу зв’язку

Фільтрування MAC-адреси, також відома як керування доступом до носія, або керування доступом до медіа. Це унікальний ідентифікатор обладнання, який надає виробник. Фільтрація MAC-адреси означає, що доступ до мережі буде обмежений певними користувачами. Хоча це не зупиняє злочинця, це додає йому додаткову заваду. Крім того, для великих мереж важко швидко оновлювати список MAC-адрес.

Заборона трансляції ідентифікатора SSID у різних мовах. SSID. Це ідентифікатор мережі, який потрібно знати, щоб підключитися. CSID може бути широко поширеним в ефір або «прихованим». У другому випадку клієнт повинен визначити ідентифікатор у налаштуваннях підключення. Більшість пристроїв дозволяють приховати його, щоб при скануванні мережі його не було видно. Крім того, необхідно змінити встановлений SSID. Хоча це не надто значна перешкода, вона вимагає елементарних заходів безпеки. Також заборона доступу до налаштувань роутера або точки доступу через бездротову мережу. Активація цієї функції дозволяє заблокувати доступ до налаштувань точки доступу через мережу Wi-Fi. Мінімальна радіозона ідеально підходить, щоб вона не виходила за межі контрольованої території. Параболічні відбивачі можна встановити, якщо це необхідно, щоб запобігти розповсюдженню сигналу в небажаних напрямках.

Один із способів є резервне створення мережі на випадок якщо один із них буде не доступна, також можливо зазначити, що через цей спосіб можливо покращити стійкість мережі[1].

# ВИСНОВОК

Як результат у цій роботі було виконано аналіз радіопротидії нормальному функціонуванню БПЛА, можливі кібератаки на дрон та способи їх запобіганню.

Ознайомився з структурою безпілотника, а також його бортове обладнання та категорію БПЛА. Крім того, були враховані системи управління безпілотниками;

Проаналізовано існуючі системи безпеки, які захищають безпілотні системи, включаючи криптографічні та некриптографічні системи. Криптографічні рішення спрямовані на захист даних і зв'язку безпілотників.

Ознайомився з можливимим методами безпеки БПЛА, а також методи запобігання та рішення, пов'язані з безпекою зв'язку та мереж БПЛА, які є важливими для збройних сил і рятувальних операцій; Також після ознайомлення було розроблено рекомендації щодо підвищення безпеки безпілотників. Були застосовані види та методи застосування криптографічного алгоритму семитричного блочного шифрування та асемитричного шифрування. Під час виконання цієї роботи було проведено аналіз ефективності та надійності кожного методу шифрування та зазначили їхні переваги та певні недоліки. Зрівнюючи методи які були використані, на мою думку більш ефективним є AES та ECC. Хоча у результаті аналізу було виявлено, що кожен криптографічний алгоритм має як переваги, так і недоліки. Не існує одного криптоалгоритму, який може вирішити всі проблеми конфіденційності зв'язку БПЛА кожен може вибрати різний метод, який йому буде більше підходити враховуючи свої характеристики обладнання.

Також під час роботи ознайомився з частотною модуляцію як одним із вирішенням захисту від РЕБ та антидронів. Цей метод ефективний і водночас користний для розвідних-БПЛА яким потрібно простір для успішної розвідки, наведення координатів для артелерії, збирання інформації про ворого яку дуже важливо не втратити як і БПЛА .

Результати були опробовані на конференції з кіберзахисту[38] радіозв'язку в умовах військового часу та особливості на які слід звертати увагу а саме види кібератак та рекомендації запобігання їхніх впливів. За вдяки цьому дізнався про

більш сучасні методи радіоелектроної боротьби та технології які використовуються на фронті. Зробивши для себе висновок можна зазначити, що частотна модуляція є одним із найбільш ефективним методом захисту від перехоплення зв’язку.

# ПЕРЕЛІК ПОСИЛАНЬ

1. ЗАХИСТ КАНАЛУ ЗВ’ЯЗКУ WI-FI МІЖ ПУЛЬТОМ КЕРУВАННЯ ТА БЕЗПІЛОТНИМ АПАРАТОМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ проф. Власюк Г. Г., доц. Співак В. М., проф. Розоринов Г. М. Україна, Національний технічний університет України "Київський політехнічний інститут"

2. Завадостійка електронна система керування наземним безпілотним транспортом Курпас Д.В., Бевза О.М.

3. GPS-спуфінг- https://armyinform.com.ua/2019/10/27/gps-spufing-vorog-bezpilotnykiv-%E2%84%961/

4. Значення радіоелектронної боротьби у війні: який арсенал РЕБ має РФ- https://fakty.com.ua/ua/ukraine/suspilstvo/20240329-znachennya-radioelektronnoyi-borotby-u-vijni-yakyj-arsenal-reb-maye-rf/

5. Частотна модуляція - https://www.rfcafe.com/references/electrical/frequency-modulation.htm

6. DJI Mavic 3 - https://fakty.com.ua/ua/ukraine/suspilstvo/20230222-dopomagayut-vesty-rozvidku-ta-znyshhuvaty-voroga-osoblyvosti-kopteriv-dji-mavic-3/

7. Кропива- https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%BE%D0%BF%D0%B8%D0%B2%D0%B0_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0)

8. Starlink в Україні: хто може користуватися та як підключитися- https://informator.ua/uk/starlink-v-ukrajini-hto-mozhe-koristuvatisya-ta-yak-pidklyuchitisya

9. Зібрано детальну статистику використання FPV-дронів на полі бою: які можна зробити висновки-https://defence-ua.com/minds_and_ideas/zibrano_detalnu_statistiku_vikoristannja_fpv_droniv_na_poli_boju_jaki_mozhna_zrobiti_visnovki-14298.html

10. Чи можна заглушити FPV дрон?- https://wondertech.ua/ua/blog/chi-mozhna-zaglushiti-fpv-dron

11.Пристрій протидії БПЛА направленої дії Antidrone jammer DJ-04-70 - https://lockers.com.ua/glushilka-dronov-anti-drone-jammer-dw-04-a-dalnost-do-1800-metrov-4-chastoti/

12.Дрони – найдешевший спосіб знищення бійців РФ, Javelin – найдорожчий- https://forbes.ua/war-in-ukraine/droni-naydeshevshiy-sposib-znishchennya-biytsiv-rf-javelin-naydorozhchiy-forbes-porakhuvav-vartist-znishchennya-rosiyskikh-soldativ-ta-tekhniki-11042023-12982

13.Огляд DJI Mavic 3 для України в 2024 році - https://www.bestdrone.com.ua/dji-mavic-3/

14.Офіційний сайт DJI Mavic 3 - https://www.dji.com/global/support/product/mavic-3

15.Битва безпілотників. Навіщо Україні FPV та чи змінить мільйон дронів хід війни - https://www.rbc.ua/rus/news/bitva-bezpilotnikiv-navishcho-ukrayini-fpv-1703172982.html#%D0%BF%D1%80%D0%B5%D0%B8%D0%BC%D1%83%D1%89%D0%B5%D1%82%D1%81%D0%B2%D0%B0%20%D0%B8%20%D0%BD%D0%B5%D0%B4%D0%BE%D1%81%D1%82%D0%B0%D1%82%D0%BA%D0%B8

16.Пічугін М. Ф., Носова Г.Д. Збірник наукових праць ЖВІ НАУ. Випуск 3 — Аналіз тактики застосування підрозділів РЕБ у сучасних війнах та локальних збройних конфліктах. —К., 2010.

17.О. М. Семененко, Р. В. Бойко, Ю. Б. Добровольський, В. Л. Іванов, О. І. Кремешний. Контррадіоелектронна боротьба як складова частина радіоелектронної боротьби в Збройних Силах України // Системи озброєння і військова техніка. —2016. —Вип. 46. —С. 141-145

18.Про основні засади забезпечення кібербезпеки України - https://zakon.rada.gov.ua/laws/show/2163-19#Text

19.Що таке спуфінг і як запобігти атаці? -https://cybercalm.org/novyny/shho-take-spufing-i-yak-zapobigty-atatsi-porady/

20.Спуфінг- https://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D1%83%D1%84%D1%96%D0%BD%D0%B3

21. Spoofing MAC-адреси- https://en.wikipedia.org/wiki/MAC_spoofing

22. IP spoofing- https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

23. Аналізатор трафіку - https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%82%D0%BE%D1%80_%D1%82%D1%80%D0%B0%D1%84%D1%96%D0%BA%D1%83

24. Що таке VPN і як це працює? - https://surfshark.com/uk/learn/what-is-vpn

25. Advanced Encryption Standard - https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard

26. Василенко С.В. (2016). Системи радіозв'язку з псевдовипадковим переналаштуванням робочої частоти / Електронне наукове фахове видання-журнал Проблеми телекомунікацій. № 1 (18). С. 91-100.

27. Дзяйло В.В. (2017) Покращення характеристик каналів радіозв'язку з частотним мультиплексуванням: автореф. магістра: Тернопільський національний технічний університет імені Івана Пулюя. Тернопіль: ТНТУ, 7 С.

28. Бігун Н., Грозовський Р. (2019). Оцінка розвідзахищеності системи зв'язку, побудованої на сучасних засобах радіозв'язку: Сучасні інформаційні технології в галузі безпеки та оборони, № 1(34), С. 53-58 - https://doi.org/10.33099/2311-7249/2019-34-1-53-58.

29. RSA - https://uk.wikipedia.org/wiki/RSA

30. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? - https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/

31. Еліптична криптографія - https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

32. Інженерний курс «Народний FPV» - https://apps.prometheus.org.ua/learning/course/course-v1:Prometheus+FPV101+2024_T1/home

33. Виносна антена для керування дронами та БПЛА з укриття Profi long range - https://camsecurity.com.ua/ua/vynosnaya-antenna-dlya-upravleniya-dronami-i-bpla-iz-ukrytiya-profi-long-range.html

34. Serpent- https://uk.wikipedia.org/wiki/Serpent_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F)

35. РЕБ. Що це і як засоби радіоелектронної боротьби протидіють ворожим ракетам - https://mind.ua/publications/20269499-reb-shcho-ce-i-yak-zasobi-radioelektronnoyi-borotbi-protidiyut-vorozhim-raketam

36. Що таке спуфінг і як запобігти атаці? - https://cybercalm.org/novyny/shho-take-spufing-i-yak-zapobigty-atatsi-porady/

37. Чому підробка GPS є проблемою (і що з цим робити) - https://nextnav.com/gps-spoofing/

38. Стаднік Б. -Захист каналу зв’язку безпілотних літальних апаратів. Матеріали конференції Суспільство та держава в умовах воєнного стану:виклики та перспективи, 27 квітня 2023 рік Одеса