НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроники та телекомунікацій

Кафедра аеронавігаційних систем

До захисту допущено:

Завідувач кафедри

_____

«___»_____20__р.

Дипломна робота

на здобуття ступеня магістра

за освітньо-професійною програмою «Безпілотні авіаційні комплекси»

спеціальності 272 «Авіаційний транспорт»

на тему: «Оцінка ефективності застосування систем боротьби із БПС»

Виконав:

студент, групи 266-М

Батіщев Данило Володимирович _____

Керівник:

Завідувач кафедри

Ларін Віталій Юрійович _____

Київ – 2023 року

Календарний план

№	Назва етапів виконання дипломного проєкту	Термін виконання етапів проєкту	Примітка
1	Огляд існуючих рішень	10.03.23 – 20.03.23	
2	Пошук даних для машинного навчання	20.03.23 – 03.04.23	
3	Тренування моделі комп’ютерного зору	03.04.23 – 12.04.23	
4	Розробка концептуального додатку, що використовує натренеровану модель	13.04.23 – 25.04.23	
5	Перевірка роботи моделі та її коректування	25.04.23 – 29.04.23	
6	Проектування системи	29.04.23 – 05.04.23	
7	Підбір компонентів системи	09.05.23 – 10.05.23	
8	Розроблення схем та діаграм	10.05.23 – 21.05.23	
9	Оформлення текстової документації	21.05.23 – 08.06.23	

Студент Батіщев Д. В.

Керівник Лпрін В. Ю.

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Оцінка ефективності застосування систем боротьби із БПС».

Мета дипломної роботи – оцінка ефективності систем боротьби з БПС, огляд існуючих рішень, розробка системи боротьби з БПС на базі існуючих рішень.

Об'єкт дослідження – системи виявленя та нейтралізації БПС.

Предмет дослідження – моделювання процесу розробки системи протидії БПС. Дослідження, проведене в рамках цього проекту, спрямоване на вивчення та оцінки методів виявлення та протидії БПС. Використання радіоелектронної боротьби та аналізу зображень є ключовими компонентами системи боротьби із БПС. Особлива увага приділяється використанню машинного навчання для розпізнавання БПС на зображеннях та подальших заходів з їх нейтралізації.

Методи дослідження – теоретичні методи, методи математичного та комп'ютерного моделювання, математичні обчислення.

Актуальність – оцінка ефективності існуючих рішень та розроблена система протидії БПС дасть змогу захистити конкретний простір від небажанного втручання та зпобігти потенційні загрози, особливо в контексті безпеки, конфіденційності та правопорядку

Ключові слова: ОЦІНКА ЕФЕКТИВНОСТІ, СИСТЕМИ БОРОТЬБИ ІЗ БПС, КОМП'ЮТЕРНИЙ ЗІР, НЕЙРОМЕРЕЖІ, РОЗПІЗНОВАННЯ ЗОБРАЖЕНЬ, БПЛА, РАДІОЕЛЕКТРОНА БОРОТЬБА, СИГНАЛ, МЕТОД ВИЯВЛЕННЯ, ПОМИЛКОВА ТРИВОГА, АДПТАЦІЯ, ОБРОБКА СИГНАЛІВ, РАДІОЛОКАЦІЙНА СТАНЦІЯ

АРКУШ ЗАУВАЖЕНЬ

ЗМІСТ

Перелік умовних скорочень…….....6

ВСТУП……....7

1. Задачі і класифікація БПЛА…….....10

1.1 Історія виникнення БПЛА……..11

1.2 Класифікація БПЛА……14

1.3 Будова БПЛА…….....16

2. ОГЛЯД ТА АНАЛІЗ ІСНУЮЧИХ СИСТЕМ БОРОТЬБИ З БПС ….…….18

2.1 Профілактичні заходи…….....21

2.2 Виявлення Бпс....…….....……..25

2.2.1 Акустичі датчики і системи…….....…….25

2.2.2 Радарні системи……..……31

2.2.3 Оптичні системи.....……..…34

2.2.4 Радіочастотні системи…….……...35

2.2.5 Мультисенсорні системи……..…….…….38

2.3 Нейтралізація БПС…….....38

2.3.1. Радіоподавлення та перехоплення управління……..……..39

2.3.1.1 Радіочастотні перешкоди…….....39

2.3.1.2 Радіоподавлення GNSS…..……...40

2.3.1.3 Спуфінг……...…….41

2.3.1.4 Нейтралізатори, що використовують атаки на основі протоколу та атаки повторення……..…….....41

2.3.1.5 Потужні електромагніти та лазери……..42

2.3.2 БПЛА перехоплювачі……...43

2.3.3 Зброя стрілецька та інша…….....43

3. Існуючі розробки.....…….....45

3.1 OpenWorks Engineering .....…….....45

3.2.REX-1.....….....…….....46

3.3. Aerosnare.....…….....47

3.4. SkyFence.....48
3.5.Kaspersky Antidrone.....48
3.6.Anduril Roadrunner.....49
3.7. DroneShield-DroneSentinel ...49
Висновки до розділу 2-3.....50
4.1 Функціональний Розбір системи.....51
4.2 Опис системи.....51
4.3 Опис алгоритму роботи системи.....52
4.3.1 Реалізація виявлення БПС.....53
4.3.1.1 Локатор.....54
4.3.1.2 Магнетрон.....55
4.3.1.3 Антена.....55
4.3.1.4 Дуплексер.....56
4.3.1.5 Приймач.....57
4.3.2. Комп’ютерний зір.....57
4.3.3 Тренування моделі.....60
4.4 Ралізація нейтралізації БПС.....64
ВИСНОВКИ.....65
Перелік Посилань.....68

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЛА – літальний апарат

БПЛА – безпілотний літальний апарат

БД – база даних

РЕП - радіоелектронного придушення

РЛС - радіолокаційна станція

ЧМБС - частотно - модульований безперервний сигнал

CFAR - постійна ймовірність фіктивних тривіг

STFT - віконне перетворення Фур'є

CW - сигнали безперервної хвилі

ППО – протиповітряна оборона

БАС - Безпілотна Авіаційна Система

БПАК - Безпілотний Повітряний Комплекс

GPS - Глобальна Позиційна Система

БПС - Безпілотні Повітряні Системи

РЕБ - Радіоелектронна Боротьба

ВСТУП

БПС поступово стають неодмінною складовою різних сфер життя, розширюючи можливості технологічного прогресу. У сільському господарстві вони впроваджуються для опилення полів, забезпечуючи нові стандарти ефективності та екологічної безпеки. БПС виявляються важливими в доставці медикаментів
та гуманітарних вантажів, а їх використання в моніторингу інфраструктури,
такої як лінії електропередач та трубопроводів, сприяє підвищенню рівня безпеки та ефективності.Виробники безпілотних систем (БПС) постійно вдосконалюють свої моделі, що створює можливість практично непомітно збирати інформацію про різноманітні об'єкти та суб'єкти, які можуть бути об'єктом цікавості. Ці об'єкти можуть включати людей, групи людей чи території, пов'язані з вашою компанією. Водночас із зростанням можливостей безпілотних систем для корисних застосувань, виникає актуальна та серйозна проблема - використання БПС у неналежних цілях.

Ця проблема стала пріоритетною у всьому світі, оскільки БПС можуть використовуватися для негативних цілей, таких як порушення приватності, шпигунство, атаки на об'єкти чи території. Можливість БПС непомітно та ефективно збирати інформацію може породжувати загрози для безпеки та конфіденційності.

Органи влади та компанії, що спеціалізуються на розробці та впровадженні технологій безпілотних систем, активно працюють над розробкою та вдосконаленням систем ідентифікації, виявлення та нейтралізації потенційно небезпечних БПС. Виробники безпілотних систем також взяли на себе зобов'язання розвивати технології, які допомагатимуть у виявленні та запобіганні зловживанням. Це наголошує важливість збалансованого регулювання та використання технологій БПС для забезпечення безпеки, захисту приватності та уникнення негативних наслідків їх використання у сферах, що вимагають високого рівня відповідальності та обережності.. БПС використовуються у військових операціях, та незаконних активностях (терористична діяльність, розвідка та кража таємної інформації, вандалізм, створення першкод для воздушного простору, логістика незаконних грузів, шпигунство) перетворюючись на загрозу для безпеки та приватності.

У зв'язку з цим виникає важлива необхідність розробки ефективних

методів протидії неправомірному використанню БПС.

Системи протидії:

1. **Акустичні системи:** Використовуються для виявлення та локалізації БПС за звуковими сигналами.
2. **Лазерні системи:** Використовуються для впливу на оптичні системи БПС та заваджання їхній роботі.
3. **Мікрохвильові системи:** Ефективні для впливу на електроніку БПС, перешкоджаючи їхньому зв'язку та управлінню.
4. **Системи із снарядами:** Використовуються для фізичного знищення або вимикання БПС за допомогою спеціалізованих проектілів.
5. **Системи РЕБ (Радіоелектронна боротьба):** Використовуються для блокування сигналів управління та передачі даних БПС.
6. **Системи перехоплення управління:** Спрямовані на перехоплення контролю над БПС та його управління.

Нейромережі грають ключову роль у виявленні БПС завдяки своїм унікальним можливостям у глибокому аналізі та обробці великих обсягів даних. Ось декілька способів, які нейромережі сприяють виявленню БПС:

Розпізнавання образів:

Нейромережі, зокрема засновані на архітектурі глибокого навчання, можуть бути навчені розпізнавати характеристики та шаблони, що властиві БПС. Вони аналізують вхідні дані, такі як зображення чи відеопотік, і автоматично визначають аномалії, що можуть вказувати на присутність БПС.

Аналіз поведінки:

Нейромережі можуть вивчати типові патерни поведінки об'єктів у визначеному просторі, наприклад, у небі. Вони можуть виявляти незвичайні або відхилені рухи, які можуть свідчити про наявність БПС.

Аналіз сигналів:
Нейромережі можуть бути використані для обробки та аналізу сигналів, які видають БПС. Наприклад, вони можуть розпізнавати унікальні радіосигнали, які використовуються для керування та зв'язку з дронами.
Інтеграція з сенсорами:
Нейромережі можуть об'єднувати інформацію з різних джерел, таких як радари, камери, акустичні сенсори та інші, для створення комплексного зображення навколишнього середовища. Це дозволяє виявляти та відслідковувати БПС у реальному часі.
Автоматизоване навчання:
Системи навчання нейромереж можуть автоматично адаптуватися до нових типів БПС та їх характеристик, що робить їх ефективними у вирішенні постійно змінюючихся загроз.
Динамічне виявлення аномалій:
Нейромережі можуть працювати у режимі реального часу та виявляти аномалії у поведінці або зовнішніх сигналах, що можуть вказувати на незаконне чи небезпечне використання БПС.
Використання нейромереж для виявлення БПС дозволяє автоматизувати та покращити ефективність систем безпеки, забезпечуючи реакцію в реальному часі на потенційні загрози.
Існуючі виклики у вигляді високої вартості та можливої небезпеки для людей, які знаходяться поблизу, залишають актуальними питання розвитку та впровадження таких систем протидії. Ставлю задачу дослідити ефективність кожної системи, зробити висновок та вдосканалити існуючу систему.

1. ЗАДАЧИ І КЛАСИФІКАЦІЯ БПЛА.

1.1 Історія виникнення БПЛА

Поняття "безпілотні літальні апарати" може бути відтворене аж з 1849 року, коли Австрія використовувала безпілотні повітряні кулі, напхані вибухівкою, під час нападу на Венецію. Австрійські війська, облегшуючи місто, запустили близько 200 таких піонерських аеростатів як зображено на рис 1.1, кожен із яких перевозив 24-30 фунтів (11-14 кг) бомб. Ця епізодична ініціатива, хоч і не дуже успішна, відзначає початок військового застосування безпілотних систем. Схоже, що вже тоді військові стратеги думали про можливості використання безпілотних апаратів, навіть якщо ці технології значно відрізнялися від сучасних. Використання аеростатів насправді не

відповідає сучасному визначенню БПЛА, проте це історичне відстеження підкреслює еволюцію військових дронів.

Іншим прикладом є розгляд ранньої конфігурації квадрокоптера у 1907 році, як Жак і Луї Бреге спільно з професором Шарлем Ріше створили гіроплан, передвісник гвинтокрила. Незважаючи на обмежену висоту польоту та нестабільність, цей експеримент дав початок дослідженням технологій квадрокоптерів.

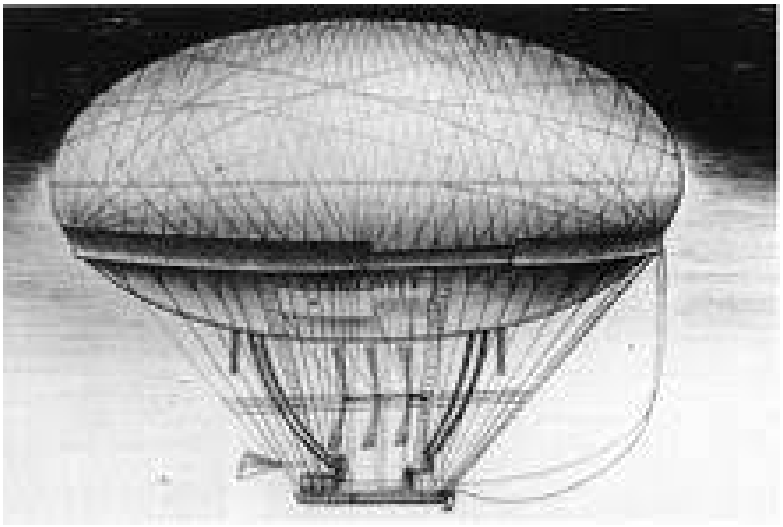


Рис. 1.1-перші БПС

Сучасні комерційні БПС, часто у формі квадрокоптерів, суттєво відрізняються від їхніх попередників. Технологічний розвиток дозволяє створювати надійні та маневрені системи, здатні виконувати різноманітні завдання.

Такий історичний нарис використання безпілотних технологій свідчить про поступовий прогрес у галузі військового застосування та цивільного використання дронів, що залишає відкритими безліч можливостей для майбутніх технологічних інновацій та розвитку.

1.2 Класифікація БПЛА

На поточному етапі розвитку безпілотних літальних апаратів (БПЛА) їх призначення охоплює широкий спектр завдань: спостереження, транспортування вантажів, ретрансляція даних та інші, які вони виконують як за дистанційного управління оператором, так і в режимі автономної дії за заздалегідь програмованою маршрутною схемою.

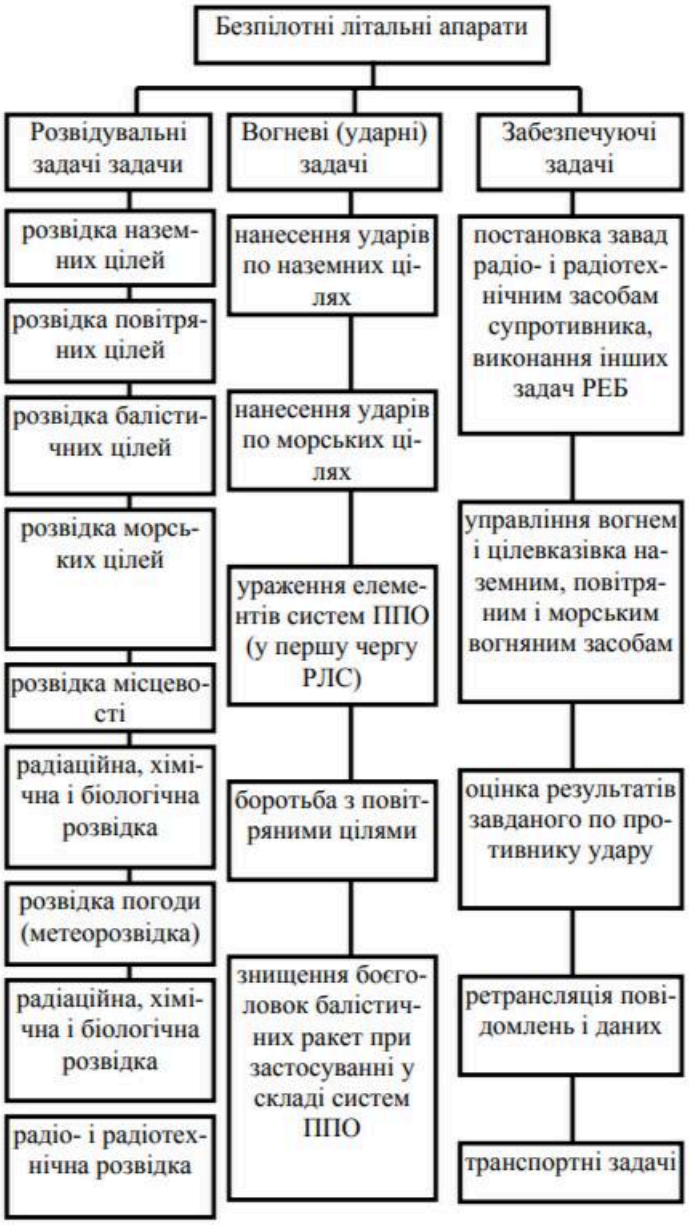
Приблизно в період з 2005 по 2010 роки досягнення в електроніці призвели до виробництва бюджетних контролерів польоту, акселерометрів (IMU), глобальної системи позиціонування та камер. Це призвело до зростання популярності конфігурації квадрокоптера для невеликих БПЛА,

завдяки їхнім компактним розмірам і високій маневреності. Квадрокоптери стали практичними для використання як у приміщеннях, так і на відкритому повітрі.

Для малих БПЛА квадрокоптери виявилися вигідними з точки зору ефективності і тривалих експлуатаційних характеристик порівняно з традиційними вертольотами, завдяки їхній простоті у будові. Менші лопаті роторів також зменшують кінетичну енергію, зменшуючи можливість нанесення шкоди. Захисні кожухи на роторах додатково зменшують ризик пошкодження. Однак при збільшенні розмірів квадрокоптери зі стаціонарними лопатями мають недоліки порівняно з традиційними вертольотами, так як збільшення розміру лопаті збільшує їх імпульс, що впливає на контроль.

З появою середніх і малих БПЛА виникла актуальна проблема протидії їх неправомірному використанню в обмежених зонах. Від середини 2000-х років стали з'являтися повідомлення про використання малих БПЛА вблизь аеропортів, а з 2010-х - про їхнє застосування для незаконного спостереження, транспортування заборонених вантажів і військових операцій. Це призвело до активного наукового дослідження в галузі протидії БПЛА.

БПЛА поділяються за призначенням на наукові та прикладні, а також за типом управління: автоматичні, дистанційно пілотовані і дистанційно керовані. У напрямку зльоту їх класифікують як горизонтальні, вертикальні і змішані (конвертоплани). Враховуючи тип літального апарату, вони бувають літакові, вертолітні і змішані (конвертоплани).



Зараз проблематика протидії БПЛА активно досліджується, і науковці розвивають методи захисту від їх неправомірного застосування, зокрема за допомогою систем радіоелектронного придушення та лазерних технологій. Цей напрямок досліджень стає все більш актуальним і сприяє формуванню заходів для захисту об'єктів, таких як аеропорти та електростанції, від можливих загроз з боку БПЛА. Класифікація БПЛА за їхніми основними характеристиками поділяє їх на малорозмірні та середні і великі. Ця поділка враховує їх розміри та функціональні можливості, що дозволяє ефективно використовувати ці технології в різних областях. Задачі БПЛА зображено на схемі 1.2

Схема 1.2 - задачі БПЛА

1.2.1. Багатороторні дрони.

Багатороторні дрони, також відомі як гвинтокрилі, є найбільш широко використовуваним типом

дронів для рекреаційного та професійного 12 використання. Їх невеликий розмір і чудове керування роблять багатороторні дрони найкращим вибором для аерофотозйомки. На рис. 1.3 зображено багатороторний дрон.

Рис. 1.3. Зовнішній вигляд багатороторного дрону.

Пропонуючи велику універсальність, вони дозволяють встановлювати всі типи камер для виконання різних завдань. Це безпілотники, які можуть легко зависати та злітати вертикально, що також додає більше гнучкості . Однак найбільший недолік багатороторних дронів зазвичай пов’язаний з автономністю польоту, яку вони пропонують. Додавання додаткових роторів ускладнює керування дроном. Усі ці рухомі частини також споживають додаткову енергію, розряджаючи акумулятор швидше. Більшість багатороторних дронів мають час польоту менше години. Якщо ми хочемо виконувати певні завдання, які займають багато часу, нам потрібно мати кілька акумуляторів, щоб їх замінити. Це також означає додаткові витрати.

1.2.2. Безпілотники з нерухомим крилом

Безпілотники з нерухомим крилом здатні використовувати повітря та генерувати сили, які дозволяють їм залишатися в повітрі, використовуючи переваги своєї аеродинаміки. Вони подібні за дизайном або естетикою до радіокерованих літальних апаратів і часто використовуються для картографування великих територій завдяки своїй великій автономності. Вони використовують переваги своєї аеродинаміки та дизайну, щоб утримувати їх на 13 плаву, а це означає, що вони мають більшу витривалість і швидкість польоту. На рис. 1.4 зображено безпілотник з нерухомим крилом

Рис. 1.4. Зовнішній вигляд безпілотника з нерухомим крилом.

Недоліком безпілотників з нерухомим крилом є те, що вони, як правило, дорожчі порівняно з багатороторними дронами. Їм потрібен великий вільний простір для зльоту та посадки, як і літакам. Деякі більші моделі також вимагають спеціалізованого наземного обладнання, щоб допомогти їм злетіти та приземлитися. Крім того, дрони з нерухомим крилом можуть літати лише вперед, тому вони не пропонують такої ж маневреності, як багатороторні дрони.

1.1.3. Одноторні гелікоптерні дрони

Потужні та довговічні одноторні безпілотні літальні апарати за своєю конструкцією та дизайном схожі на справжні вертольоти, лише з одним ротором, який забезпечує потужність, а також хвостом для контролю напрямку та стабільності. Поєднуючи в собі переваги крихітних багатороторних дронів і одноторних дронів, вони краще підходять для перевезення більшого корисного навантаження та літають ефективніше, ніж багатороторні. У одноторних апаратах зазвичай використовуються газові двигуни, а не батареї, що значно збільшує час їх польоту. На рис. 1.5 зображено гелікоптерний дрон.

Рис. 1.5. Зовнішній вигляд гелікоптерного дрону.

Однак ці дрони, як правило, більші та складніші за інші типи БПЛА. Це означає, що вони дорожчі та важчі в експлуатації, а їхні великі леза можуть зробити їх більш небезпечними.

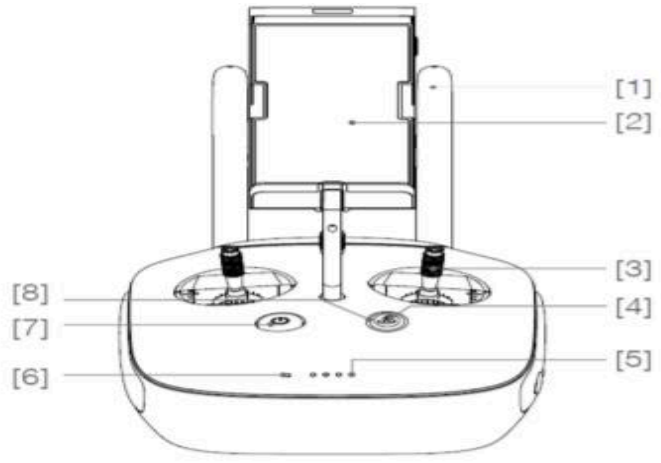
1.1.4. Гібридні дрони VTOL з нерухомим крилом

Гібридні безпілотні літальні апарати VTOL з нерухомим крилом, як остання технологія безпілотних літальних апаратів, відносяться до літальних апаратів з нерухомим крилом, які були модифіковані для вертикального зльоту та посадки. Вони поєднують дальність і час польоту БПЛА з нерухомим крилом із можливістю вертикального зльоту гвинтокрилих пристроїв, усуваючи недоліки БПЛА з нерухомим крилом, які потребують великого простору для зльоту та посадки. Вони призначені для картографування, спостереження, сільського господарства та рятувальних операцій. На рис 1.6 зображено гібридний безпілотник.

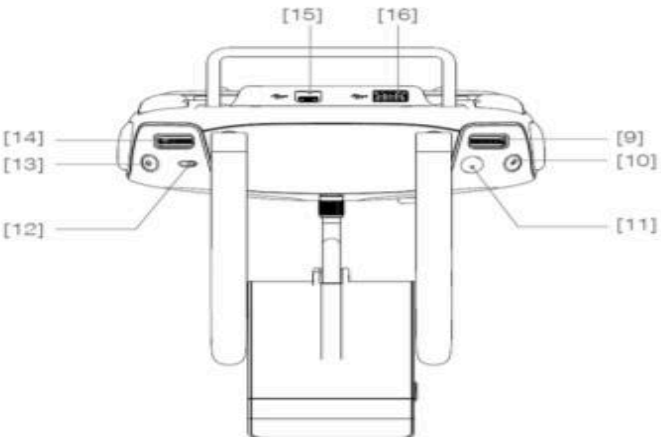
Рис. 1.6. Зовнішній вигляд гібридного безпілотника

1.3 Будова БПЛА

Сучасні безпілотні літальні апарати (БПЛА) складаються з комплексу технічних систем, які забезпечують їхню навігацію, управління, збір і передачу даних, а також виконання конкретних завдань залежно від їхнього призначення. На рисунках 1.7 та 1.8 зображені основні компоненти пульта дистанційного керування та дрону.

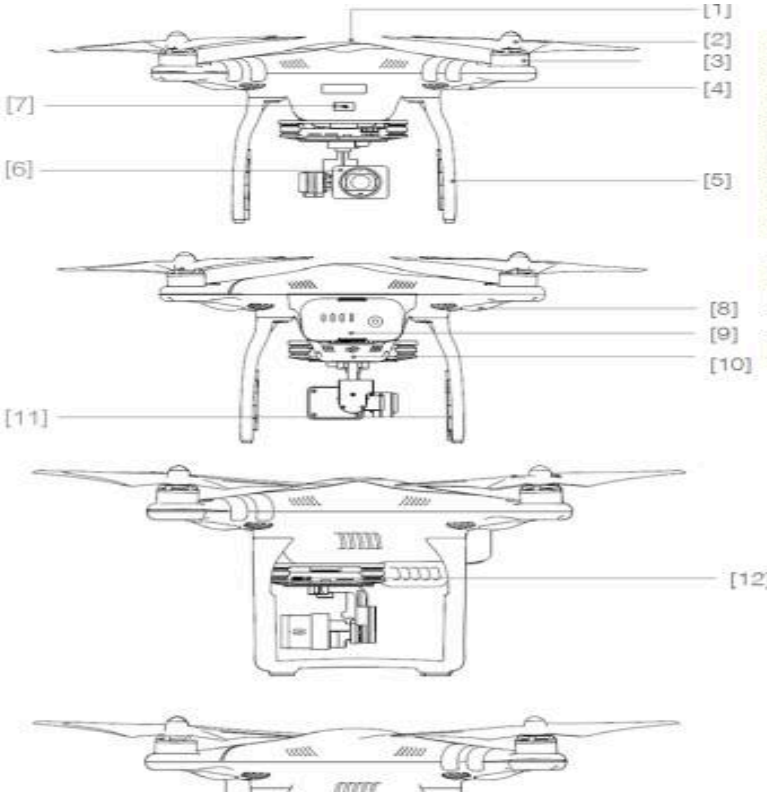


[1] – антени для керування коптером та прийому відеосигналу
[2] – тримач для мобільного пристрою
[3] – ручка керування орієнтацією та рухом коптера
[4] – кнопка RTH повернення додому
[5] – LED рівня зарядки акумулятора
[6] – статус LED відображає стан пульта ДУ
[7] – кнопка живлення
[8] – RTH LED. LED кільце навколо кнопки RTH показує RTH статус



[9] – диск налаштування камери
[10] – кнопка відтворення зображень чи відео
[11] – кнопка спуску затвора
[12] – перемикач режимів польоту для перемикання між режимами P, A і F
[13] – кнопка запису відео
[14] – диск підвісу використовується для нахилу підвісу
[15] – порт Micro-USB для підключення картрідера SD-карти для оновлення прошивки
[16] – порт USB для підключення до мобільного пристрою або для оновлення прошивки

Рис. 1.7 — комплектуючі пульта дистанційного керування



[1] – GPS
[2] – пропелер
[3] – двигун
[4] – передній LED- індикатор
[5] – шасі
[6] – підвіс і камера
[7] – порт Micro-USB коптера
[8] – статус індикатор коптера
[9] – акумуляторна батарея
[10] – сенсор візуального позиціонування
[11] – антени
[12] – слот для Micro-SD
[13] – порт Micro-USB камери
[14] – кнопка прив'язки

Рис. 1.8 — комплектуючі дрона

Ось основні аспекти роботи сучасних БПЛА з технічної точки зору:

Система Навігації:

Глобальна Система Позиціонування (GPS): Використовує сигнали супутників для визначення точного місцезнаходження.

Інерційні вимірювальні пристрої (IMU): Детектують і вимірюють зміни в русі і орієнтації БПЛА.

Барометри і сенсори висоти: Використовуються для вимірювання висоти.

Система Управління та Автопілот:

Автопілот: Комп'ютерна система, що автоматично керує польотом БПЛА, виконуючи задані команди та маршрути.

Контроль стабільності: Забезпечує підтримання стабільності та керованість під час польоту.

Системи Спостереження та Сенсори:

Камери: Використовуються для збору візуальної інформації.

Радари: Дозволяють виявляти об'єкти на значних відстанях та в умовах обмеженої видимості.

Інфрачервоні (ІЧ) та Ультразвукові сенсори: Допомагають виявляти та взаємодіяти з об'єктами на основі теплового випромінювання чи звуку.

Система Зв'язку:

Радіо та супутникові засоби зв'язку: Забезпечують передачу даних між БПЛА та наземним пунктом управління.

Безпека та Захист:

Антивірусне програмне забезпечення: Захищає від потенційних загроз та вторгнень в систему управління.

Системи Уникнення Зіткнень: Допомагають уникати зіткнень з іншими об'єктами, включаючи інші літальні апарати.

Система Живлення:

Акумулятори або пальне: Забезпечують енергію для роботи всіх систем.

Система Керування Бортовою Інформацією:

Системи збору, обробки та зберігання даних: Забезпечують ефективну роботу та аналіз зібраних інформаційних потоків.

Автономні Технології:Штучний Інтелект та Машинне Навчання: Забезпечують здатність БПЛА приймати рішення на основі аналізу даних та ситуації.

1.4 Метод роботи сучасних БПЛА

Метод роботи безпілотних літальних апаратів (БПЛА) визначається їхніми характеристиками, призначенням та завданнями, які вони виконують. Однак існують загальні принципи та етапи роботи БПЛА, які можна узагальнити:

Планування місії:

Визначення конкретних завдань, які повинен виконати БПЛА.

Встановлення параметрів місії, таких як область дії, тривалість польоту, висота польоту тощо.

Розробка маршруту та точок інтересу.

Запуск і підготовка до польоту:

Перевірка систем та обладнання на наявність несправностей.

Завантаження програмного забезпечення та необхідних даних.

Перевірка і калібрування сенсорів та систем управління.

Зліт і виконання місії:

Автоматичний чи дистанційно керований зліт БПЛА.

Виконання запланованої місії, включаючи збір і передачу даних.

Навігація та управління:

Автоматичне управління рухом та навігацією.

Виправлення траєкторії польоту з урахуванням змін у середовищі чи задач місії.

Сенсорний збір та обробка інформації:

Використання різноманітних сенсорів (камер, радарів, ІЧ-систем, тощо) для отримання даних.

Обробка та аналіз інформації для вирішення поставлених завдань.

Збір та передача даних:

Збір даних про об'єкти чи області інтересу.

Передача даних на наземні станції або інші пункти призначення.

Автономність та прийняття рішень:

Використання вбудованих алгоритмів та систем штучного інтелекту для прийняття рішень.

Автоматична або дистанційно керована реакція на зміни у середовищі чи поблизу об'єктах.

Повернення та посадка:

Повернення до точки старту або іншого призначення.

Автоматична чи дистанційно керована посадка.

Аналіз та звітність:

Аналіз отриманих даних та результатів місії.

Підготовка звітів чи іншої інформації для користувача.

Метод роботи БПЛА може суттєво відрізнятися в залежності від класу, призначення та характеристик конкретного літального апарата.

На рисунку 1.9 зображена типова траєторія польоту БПЛА

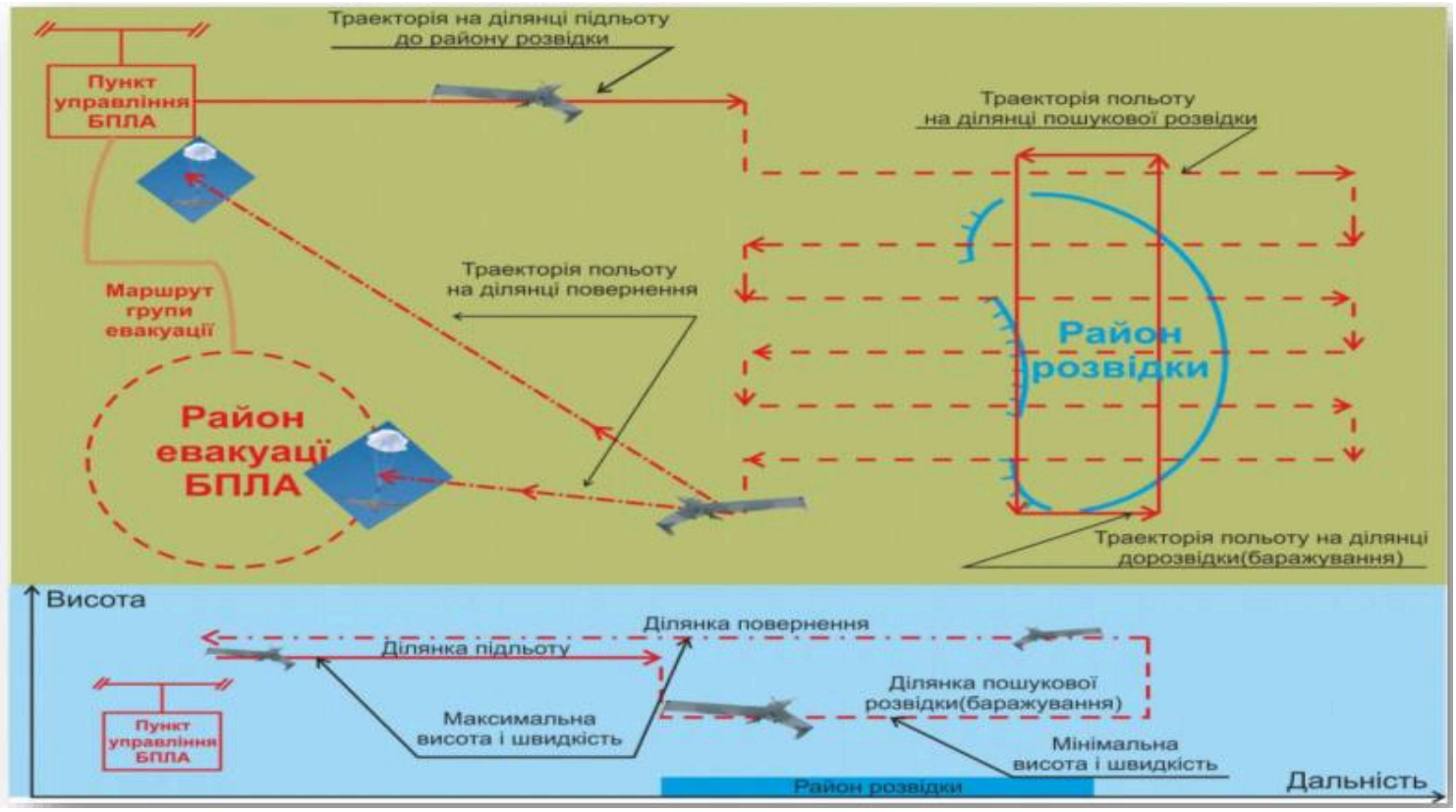


Рис. 1.9 — типова траєкторія польоту БПЛА

2. ОГЛЯД ТА АНАЛІЗ ІСНУЮЧИХ СИСТЕМ БОРОТЬБИ З БПС

Сфера застосування БПС сьогодні значно розширилася. Дрони часто з'являються в аеропортах, у пристроях безпеки (пунктах затримання, військових заводах) і також використовуються для відстеження людей. Багато хто оцінив переваги повітряного розвідування і активно користується ним, порушуючи особисте життя та роблячи неможливим займатися своїми справами.

Виробники постійно модернізують моделі, що дозволяє практично непомітно збирати інформацію про об'єкт, який нас цікавить, будь то людина, група людей або територія вашої компанії. Проблема використання дронів у неналежних цілях є пріоритетною у всьому світі.

Чим дорожчий пристрій, тим складніше йому протистояти, що робить завдання боротьби з дронами

нерівною боротьбою, оскільки без спеціального обладнання звичайній людині немає чого висунути проти дрона.Звідси виникає необхідність розробки послідовних стандартів і правил, які, з одного боку, забезпечать простір для розвитку технологій БПЛА та їх широкого використання в економіці, а з іншого боку, забезпечать безпеку громадян і інфраструктури, яка має ключове значення для безпеки держави. Виробники систем протидії БПЛА постійно шукають найбільш ефективні інструменти для вирішення цієї проблеми. Поєднання цих факторів послужило толчком до розробки систем протидії безпілотним літальним апаратам.

Після того, як військові проаналізували небезпечну ситуацію та беззахисність перед такою загрозою, для них розробили обладнання для запобігання цим вторгненням, як засоби придушення безпілотних літальних апаратів.Так само, як і з самими дронами, засоби боротьби з військового середовища швидко розповсюджувалися у цивільний сектор. Компанії, які стали власниками глушників для дронів, оцінили ці пристрої, оскільки вони отримали ефективну зброю, яка може приглушити дрон, але не лише придушити сигнал, але і виявити оператора, який ним управляє. Крім того, були розроблені спеціальні промислові системи на основі радарів, які виявляють наближаючийся дрон задовго до того, як він увійде в захищену зону, і швидко реагують на загрозу.Також не обійшлося без захисту від квадрокоптерів для звичайних людей: були розроблені невеликі портативні глушники для дронів, які можна було брати з собою. Такі глушники працюють від акумулятора протягом кількох годин. На схемі 2.1 розглянуто методи захисту від дронів. Отже, власник глушника дронів може захистити свої інтереси в ситуації, коли його конфіденційність перебуває під загрозою.

Проте наразі не існує такої системи, яка могла б захистити на сто відсотків від БПЛА, оскільки кожен об'єкт має різні характеристики, інфраструктуру та розташування на місцевості. Тому для забезпечення максимального захисту від БПЛА необхідно застосовувати відповідне рішення в залежності від розміру об'єкта та різних систем політики безпеки:

Профілактичні:

1. Введення в законодавство обмежень використання БПЛА.
2. Розміщення попереджувальних щитів про обмеження використання БПЛА.
3. Введення в програмне забезпечення геолокаційних даних про заборону польоту над певними зонами.

Виявлення БПЛА:

1. Акустичні датчики і системи.
2. Радарні системи.
3. Оптичні системи.
4. Радіочастотні системи.
5. Мультисенсорні системи.

Нейтралізація БПЛА:

1. Радіопідавлення та перехоплення управління.
2. БПЛА перехоплювачі.
3. Зброя стрілецька та інша.

Схема 2.1 — методи захисту від дронів.

Порівняння методів виявлення БПЛА представлено у табл. 2.2

Метод виявлення	Принцип роботи датчика	Гранична дальність, м	Фактори, які впливають на якість роботи	Особливості функціонування	Робота в режимі радіомовчання
Акустичний	Використання звукових хвиль для виявлення	100-1000	Шум зовнішнього середовища	Так	Так
Оптичний	Використання світла та обробка оптичних зображень	500-600	Освітлення, погодні умови (туман, опади)	Потрібна пряма видимість	Так
Інфрачервоний	Використання інфрачервоного випромінювання	500-600	Погодні умови (туман, опади)	Потрібна пряма видимість	Так
Лідар	Використання лазерних променів для вимірювання відстані	1000	Погодні умови (туман, опади)	Пряма видимість необов'язкова	Ні
Радіолокаційний	Використання радіохвиль для визначення положення	>2000	Розмір БПЛА (ефективна площа розсіювання)	Пряма видимість необов'язкова	Ні
Радіочастотний	Використання радіохвиль для зчитування передавача на БПЛА	2000	Потужність випромінювання передавача на БПЛА	БПЛА, що керується дистанційно	Так

табл. 2.2

2.1.Профілактичні заходи

Безпілотні літальні апарати або повітряні судна (БПЛА або БПС) входять у трійку найважливіших потреб для українських сил безпеки та сил оборони, зокрема Збройних Сил, поліції, Нацгвардії, Служби безпеки й Держприкордонслужби. Саме безпілотники технологічно підсилюють наших військових на фронті та дають змогу отримати перевагу над ворогом. Основна роль БПЛА полягає в забезпеченні розвідки, а також знищення живої сили противника, їхніх автомобілів, бронетехніки, укриттів і вогневих точок. Крім того, вони мають різноманітне застосування, що включає цілодобове патрулювання, доставку вантажів до важкодоступних районів, охорону об’єктів, коригування вогню артилерії, аерофоторозвідки, отримання актуальних просторових даних, радіоелектронної розвідки та для сигналів зв’язку. Ці БПЛА здатні надавати цінну інформацію та підтримку для ефективного планування та виконання операцій силових відомств. З 24 лютого 2022

року захист повітряного простору став першочерговим завданням для ЗСУ, тому використання безпілотних літальних апаратів та легких літаків у приватних цілях у період воєнного стану заборонено. Рішення щодо можливості використання повітряного простору безпілотними повітряними суднами в конкретній області приймається Генеральним штабом ЗСУ. Наразі, необхідно покращити рівень внутрішньої безпеки в межах країни. Тому пропоную розібратися у законодавчій базі щодо використання безпілотників та відповідальності за порушення повітряного простору.

Законодавчий аспект:

На сьогодні, чинне законодавство щодо визначення, класифікації та використання БПС регулюється Повітряним кодексом України, Положенням про використання повітряного простору України, затверджене постановою КМУ № 954, Авіаційними правилами України «Правила використання повітряного простору України», затверджені наказом Державної авіаційної служби України, Міністерства оборони України № 430/210, Наказом Міністерства оборони України № 661 «Правила виконання польотів безпілотними авіаційними комплексами державної авіації України». У Авіаційних правилах України щодо використання повітряного простору визначено, що «безпілотне повітряне судно» – це повітряне судно, призначене для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюються за допомогою спеціальної станції керування, що розташована поза повітряним судном. Повітряний Кодекс встановлює, що не підлягають реєстрації у Державному реєстрі цивільних повітряних суден України – безпілотні повітряні судна, максимальна злітна вага яких не перевищує 20 кілограмів і які використовуються для розваг та спортивної діяльності. Крім того, в Авіаційних правилах встановлено, що польоти безпілотних ПС масою до 20 кг включно виконуються без подання заявок на використання повітряного простору України (далі- ВПП), без отримання дозволів на нього, без інформування органів управління Повітряних Сил ЗСУ та органів об’єднаної цивільно-військової системи організації повітряного руху України (далі – ОЦВС), органів Державної прикордонної служби України, органів обслуговування повітряного руху (далі – ОПР) та відомчих органів управління повітряним рухом (далі -УПР). Це можливе за умови дотримання переліку вимог, серед низки яких є те, що польоти виконуються без перетинання державного кордону України й поза межами встановлених заборон та обмежень ВПП, крім випадків, установлених Положенням про ВПП. Польоти виконуються не ближче 5 км від зовнішніх меж злітно-посадкових смуг (далі – ЗПС)

аеродромів або не ближче 3 км від зовнішніх меж злітно-посадкової смуги, крім випадків узгодження з експлуатантом ЗПС. Також, польоти виконуються не ближче 500 м від пілотованих ПС й польоти не виконуються над: скупченням людей на відкритому просторі та над місцями щільної забудови, зокрема, об'єктами (зонами), які визначені державними органами та відносно яких здійснюється державна охорона.В інших випадках польоти безпілотного ПС масою до 20 кг включно та усі без винятку польоти безпілотного ПС масою понад 20 кг виконуються у межах спеціально встановлених зон та маршрутів з дотриманням вимог щодо подання заявок на ВПП, отримання дозволів та умов ВПП.Наказом Міністерства оборони України № 661 встановлена наступна класифікація безпілотних літальних апаратів безпілотних авіаційних комплексів (далі – БпЛА БпАК). За класами вони існують: легкі, середні й важкі. Крім того, кожен з цих класів ділиться ще й на підгрупи. За призначенням БпЛА БпАК класифікуються як бойові, розвідувальні, ударні; БпЛА БпАК розвідки та цілевказання й радіоелектронної боротьби. До того ж, існують БпЛА – перехоплювачі ПС та бойові БпЛА БпАК, які можуть мати комбіноване призначення. Існують також й спеціальні БпЛА БпАК – призначені для виконання спеціальних завдань, а також для спостереження та моніторингу об'єктів, території тощо. Крім цього, є класифікація за типом, місцем базування, способом зльоту та посадки й типом системи керування польотом.

Законодавчий аспект:

На сьогодні, чинне законодавство щодо визначення, класифікації та використання БПС регулюється Повітряним кодексом України, Положенням про використання повітряного простору України, затверджене постановою КМУ № 954, Авіаційними правилами України «Правила використання повітряного простору України», затверджені наказом Державної авіаційної служби України, Міністерства оборони України № 430/210, Наказом Міністерства оборони України № 661 «Правила виконання польотів безпілотними авіаційними комплексами державної авіації України». У Авіаційних правилах України щодо використання повітряного простору визначено, що «безпілотне повітряне судно» – це повітряне судно, призначене для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюються за допомогою спеціальної станції керування, що розташована поза повітряним судном. Повітряний Кодекс встановлює, що не підлягають реєстрації у Державному реєстрі цивільних повітряних суден України – безпілотні повітряні судна, максимальна злітна вага яких не перевищує 20 кілограмів і які використовуються для розваг та спортивної діяльності. Крім того, в Авіаційних правилах встановлено, що польоти

безпілотних ПС масою до 20 кг включно виконуються без подання заявок на використання повітряного простору України (далі- ВПП), без отримання дозволів на нього, без інформування органів управління Повітряних Сил ЗСУ та органів об’єднаної цивільно-військової системи організації повітряного руху України (далі – ОЦВС), органів Державної прикордонної служби України, органів обслуговування повітряного руху (далі – ОПР) та відомчих органів управління повітряним рухом (далі -УПР). Це можливе за умови дотримання переліку вимог, серед низки яких є те, що польоти виконуються без перетинання державного кордону України й поза межами встановлених заборон та обмежень ВПП, крім випадків, установлених Положенням про ВПП. Польоти виконуються не ближче 5 км від зовнішніх меж злітно-посадкових смуг (далі – ЗПС) аеродромів або не ближче 3 км від зовнішніх меж злітно-посадкової смуги, крім випадків узгодження з експлуатантом ЗПС. Також, польоти виконуються не ближче 500 м від пілотованих ПС й польоти не виконуються над: скупченням людей на відкритому просторі та над місцями щільної забудови, зокрема, об’єктами (зонами), які визначені державними органами та відносно яких здійснюється державна охорона. В інших випадках польоти безпілотного ПС масою до 20 кг включно та усі без винятку польоти безпілотного ПС масою понад 20 кг виконуються у межах спеціально встановлених зон та маршрутів з дотриманням вимог щодо подання заявок на ВПП, отримання дозволів на нього та інформування органів управління Повітряних Сил ЗСУ, органів ОЦВС, органів Держприкордонслужби, органів ОПР та відомчих органів управління повітряним рухом. Це відноситься до випадків здійснення польотів у ЗПС, контроль за якими здійснюється органами Повітряних Сил ЗСУ. Також вимагається дотримання додаткових умов, таких як проведення координаторських зустрічей, оформлення відомостей щодо виконання польоту, використання БПС із системою ідентифікації тощо. Усі ці обмеження та вимоги регулюються чинним законодавством, що стосується використання повітряного простору України.

Законопроектний аспект:

Відповідно до проекту № 3716, який прийнято за основу, пропонуються важливі зміни до Повітряного кодексу України. Проект передбачає уточнення понять, унормування питань обліку (реєстрації) БПС, встановлення вимог до компетентностей дистанційного пілота, його підготовки, перепідготовки, підтвердження/відновлення та підвищення кваліфікації. Також вводиться обов'язок експлуатанта БПС щодо страхування відповідальності за шкоду, заподіяну третім особам. Проект дозволяє реєстрацію БПС у випадках, коли вони мають сертифікат або еквівалентний документ,

виданий уповноваженим органом з питань цивільної авіації. Також передбачено безкоштовний облік для певних категорій БПС, таких як ті, що використовуються в освітньому процесі для здобуття позашкільної освіти, наукової та спортивної діяльності.

Проекти законів №8185 та №8186, прийняті Верховною Радою, спрямовані на протидію незаконному використанню безпілотників. Закон №8185 розширює повноваження правоохоронних органів для боротьби з терористичними актами, які виконані за допомогою безпілотних повітряних суден. Також він передбачає регулювання у сфері експлуатації цивільних безпілотників. Закон №8186 встановлює адміністративну відповідальність за порушення порядку та правил використання повітряного простору безпілотними повітряними суднами. Порушення може призвести до штрафів та конфіскації безпілотників.

Також в травні Верховна Рада прийняла закони №9275 та №9276 для підтримки виробництва дронів в Україні. Закон №9276 тимчасово звільняє від сплати ввізного мита компоненти для виробництва та ремонту безпілотних систем, а закон №9275 скасовує сплату ПДВ при ввезенні в Україну компонентів для безпілотних систем. Обидва закони діють до кінця воєнного стану.

В цілому, ці законопроекти та закони спрямовані на удосконалення регулювання у сфері безпілотних систем в Україні, забезпечення безпеки та ефективного використання цих технологій у різних галузях, включаючи оборону та цивільні сфери.

Ліцензування:

З пункту 4 розділу II Авіаційних правил видно, що політ безпілотних повітряних суден масою до 20 кг може бути здійснений без необхідності отримання дозволів та інформування відповідних державних органів. Однак, важливим є встановлення чітких механізмів сертифікації та ліцензування для безпілотних повітряних суден, які вже знаходяться в реєстрі. Це передбачає детальний технічний огляд, що включає аналіз конструкції, систем управління, автопілотів, датчиків та інших складових. Ліцензування операторів, зокрема тих, що використовують безпілотники масою понад 25 кг, вимагає спеціальної документації та дотримання встановлених правил і обмежень. Оператор повинен мати відповідну кваліфікацію та знання з питань безпеки польотів, правил використання безпілотників, процедур дозвільних режимів та інших вимог. Ситуація у країні, зокрема воєнний стан, може ускладнити всі процедури, тому розгляд питань сертифікації та ліцензування до завершення воєнного стану може бути доцільнішим підходом.Додатково, важливо забезпечити відповідність законодавства Європейського Союзу у

сфері сертифікації, ліцензування, застосування та оподаткування безпілотних систем. Це дозволить Україні взаємодіяти та виробляти технології, які відповідають європейським стандартам. Ураховуючи потужний потенціал України в області літакобудування та технологій, розширення випуску та застосування безпілотників може призвести до розвитку як національної безпеки, так і економіки, покращуючи технологічний прогрес та піднімаючи країну на новий рівень в цих галузях.

2.2 Виявлення БПЛА:

2.2.1 Акустичі датчики і системи

Автоматизований пасивний програмно-апаратний комплекс для акустичного детектування слабких звукових сигналів літальних апаратів, дронів і безпілотників відзначається своєю високою ефективністю та надійністю(рис .2.3). Здатний виявляти джерела сигналів на відстані до 500-1000 метрів, при цьому можливе виявлення сильних звукових сигналів на кілька кілометрів.

Рис. 2.3- Акутична система виявленя БПС

Шум від гвинта літального апарату виникає в результаті взаємодії лопатей гвинта з оточуючим повітрям під час створення тяги та при витісненні повітря лопатями. Це відбувається в процесі обертання гвинта, коли лопаті змушують повітря викидатися з фіксованого об’єму середовища.

Генерація звукового випромінення також може мати місце під час аеродинамічної взаємодії лопатей з турбулентними утвореннями у набігаючому потоці.

Шум малонавантаженого гвинта поділяється на дві основні категорії: шум обертання і широкосмуговий шум. Шум обертання виникає внаслідок обертання лопатей і має певну частоту, тому може бути розглянутий як звук певного тембру, з гармоніками, що відповідають частоті обертання гвинта. Кількість гармонік залежить від числа лопатей (N) і кутової швидкості обертання (Ω).

Таким чином, з точки зору періодичних динамічних систем, аналіз гвинта виконується, враховуючи, що період обертання для однієї лопаті становить

$T = 2\pi/\Omega$, а для гвинта з N лопатями — $T = 2\pi/(N\Omega)$.

Звуковий сигнал від дронів представляє собою суму гармонік із частотами, кратними частоті обертання ротору або колінчатого валу двигуна F. Амплітуди гармонік зменшуються із зростанням частоти.

Отже, розгляд шуму від гвинта важливий для оцінки його впливу на навколишнє середовище та можливість прийняття заходів для зменшення шумового випромінення дронів.

В режимі стаціонарного польоту, коли літальний апарат рухається прямолінійно і рівномірно, амплітуда кожної наступної гармоніки у звуковому випроміненні зменшується зі збільшенням її частоти. Це означає, що вищі гармоніки мають меншу амплітуду порівняно з нижчими гармоніками при зміні частоти.

Під час зміни режиму двигуна або виконання маневру відбувається зміна частоти звукового випромінення через ефект Допплера. Цей ефект виникає внаслідок руху джерела звуку відносно точки спостереження і змінює частоту звуку для спостерігача. Крім того, при виконанні маневру змінюється орієнтація дрону відносно точки спостереження, що впливає на спрямованість звукового випромінення і інтенсивність звукового поля в точці прийому.

Амплітуди певних високочастотних (ВЧ) гармонік можуть перевищити амплітуди низькочастотних (НЧ) гармонік в окремих випадках, залежно від конкретних умов. У більшості випадків перша гармоніка (основна) має найбільшу амплітуду.

Зазначте, що амплітуди гармонік та їхні фази є випадковими величинами, розподіленими рівномірно. Оскільки головним джерелом звукового шуму дронів із електричними двигунами є шум гвинта, то математична модель звукового випромінення дронів може бути описана у вказаному

вигляді (формула 2.4), за умови відсутності інших джерел шуму.

$$x_{ЕД}(t) = \sum_{m=1}^{M} A_m \cos(2\pi N F_m t + \varphi_m),$$

Формула 2.4 модель звукового випромінення дронів

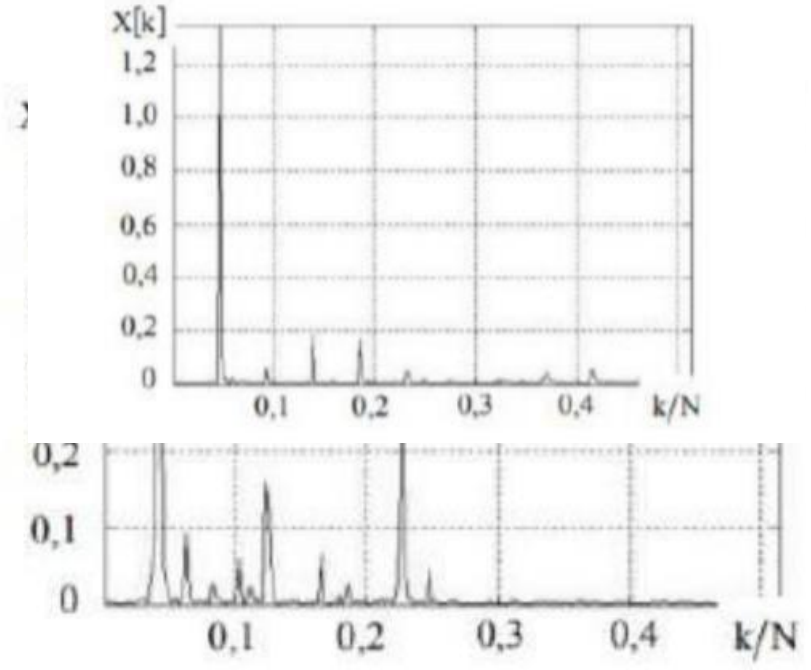
де M – число гармонік звукового випромінення;

Am – амплітуда m-тої гармоніки;

N – число лопатей гвинта;

m – фаза m-тої гармоніки.

Дана модель була створена на основі проведених вимірювань та аналізу звукових сигналів дронів і подальшої статистичної обробки отриманих результатів. Спектральний аналіз записаних реалізацій



сигналів проводився за допомогою періодограми. Нижче показано періодограму звукового сигналу дрону з електродвигуном і

повітряним гвинтом з 3-ма лопатями(рис2.5). Частота дискретизації сигналу s f =8 кГц, тривалість швидкого перетворення Фур'є складає N=512

Рис. 2.5- періодограма звукового сигналу дрону з електродвигуном і повітряним гвинтом з 3-ма лопатями.

Головним джерелом шуму дронів з двигуном внутрішнього згоряння (ДВЗ) є сам двигун. Другорядним джерелом шумів є повітряний гвинт. Модель його звукового сигналу можна записати у вигляді формули 2.6:

$$x_{ДВЗ}(t) = x_{ДВ}(t) + x_{ГВ}(t),\ де\ x_{ДВ}(t) = \sum_{k=1}^{K} A_k\ cos(\ 2\pi NF_k t + \varphi_k\ );\ x_{ГВ}(t) = x_{ЕД}(t);$$

Формула 2.6 - формула розрахунку шума дронів з ДВЗ

Ak – амплітуда k-ої гармоніки;

K – число гармонік звукового випромінення ДВЗ;

k – фаза k-ої гармоніки.

Для дрону з двотактним двигуном (ДВЗ) та гвинтом із двома лопатями гармоніки звукового випромінення, номери яких кратні двом (парні), матимуть більшу амплітуду, ніж сусідні непарні гармоніки. Це явище пояснюється додаванням потужностей гармонік, що виникають від двигуна та повітряного гвинта. У випадку дрона з чотиритактним ДВЗ гармоніки, номери яких кратні чотирьом, матимуть більші амплітуди, порівняно з амплітудами сусідніх гармонік. Перша гармоніка залишається винятком і зазвичай має найвищу амплітуду. Виняток з цього правила становить перша гармоніка, яка, як правило, має найбільшу амплітуду.

Періодограма звукового сигналу малорозмірного дрона з ДВЗ зображена на рисунку 2.7

Рис. 2.7 - Періодограма звукового сигналу малорозмірного дрона з ДВЗ

З підвищенням частоти гармонік відбувається розширення спектральних ліній звукового випромінення двигунів обох типів, оскільки починають проявлятися шуми випадкової природи. Акустичне випромінення дронів мультироторного типу від одного гвинта описується аналогічно дронам з електричним двигуном (ДВЗ на дронах такого типу, як правило, не застосовується). Зазвичай частоти кожного з двигунів не співпадають, а відмінні на певну незначну величину, що залежить від динаміки руху дрона. Тоді математичну модель звукового випромінення такого дрона можна записати у вигляді формули 2.8:

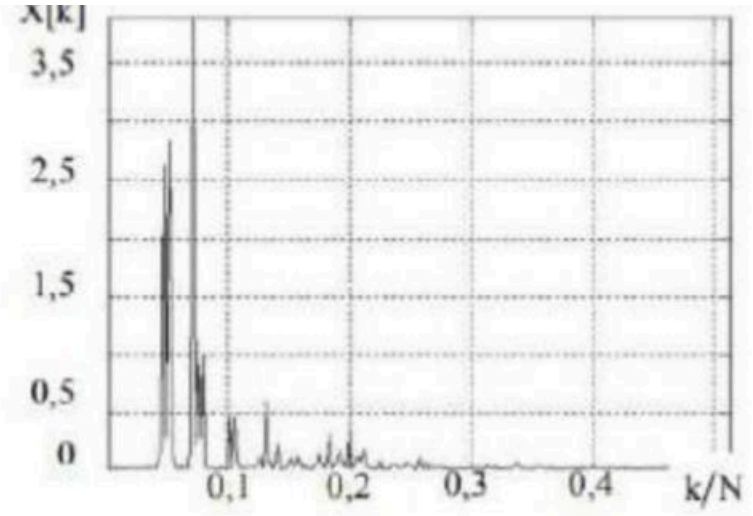
$$x_{\text{МР}}(t) = \sum_{p=1}^{P} x_p(t),\ де\ x_p(t) = x_{\text{ЕД}}(t);$$

Формула 2.8 - математична модель звукового випромінення для дронів з електричним двигуном

$$S_{ДВ}(t) = \sum_{i=1}^{MK} A_i \sin\{2\pi[F+A_{m_i}\sin(2\pi F_m t)]\, it\};$$

$$S_{ГВ}(t) = \sum_{i=1}^{K} A_i \sin\{2\pi M[F+A_{m_i}\sin(2\pi F_m t)]\, it\},$$

P – кількість гвинтів.



Через різницю у частотах обертання гвинтів спектральні лінії звукового випромінення будуть розширеними в порівнянні зі спектральними лініями звукового випромінення дронів літакового типу (з одним гвинтом).

Нижче наведена періодограма звукового випромінення дронів мультироторного типу з чотирма гвинтами (рис. 2.9)

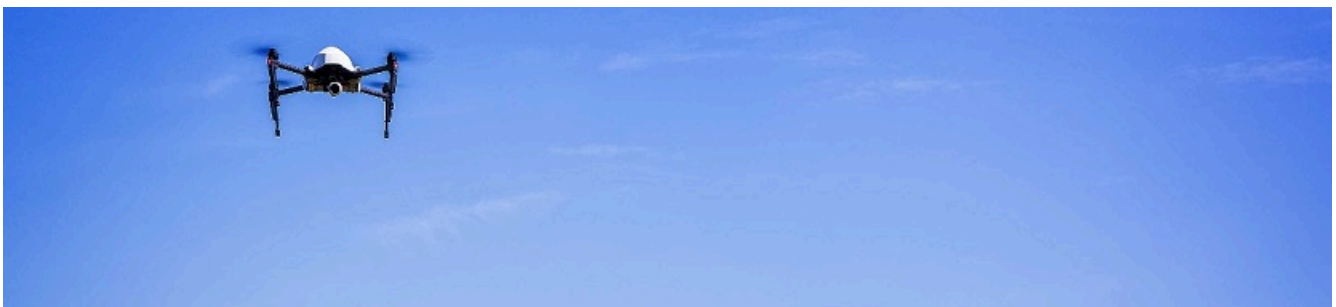
Рис. 2.9- періодограма звукового випромінення дронів мультироторного типу з чотирма гвинтами

Оскільки управління дронів мультироторного типу здійснюється саме за рахунок несійних повітряних гвинтів, то саме цим і пояснюється розширення спектральних ліній в порівнянні з дронами літакового типу (з одним гвинтом). Зі збільшенням числа повітряних гвинтів спектр звукового сигналу такого дрону стає ще більше насиченим спектральними лініями. З отриманої спектральної оцінки дуже важко зробити висновок, що в зоні огляду звукового пристрою спостереження знаходиться дрон. Для цього необхідно проводити подальшу обробку отриманої періодограми для виявлення кратних гармонічних складових.

В загальному випадку сигнали звукового випромінення дронів є частотно-модульованими і їх моделі для ДВЗ та повітряного гвинта дронів літакового типу можна записати у наступному вигляді формули 2.8 (без урахування випадкових фазових зсувів гармонік):

Формула 2.10 - сигнали звукового випромінення

де Ami – індекс частотної модуляції звукового сигналу, що виникає внаслідок зміни режиму роботи



двигуна або виконання маневру;

Fm – частота модуляції, викликана зазначеними ефектами.

Як було зазначено вище, частотний склад звукового випромінення дронів безпосередньо пов'язаний з параметрами двигуна або повітряного гвинта (їх частотою обертання)

Переваги:

- Висока ефективність та надійність детекції на великих відстанях.
- База даних навчена на основних популярних дронах.
- Різноманітні варіанти комплексів для різних потреб.
- Інтеграція з відеоаналітикою та радіочастотним методом.
- Автоматична звукова сигналізація та індикація подій у реальному часі.

Недоліки:

- Детектор звуку не ефективний в густо забудованих або гучних міських областях.
- Можливість обхідних заходів шляхом зміни характеристик БПЛА.
- Пасивні системи можуть бути менш ефективними в умовах, де інші засоби (радари, камери) також не працюють.

2.2.2 Радарні системи

Радарні системи (рис. 2.11) представляють більш досконалі пристрої для виявлення дронів, використовуючи технології ближньої радіолокації. Ці рішення застосовуються в основному в сфері військового застосування.

Через невеликий розмір дронів, обмежену пропускну здатність та потужність, а також враховуючи вартість обладнання, імпульсні радари спостереження часто не можна застосовувати, особливо коли потрібно розгорнути мережу радарів для повного покриття контрольованої зони, як це необхідно при ідентифікації БПЛА. Частотно-модульовані безперервні (FMCW) та безперервні (CW) радіолокаційні станції наразі є найбільш привабливим та економічно ефективним рішенням для вирішення цих завдань.

Рис. 2.11 – радарні системи

Сигнал FMCW, також відомий як лінійно модульований FMCW (LFMCW) або сигнал, модульований лінійною частотою (LFM), представляє собою лінійно модульовану радіоенергію безперервної хвилі, що передається у визначений напрямок. Такі сигнали часто називають чирпами

і вони відрізняються від CW, оскільки у FMCW робоча частота змінюється під час передачі. Радари, що використовують такі сигнали, стали дуже популярними, особливо в автомобільній галузі, завдяки низькій вартості апаратних компонентів та здатності надавати інформацію як про відстань, так і про доплерівські зміни частоти для визначення швидкості цілей. Сигнали FMCW передаються та приймаються; з цих сигналів можна отримати інформацію про затримку (τ) і фазу (φ), які корисні для визначення відстані і швидкості однієї чи кількох цілей одночасно.

Основна обробка прийнятого сигналу виконується за допомогою I / Q демодуляції, яка забезпечує фазові та квадратурно-фазові компоненти складного базового сигналу, відомого як сигнал бите або сигнал проміжної частоти (ПЧ). Знижувальне перетворення введено, щоб значно спростити реалізацію схем обробки, дозволяючи ланцюгу працювати на значно менших частотах порівняно з переданим сигналом. Істотна різниця між ланцюгами обробки FMCW та CW полягає лише у генераторі керуючого сигналу, який забезпечує опорний сигнал (у випадку CW він є постійним). Поєднуючи цей сигнал з осцилятором, керованим напругою (VCO), виходить результуючий ВЧ-сигнал, який буде передаватися радаром.

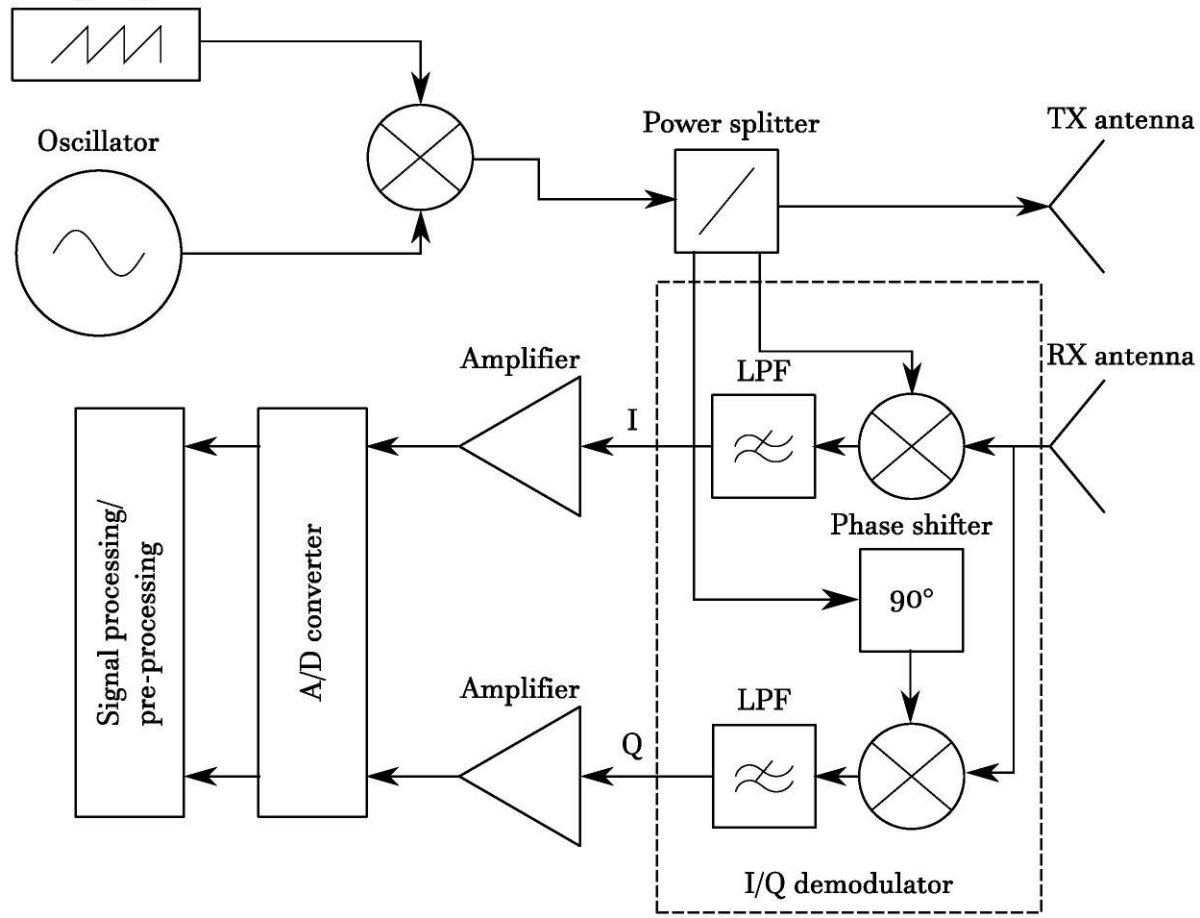


Схема 2.12 - структура радіолокаційної станції з FMCW

На схемі 2.12 зображена структура радіолокаційної станції з FMCW

Математично кажучи, переданий сигнал FMCW може бути виражений за формулою 2.13

$$S_{TX}(t)=A_{TX}\cos(2\pi f_c t + \pi S t^2 + \varphi TX), \qquad \text{(формула 2.13)}$$

де A_{TX} - амплітуда, φTX - зсув фази, S = B / T - нахил звукового сигналу, а fc - несуча частота. Якщо при t = 0 ціль знаходиться на відстані d від радіолокатора, то прийнятий сигнал буде затримкою та ослабленим варіантом переданого сигналу, тобто за формулою 2.14

$$s_{RX}(t)=A_{RX}\cos(2\pi f_c (t-\tau) + \pi S(t-\tau)^2+\varphi_{RX})+n(t), \quad \text{(формула 2.14)}$$

де n (t) - складова шуму, а τ≈2d / c (зі c швидкістю світла) - затримка, тобто час зворотного руху. Компоненти фази та квадратури-фази сигналу ПЧ (биття) можуть бути виражені як формула 2.15

$$IF(t)=IF_I(t)+jIF_Q(t)=A_{IF}e^{j(2\pi f_c \tau+2\pi S\tau t-\pi S\tau^2-\Delta\varphi)} + n_I(t) + jn_Q(t),$$
$$=A_{IF}e^{j\Psi(t)}+n_I(t) + jn_Q(t), \qquad \text{(формула 2.15)}$$

де Ψ (t) позначає фазу сигналу биття. Попередні вирази все ще є дійсними для випадку CW, єдина різниця полягає в нахилі (швидкості щільності) S, який для CW дорівнює нулю. Тоді миттєва частота, пов’язана з сигналом, відсіяним від цілі, є похідною від Ψ (t) та ми маємо формулу 2.16

$$f_{IF} = \frac{1}{2\pi}\frac{d\Psi(t)}{dt} = S\tau, \quad \text{(формула 2.16)}$$

Згадавши визначення τ, легко оцінити дальність цілі як формулу 2.17

$$\hat{d}=\frac{c}{2S}f_{IF}. \qquad \text{(формула 2.17)}$$

Вищезазначена оцінка діапазону справедлива лише для нерухомих об'єктів. Для отримання оцінок дальності та швидкості для рухомого об'єкта, такого як дрони, необхідно враховувати коливання відстані як функцію часу, створюючи, в свою чергу, змінну в часі τ, як показано у формулі 2.18

$$\tau(t)=\frac{2d}{c}+\frac{2v_r t}{c}cos(\theta), \qquad \text{(формула 2.18)}$$

де vr = λ2fD - радіальна швидкість цілі, залежно від допплерівської частоти fD, а θ - кут огляду між радіолокаційною прямою видимістю (LOS) і траєкторією цілі.

Переваги:

- Висока дальність дії на відкритих просторах
- Здатність розпізнавати рух об'єкта та надавати повну інформацію.
- Можливість фіксації відеокадрів для візуального спостереження.
- Деякі моделі мають велику кількість одночасно визначених цілей.
- Доплерівський радар розпізнає швидкість руху, виявляючи дрони.

Недоліки:

- Ефективність обмежена в густо забудованих або гучних міських областях.
- Можливість обхідних заходів, зокрема, зміни характеристик дронів.
- Менш ефективні виявлення малогабаритних безпілотників на невеликих висотах.
- Спрямованість на виявлення великих апаратів, що може ускладнити реакцію на малі дрони.

2.2.3 Оптичні системи

Візуальні системи виявлення дронів використовують камери спостереження для реєстрації рухливих повітряних об'єктів. Вони намагаються відрізнити безпілотники від птахів за розміром, траєкторією польоту та стилем руху. Зазвичай, такі камери мають обмежену дальність до близько 350 метрів. Навіть при використанні комп'ютерних алгоритмів для відстеження політу моделі, визначення, чи це птах чи безпілотник, може бути дуже складним завданням, оскільки деякі

ключові показники польоту безпілотника можуть схожі на рухи птахів.

Проте, впровадження штучного інтелекту (ШІ) та програмного забезпечення (ПЗ) може полегшити ідентифікацію дронів за зображеннями, отриманими від камер. Ці технології дозволяють відокремити характеристики польоту, роблячи ідентифікацію точнішою.

Переваги:

- Здатність відслідковувати рух об'єктів на значній відстані.
- Використання алгоритмів і ШІ для покращення точності ідентифікації.
- Невелика вартість в порівнянні з деякими іншими технологіями.
- Потенціал для розширення функціональності через оновлення програмного забезпечення.
-здатна фіксувати відеозображення як доказову базу для застосування у розслідуванні злочинів.

Недоліки:

- Обмежена дальність спостереження, особливо порівняно з радарними системами.
- Складність відрізнення дрона від птаха лише за допомогою оптичних методів.
- Залежність від видимості та погодних умов.
- Можливість помилкової ідентифікації, особливо на великих відстанях.

2.2.4 Радіочастотні системи

Ця система обнаруження дронів (рис. 2.20) базується на технології направленого вимірювання радіочастот, яка в реальному часі визначає радіосигнали дрона та його пульта дистанційного управління, як зображено на схемі 2.19 Радіочастотні (РЧ) системи є основою будь-якого дрона, що дозволяє йому спілкуватися з контролером та іншими дронами в цьому районі.

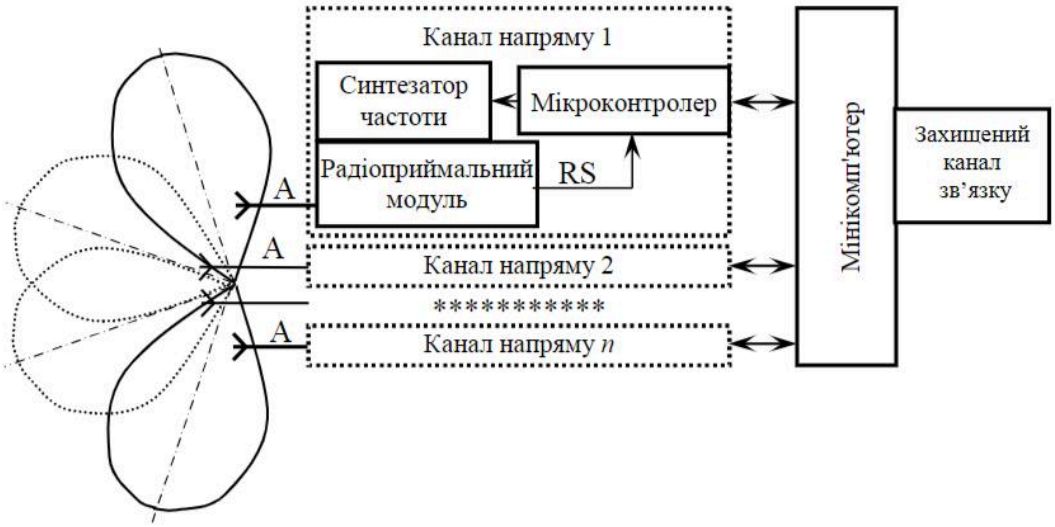


Схема 2.19 – принцип роботи РЧ системи

Система надає попередження оператору про наближення дронів, має необмежену дальність виявлення (визначається мощністю передавача дрона) і виявляє дрони, які тільки увімкнулися. Крім того, вона може ідентифікувати тип дрона, забезпечує високу точність відслідковування і працює в різних умовах, включаючи міське середовище. Система також може інтегруватися з іншими системами.

У системах радіомоніторингу з одночасним пошуком по частоті і напрямку (за допомогою керованих фазованих антенних грат – ФАГ) збільшується ймовірність пропуску сигналу. Тому прийнятним компромісом є пошук по частоті та багатоканальна система з декількома антенами і радіоприймальними модулями для паралельного виявлення сигналів з декількох напрямків по азимуту і по куту місця .

Ширина діаграми спрямованості антени в кожному каналі визначається необхідною точністю визначення напрямку на джерело радіовипромінювання. Кількість каналів «n» залежить від ширини повного сектора спостереження і ширини діаграми спрямованості кожної антени. У кожному каналі є мікроконтролер, який:

Рис. 2.20 – РЧ система виявленя

-приймає команди від мінікомп'ютера;

-формує коди для вибору частоти в синтезаторі радіоприймального модуля;

-встановлює часові затримки на час завершення перехідних процесів в синтезаторі радіоприймального модуля;

-приймає і зберігає сигнали з виходу радіоприймального модуля для кожної частоти прийнятого сигналу;

-проводить первинну обробку прийнятих сигналів;

-передає в мінікомп'ютер результати радіочастотного сканування всього частотного діапазону.

Завдяки тому, що комплекс складається з блоків (каналів), можливе створення необхідної конфігурації для специфіки виконання конкретного завдання. Мінікомп'ютер (або ноутбук) проводить обробку результатів радіочастотного сканування для кожного каналу напряму.

Після отримання результатів радіочастотного сканування всього частотного діапазону, визначаються частоти спектра з максимальними прийнятими рівнями сигналів. Сигнали порівнюються з рівнями сигналів для тих же частот у сусідніх каналах напряму для розрахунку уточненого пеленгу на радіопередавальний пристрій МБПЛА.Враховуючи жорсткі міжнародні вимоги щодо електромагнітної сумісності та усунення взаємних радіоперешкод, радіочастотний обмін між БПЛА

і оператором здійснюється в більшості випадків в діапазонах частот (табл. 2.21) для ромислової, наукової і медичної апаратури - Industrial, Scientific and Medical band ISM).

Частота, МГц	Ширина діапаз., МГц	Макс. потуж-ність, мВт
2400	85	100
5000	100	200
5800	350	500

Таблиця 2.21 - діапазон частот ISM

Переваги:

- Раннє виявлення: Система спроможна виявляти дрона ще до його зльоту, дозволяючи оператору підготуватися до потенційної небезпеки.
- Низький рівень помилкових сигналів: Система ефективно розрізняє між радіочастотним випромінюванням дронів та іншими об'єктами, зменшуючи ризик ложнопозитивних результатів.
- Інтеграція з іншими системами: Система може бути легко інтегрована з іншими системами Rantelon, розширюючи її функціональність та ефективність.

Недоліки:

- Обмеження в густонаселених міських зонах: В деяких умовах, таких як густонаселені міські області, система може зазнавати обмежень в ефективності через інтерференцію.
- Не визначає напрямок малих об'єктів: Важко визначити напрямок малих безпілотників або дронів, що може вплинути на реакцію на загрозу.
- Вартість та підтримка: Висока вартість системи та необхідність кваліфікованого технічного обслуговування можуть стати фактором, особливо для менших компаній чи організацій.

2.2.5 Мультисенсорні системи

Сучасні системи виявлення безпілотних літальних апаратів (БПЛА) широко використовують мультисенсорні методи для надійної та ефективної роботи. Мультисенсорні детектори дронів

використовують різні канали для обробки сигналу від мети:
Візуальний канал: Використання оптичних сенсорів для виявлення дронів на основі видимого світла.
Тепловий канал: Застосування інфрачервоних камер для виявлення теплових слідів дронів, що може бути корисним у різних умовах освітлення.
Акустичний канал: Використання мікрофонів для виявлення звукових сигналів, що можуть бути вироблені дронами.
Ультразвуковий канал: Використання ультразвукових сенсорів для виявлення ультразвукових сигналів, що можуть виникати при роботі дронів.
Радіочастотний канал: Використання радіочастотних сенсорів для виявлення сигналів, що випромінюються дронами, таких як Wi-Fi або радіолокаційні сигнали.
Радіолокаційний канал: Використання радіолокаційних сенсорів для визначення положення та руху дронів.
Кожен з цих каналів має свої переваги та недоліки, і використання мультисенсорних систем дозволяє комбінувати їх для покращення ефективності виявлення дронів. Мультисенсорний підхід забезпечує високу точність виявлення та дозволяє зменшити ймовірність помилкових спрацювань, зробивши його ефективним для використання в міських умовах або в ситуаціях швидкого розгортання на різних об'єктах.
Загалом, мультисенсорні методи виявлення БПЛА є потужним інструментом для забезпечення безпеки та захисту від можливих загроз дронів. Їхні переваги у високій точності виявлення та класифікації дронів підсилюються актуальністю баз даних та можливістю роботи в різних умовах. Однак обмеження у портативності та можливих проблемах у виявленні дронів у високоінтерференційних середовищах створюють виклики для подальшого вдосконалення цих систем.

2.3 Нейтралізація БПС

З огляду на зростаюче використання БПС, необхідно враховувати питання, пов’язані з безпекою, безпекою та конфіденційністю. Їхнє використання може завдати шкоди суспільству через збої та неналежне або злочинне використання. Відзначено значне збільшення кількості аварій з участю дронів або безпілотних літальних систем (БПЛА). Наприклад, неправильне використання поблизу аеропорту може становити серйозну загрозу громадській безпеці та викликати дискомфорт.

З цієї причини розробка технологій виявлення, ідентифікації та пом’якшення шкідливих дронів набула першочергового значення. Система контрзаходів, яку також називають системою протидії UAS, може ідентифікувати та нейтралізувати безпілотник-зловмисник, який класифікується як загроза.

Системи нейтралізації активуються системою командування та управління, щоб реагувати на загрозу, яку представляє виявлений зловмисний дрон. Декілька систем нейтралізації можуть бути активовані одночасно, щоб співпрацювати для підвищення ефективності нейтралізації. Крім того, ці системи можуть бути розташовані на одній або кількох різних платформах відповідно до фізичної архітектури системи протидії.

Системи нейтралізації можуть виконувати різні дії, такі як попередження, керування, переривання, відключення та знищення дронів. Ці дії реалізуються за допомогою методів нейтралізації, які ще називають нейтралізаторами або пом'якшувачами. В літературі різні автори класифікують нейтралізатори по-різному.

Нейтралізатори можна розділити на фізичні та нефізичні в залежності від того, чи відбулося фізичне пошкодження дрону. Нефізичні нейтралізатори не взаємодіють прямо з дроном, але деякі з них можуть все ж завдати йому шкоди. Існує подібний підрозділ, навіть якщо деякі нейтралізатори потрапили в різні класи.

Було проведено розділ на електронні нейтралізатори, які базуються головним чином на використанні електромагнітних хвиль та не спричиняють прямих пошкоджень дрону (наприклад, глушіння), і кінетико-механічні нейтралізатори, що використовують механічні засоби і передбачають фізичний контакт нейтралізатора (або його складової) з шкідливим дроном.

2.3.1. Радіоподавлення та перехоплення управління:

2.3.1.1 Радіочастотні перешкоди

Методи радіочастотного (РЧ) перешкоджання є ефективними засобами впливу на безпілотні літальні апарати (БПЛА), дозволяючи користувачам порушувати чи навіть блокувати зв'язок між шкідливим дроном і його контролером. Ці методи включають генерування сигналів завад для зниження відношення сигнал/перешкода плюс шум (SINR) в приймачі дрону, ускладнюючи або повністю унеможливлюючи отримання інформації від дистанційного керування.

Залежно від реакції дрону на радіочастотні перешкоди, він може здійснити посадку, виконати процедуру повернення додому, впасти без контролю або летіти у випадковому напрямку.

Перешкоди можуть бути спрямовані не лише на дистанційний пульт, але й на відеоканал для функції перегляду від першої особи (FPV), підвищуючи ймовірність перехоплення зв'язку. Існує кілька методів радіочастотних перешкод.

Перший метод, шумове глушіння(noise jamming) — найпростіший у виконанні і полягає у застосуванні шумового сигналу до частини або до всієї спектральної смуги, зайнятої сигналом, який необхідно заглушити, щоб зменшити ємність каналу і збільшити кількість помилок в отриманих даних.

Другий метод — це глушіння тону(tone jamming): в цьому випадку для створення перешкод використовується один або кілька тонів (тобто вузькосмугових сигналів). Ефективність залежить від розташування тонів і потужності, що передається.

Третій метод — глушіння розгортки(sweep jamming), який полягає в передачі вузькосмугового сигналу, який змінює спектр частот, що цікавить, з часом. У кожен момент часу охоплюється лише частина спектру, але в певний період (кількість часу, необхідного для повної розгортки) зачіпається вся цікава смуга.

Четверта і остання техніка — це розумне глушіння(smart jamming), також відоме як глушіння з урахуванням протоколу. Він може бути застосований, коли характеристики цільового сигналу відомі апріорі. Наприклад, якщо система зв’язку під час перешкоджання використовує розширений спектр (FHSS) зі стрибковою зміною частоти і шаблон стрибкоподібних перепадів відомий, то нейтралізатор може виконувати ті самі стрибки частоти, що й ціль, і зменшувати смугу пропускання, необхідну для сигналу перешкоди

Застосування технологій, таких як програмована радіо та аналізатори сигналу, робить інтелектуальне глушіння ефективним та гнучким методом, що враховує характеристики системи зв'язку. Відоме також як глушіння з урахуванням протоколу, цей метод дозволяє точно калібрувати перешкоди для конкретного цільового сигналу.Враховуючи постійний розвиток технологій та використання програмованих радіо, радіочастотні перешкоджання стають все більш потужним та складним засобом контролю над безпілотними системами.

2.3.1.2 Радіоподавлення GNSS

Практика заглушення Глобальної навігаційної супутникової системи (GNSS) відрізняється від радіочастотних перешкод, спрямовуючись безпосередньо на глушіння сигналів GNSS, які мають велику уразливість до таких втручань. Заглушення GNSS може виникати з використанням тих самих радіочастотних методів, що були розглянуті раніше, і визначається своєю ефективністю у нейтралізації сигналів GNSS.

У порівнянні з іншими перешкодами, заглушення GNSS може впливати на поведінку комерційних дронів, призводячи до дрейфу, утруднень у керуванні та порушення процедур повернення додому (RTH). Важливою особливістю є те, що зловмисне впливання на сигнали GNSS може виникнути, навіть якщо дрон оснащений системою внутрішньої навігації IMU, та може бути важко виявлене, якщо дрон використовує інші методи управління або програмований маршрут.

Розумне глушіння та глушіння розгортки визнані найефективнішими методами у боротьбі з GNSS перешкодами, причому перше спрямоване на зведення сигналу GNSS до непридатного для приймача, а друге визначається простотою використання. Треба відзначити, що ефективність таких методів залежить від ряду чинників, таких як швидкість розгортки смуги частот і наявність інших датчиків у дрона. Подолання внутрішніх недоліків, виявлених радіочастотними та GNSS перешкодами, може бути досягнуте використанням обох методів для симультанного застосування, що підвищує загальну ефективність нейтралізації.

2.3.1.3 Спуфінг

Спуфінг є стратегією, що передбачає створення автентичного підробленого сигналу з достатньою силою для обману приймача зловмисного дрона, змушуючи його вважати цей сигнал легітимним. Такий вид втручання може охоплювати різні типи сигналів, таких як комунікація дистанційного керування, передача даних корисного навантаження, GNSS та датчики. Для успішного спуфінгу необхідно мати знання використовуваних стеків протоколів зв'язку та їх можливість точного відтворення. Спуфінг, хоча теоретично можливий, є складним завданням і не завжди дієвим. В практиці цей метод може бути використаний для прихованого взяття під контроль зловмисного дрона та змушення його відступити від захищеної зони.

Спуфінг часто впроваджується у сигналах GNSS, де він може впливати на поведінку дрона, змушуючи його приземлитися, включити автопілот, залишитися у повітрі або слідувати визначеному маршруту. Існують дві стратегії: явний спуфінг, коли нейтралізатор не приховує свої спроби підпорядкувати цільову систему, і прихований спуфінг, де спуфер уникдає виявлення

підроблення, використовуючи підроблені сигнали, що максимально подібні до легітимних.
У випадку успішного прихованого спуфінгу спуфер може взяти під контроль вузли відстеження приймачів з малим відношенням потужності підробленого до легітимного сигналу, що дозволяє надійно і приховано маніпулювати системою. Спуфінг також може бути направлений на бортові датчики, викликаючи дестабілізацію системи управління дроном, хоча такі атаки обмежені звуковою хвилею та вимагають значної динамічності.

2.3.1.4 Нейтралізатори, що використовують атаки на основі протоколу та атаки повторення

Деякі кібератаки спрямовані на використання вразливостей, які існують у протоколах, використовуваних у комунікаційних мережах, з метою вчинення шкідливих дій. Атаки цього типу включають в себе атаки відмови в обслуговуванні (DoS), що полягають у відключенні машини або мережі, зробивши їх недоступними для законних користувачів. Деаутентифікація Wi-Fi, яка включає відключення користувача від точки доступу (WAP), а також атака "flooding", що полягає в відправленні великого обсягу трафіку до цілі, щоб перевантажити її та заважати обробці легітимних повідомлень, належать до цього класу атак. Зазначимо, що ці атаки можуть бути спрямовані на дрони.

Наприклад, комерційні дрони, які використовують зв'язок Wi-Fi без аутентифікації для доступу до мережі, стали вразливими до атак деаутентифікації та переповнення контролера мережевого інтерфейсу дрона (NIC). Використовуючи деаутентифікацію, злоумисники можуть відокремити дрон від його дистанційного пілота, активуючи процедуру безпеки та використовуючи вікно відключення для набуття контролю над безпілотником.

Інша кібератака, спрямована на від'єднання комерційного дрона від його контролера, це атака на отруєння кешу протоколу розділення адрес (ARP). Хоча багато з цих атак можна уникнути за допомогою мережі з аутентифікацією, основна ідея може бути використана для створення нейтралізатора, використовуючи аналіз протоколів, які використовуються дронами, для виявлення слабких місць у стеку зв'язку.

Такий нейтралізатор може бути застосований до комерційних дронів, які використовуються неправильно, як перший метод нейтралізації, хоча його ефективність обмежена можливістю користувачів виправляти виявлені недоліки. Додатковою можливістю є атака відтворення, яка полягає у перехопленні та повторній передачі даних для захоплення та дезорієнтації дрона. Слід враховувати, що такі атаки, хоча й прості, можуть бути контролювані зловмисниками, тому

застосовані контрзаходи та аналіз вразливостей є важливими.

2.3.1.5 Потужні електромагніти та лазери

Високопотужні електромагнітні пристрої можна використовувати для створення променів електромагнітної енергії в широкому спектрі частот, в узько- або широкосмуговому режимі, що призводить до тимчасових або постійних впливів на електроніку цільових дронів. Ці засоби можна поділити на два класи: вузькосмугові електромагнітні (відомі як високопотужні мікрохвилі, HPM), які випромінюють високу потужність на майже одній частоті, і широкосмугові електромагніти, які використовують короткі імпульси у часовій області та розподілену енергію по широкій смузі.

Для ефективності використання високопотужних електромагнітів, потужний електромагніт повинен бути точно спрямований на ціль, інакше його ефективність значно знижується. Оцінка результатів нейтралізації після використання таких електромагнітів також є важливим аспектом, оскільки деякі пристрої можуть продовжити роботу після впливу.

Лазери, які використовуються як пом’якшувачі, можуть вивести з ладу або знищити дрон. Електролазер іонізує шлях до дрона, випромінюючи електричний струм по провідній доріжці іонізованої плазми. Їх можна класифікувати на малопотужні (для нейтралізації деяких чутливих датчиків) та потужні (здатні до знищення дрона).

Обидві категорії вимагають точного прицілювання та часу для відстеження цілі. Лазери, проте, мають обмежену застосовність у цивільному середовищі через великі розміри та вагу, чутливість до погодних умов та потребу в точному наведенні.

Однак важко зробити висновок про використання потужних електромагнітів та лазерів у цивільних умовах через їхню велику масу та потребу в високих технологіях. Низьковисотні платформи, такі як міні-дрони, можуть зустрічати труднощі у використанні цих засобів безпеки в ефективний спосіб

2.3.2 БПЛА перехоплювачі:

Опис: Цей метод включає в себе використання спеціальних безпілотних літальних апаратів, призначених для перехоплення та вимкнення інших дронів. Ці перехоплювачі можуть використовувати різноманітні методи, включаючи блокування сигналів чи фізичні засоби втручання.

У цьому контексті для протидії зловмисному дрону використовується спеціальний безпілотний літальний апарат (БПЛА), що обладнаний засобами виявлення та відстеження, призначеними для виявлення та нейтралізації загрози. Дрон-нейтралізатор має високу швидкість для ефективного

переслідування шкідливого дрону. Зазвичай такі засоби ефективні у випадку невеликих дронів, що операційно діють у захищених зонах.

Безпілотники для зіткнення можуть використовувати методи виявлення, засновані на технологіях комп'ютерного зору, і можуть бути оснащені вибуховими матеріалами для максимізації пошкодження при зіткненні з дроном. Ці безпілотники можуть завдати побічної шкоди, подібно до снарядів, і характеризуються більшою затримкою у порівнянні з заходами, що використовуються в ракетних системах.

Нейтралізатори такого типу є одноразовими системами, які виступають як гібрид між дроном і ракетою

Переваги:

-Здатність фізично зупиняти небажаний БПЛА.

-Ефективність відносно відкритих просторів.

Недоліки:

-Обмежена ефективність в зоні з великою концентрацією дронів.

-Ризик втрати або пошкодження власного перехоплювача під час втручання.

2.3.3 Зброя стрілецька та інша:

Опис: Цей метод полягає в застосуванні різноманітних стрілецьких та фізичних засобів для фізичного вимкнення дронів. Стрілецька зброя, лазери чи інші пристрої використовуються для нейтралізації небажаного БПЛА.

Ці нейтралізатори представляють собою дійсну зброю, яка використовує снаряди для знищення дронів. До них належать кулемети, боєприпаси, керовані ракети, артилерія, міномети та ракети. Керовані ракети можуть потребувати систем наведення та відстеження для точного визначення положення та ураження цілі дрона, тоді як інші можуть бути обладнані оптичними датчиками для виявлення та відстеження об'єктів. Ці рішення є висококоштовними (з високою вартістю пострілу) і зазвичай використовуються у військових сценаріях. Окрім того, вони можуть викликати побічні ефекти, оскільки вражений дрон може впасти на землю, завдаючи шкоди людям та/або інфраструктурі.

Використання птахів для виявлення та усунення дронів представляє собою останній напрямок у боротьбі з безпілотними літальними апаратами (БПЛА). Недавно Нідерланди вдосконалили навички птахів у протистоянні з БПЛА. Поліція Нідерландів вжила заходів для того, щоб зіткнутися

з дронами в аварійних ситуаціях, розглядаючи це як один із методів протидії БПЛА. У співпраці з фірмою з навчання хижаків у Гаазі, голландська поліція навчила птахів розпізнавати та захоплювати дрони. Захопивши дрон із повітря, птах переносить його в безпечне місце подалі від людей. Місяці навчання включають розпізнавання та захоплення дронів, навчання, що дозволяє птахам нести дрони назад до своїх тренерів. Інтересно відзначити, що під час атаки дронів птахи не отримують травм від роторів, оскільки їх метод атаки дуже точний, і вони чітко бачать ротори, навіть у відміну від людей. Більше того, птахи можуть ефективно збивати дрони на землю, не завдаючи нікому шкоди. Хоча вони здатні атакувати дрони, аналогічні за розміром їм, більші дрони можуть викликати певні турбулентності серед птахів. Дресирувальники використовують силові орли, навчені механічним видобутком в безпечних місцях, далеко від натовпу. У співпраці з поліцією, протягом декількох місяців випробувань, переконувалися, що орли ефективно справляються з завданням перехоплення дронів. Зазначимо, що у майбутньому може знадобитися додатковий захист для птахів, особливо при взаємодії із більшими БПЛА, які можуть представляти загрозу для їхнього безпеки

Переваги:

-Висока ефективність у нейтралізації дронів.

-Здатність працювати у різних погодних умовах.

Недоліки:

-Потенційно великий ризик для оточуючого середовища та персоналу.

-Вимагає великого досвіду та високоточного обладнання для забезпечення безпеки в ході втручання.

3. Нейронна мережа

Нейронні мережі, також відомі як штучні нейронні мережі (ШНМ) або імітовані нейронні мережі (ІНМ), є важливою складовою сфери машинного навчання та лежать в основі алгоритмів глибокого навчання. Їх назва та структура взяті на озброєння від природи, імітуючи взаємодію біологічних нейронів у людському мозку. Узагальнена структура нейронної мережі проілюстрована на рис. 3.1.

Штучні нейронні мережі складаються з вузлів, які утворюють вхідний рівень, один чи кілька прихованих шарів і вихідний рівень. Кожен вузол з'єднаний з іншим і обладнаний вагою та порогом.

Вихід вузла активується, якщо його значення перевищує встановлений поріг, передаючи інформацію на наступний рівень. Цей механізм передачі сигналів в нейронних мережах сприяє адаптації та вивченню залежностей у вхідних даних.

За допомогою такої архітектури нейронних мереж можна вирішувати різноманітні завдання, від розпізнавання образів до прогнозування трендів. Важливість їх застосування полягає в можливості автоматичного вивчення та адаптації до змін в навчальних даних, надаючи системі гнучкість та ефективність у вирішенні складних завдань

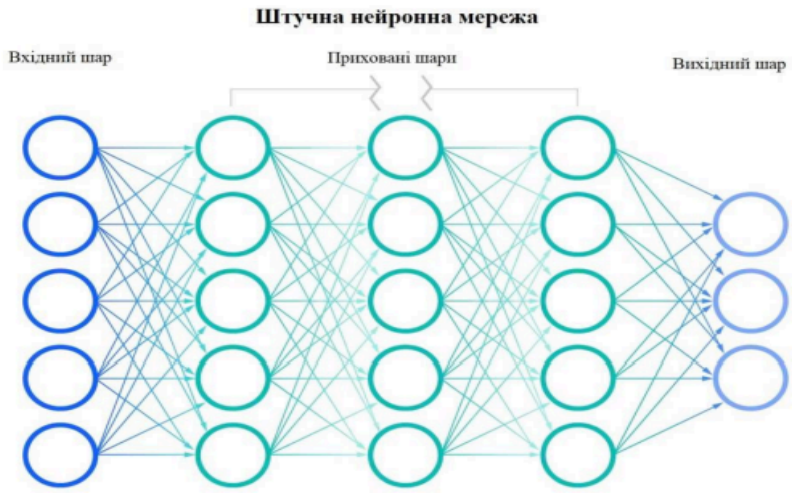


рис 3.1 Структура нейронної мережі прямого зв’язку

Ефективність нейронних мереж напряму залежить від якості та репрезентативності навчальної бази даних. Чим більш ретельно відібрані дані, тим вища точність моделі. Коли алгоритми навчені з високою точністю, вони стають потужними інструментами в галузі інформатики та штучного інтелекту, дозволяючи класифікувати та кластеризувати дані з надзвичайною швидкістю.

Алгоритми, дотримані точних налаштувань, виявляються важливими для індустрії штучного інтелекту, забезпечуючи ефективне вирішення завдань, таких як ідентифікація мовлення чи розпізнавання зображень. Час вирішення таких завдань може значно зменшитися, порівняно з ручним розпізнаванням експертами. Наприклад, завдання розпізнавання мовлення чи обробки зображень може займати лише декілька хвилин чи годин, що дуже ефективно порівняно з тривалим та більш витратним процесом ручного аналізу.

Однією з найвідоміших нейронних мереж є пошуковий алгоритм, розроблений компанією Google, що відзначається вражаючою здатністю до класифікації та обробки великого обсягу даних на високій швидкості.

3.1 Різновиди Нейронних Мереж

У світі штучних нейронних мереж існує розмаїття різних типів, кожен з яких має свою унікальну складність та призначення. Ці типи віддзеркалюють визначену мету відтворення функцій людського мозку для розв'язання різноманітних проблем та завдань . Кожен вид штучної нейронної мережі відтворює структуру нейронів та синапсів, проте вони відрізняються за рівнем складності, варіантами застосування та архітектурою.

Різні типи штучних нейронних мереж розрізняються способом моделювання штучних нейронів та зв'язків між вузлами. Крім того, вони відрізняються в тому, як дані проймають через мережу та густотою вузлів. Деякі з найвідоміших видів включають:

Штучні Нейронні Мережі Прямого Зв'язку: Базовий тип, де інформація рухається від вхідного до вихідного шару без циклічних зв'язків.

Персептрон: Проста форма нейронної мережі з одним шаром, яка використовується для бінарної класифікації.

Багатошаровий Персептрон: Розширення персептрона з декількома шарами, що дозволяє вирішувати більш складні задачі.

Радіальна Основа Функції Штучних Нейронних Мереж: Використовує радіальні функції для обробки інформації у високорозмірних просторах.

Рекурентні Нейронні Мережі: Мережі, що мають циклічні зв'язки, дозволяючи враховувати контекст та залежності в часі.

Згорткові Нейронні Мережі: Особливо ефективні для обробки зображень, враховуючи просторові залежності.

Ці варіації нейронних мереж дозволяють вирішувати різноманітні завдання відповідно до їхньої специфікації та структури, роблячи їх потужними інструментами у сфері інтелектуальних технологій.

3.2 Нейронні Мережі Прямого Зв'язку:

Штучні нейронні мережі, які ґрунтуються на концепції людського мозку, використовують елементи, що імітують основні функції біологічного нейрону. Граючи роль основного будівельного блоку в нейронних мережах, ці штучні нейрони створюють вражаючі можливості для обробки та аналізу інформації. Узагальнена модель нейрона, використана в цьому контексті, наведена на рис. 3.2.

Цей штучний нейрон має вхідні з'єднання, що представляють собою сигнали від інших нейронів чи зовнішніх джерел. Кожне з'єднання має вагу, яка визначає важливість вхідного сигналу. Загалом, ваги та поріги визначають, чи активується цей нейрон. Якщо сума вагованих вхідних сигналів перевищує поріг, нейрон активується і передає сигнал на наступний шар мережі.

Така архітектура дозволяє ефективно моделювати різноманітні завдання та вирішувати їх шляхом зміцнення чи пригнічення ваг та сигналів. Завдяки цим властивостям штучні нейронні мережі прямого зв'язку стають важливим інструментом в сфері машинного навчання, обробки сигналів та штучного інтелекту.

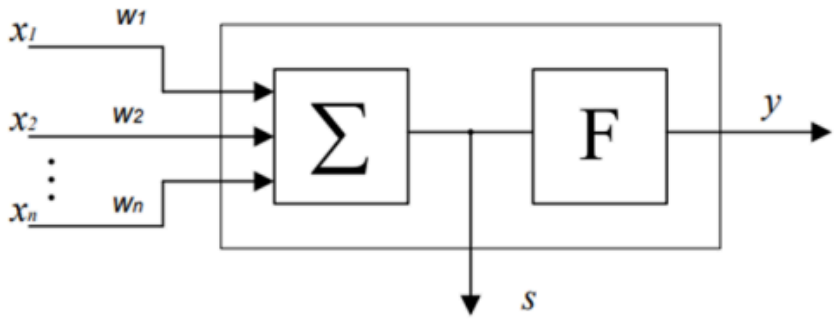


Рис.3.2. Штучний нейрон з активаційної функцією

В процесі роботи нейрона вхідні сигнали, кожен з яких множиться на вагу, сумуються, утворюючи результат підсумовування s (3.3).

Цей результат стає вхідним параметром для функції активації, що визначає відгук нейрона y (3.4) на комбінацію вхідних сигналів. Функція активації перетворює вхідні впливи у вихідний сигнал з необхідними характеристиками.

$$s = \sum wixi + w0 \; p \; i=1 \quad (3.3)$$

$$y = f(s) \quad (3.4)$$

де w i - вага нейрона

- w 0 - коефіцієнт переміщення;

s - підсумок;

x i – частина вхідного вектора

y – вихідні дані нейрона;

p - кількість входів синапсиса;

f - функція активації.

Функція активації може бути як дійсним, так і цілим числом.

Вхідні дані, вагові коефіцієнти та значення зсуву, як правило, приймають дійсні числа. Вихід y називається результатом функції активації. Він може бути як позитивним, так і від'ємним числом. Звичайно використовується функція активації f(x), яка є лінійною (3.5).

$$y=k(s) \; , \quad (3.5)$$

де k - стала порогової функції.

Важливими параметрами нейрона є ваги wi , коефіцієнт переміщення w0, а також функція активації f Функція активації може бути "стисканням", що обмежує діапазон зміни величини s, наприклад, логістична функція, яка широко використовується в експериментах (рис. 3.6).

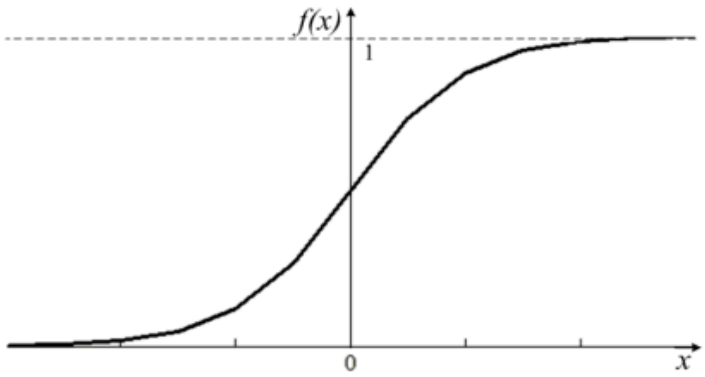


Рис. 3.6. Сигмоїдальна функція

Логістична функція обчислюється формулою (3.7)

$$f(x) = 1\ 1+\exp(-x) \quad (3.7)$$

Іншою часто використовуваною активаційною функцією є гіперболічний тангенс(3.8)

$$f(x) = th\ (x) \quad (3.8)$$

Графік функції гіперболічного тангенсу представлений на рис. 3.9.

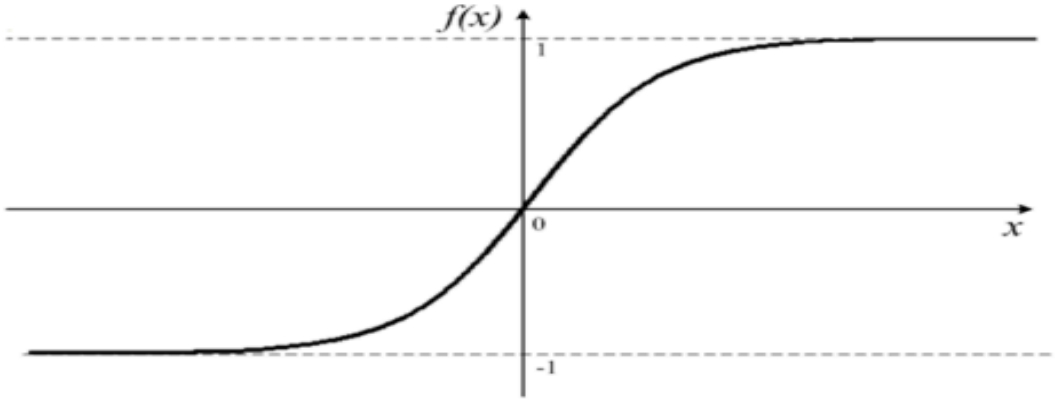


Рис. 3.9. Функція гіперболічного тангенсу

Незважаючи на те, що один нейрон може виконувати найпростіші ідентифікаційні процедури, справжня потужність нейронних обчислень проявляється в їх з'єднанні в мережі.

Нейронна мережа представляє собою сукупність нейронів, які взаємодіють між собою і мають внутрішні властивості та особливу топологію. Навчання мережі включає в себе використання правил для досягнення необхідного вихідного сигналу. Під час навчання мережі надається велика кількість вхідних та вихідних векторів, де кожен вхід або вихід є вектором. Процес навчання полягає в тому, щоб налаштовувати ваги мережі, змінюючи їх поетапно, таким чином, щоб мережа надавала вихідні вектори, бажані для кожного вхідного вектора.

Існують три основних типи навчання: "з ментором", самонавчання та змішане. Навчання з вчителем ґрунтується на достовірних висновках для кожного вхідного прикладу, де мережа спробує відтворити відомі відповіді. У самонавчанні не потрібно знати правильні відповіді; це включає в себе вивчення внутрішньої структури даних та самокореляцію між прикладами у базі даних. Змішане навчання

поєднує методи навчання з вчителем та самонавчання, дозволяючи мережі використовувати обидва підходи для ефективного навчання.

Такий підхід дозволяє створювати нейронні мережі, які здатні адаптуватися до різноманітних завдань і вирішувати їх, використовуючи внутрішні механізми самонавчання та здатність до змішаного навчання.

3.3 Персептрон:

Одною з простих архітектур нейромереж є одношаровий персептрон, що складається з одного шару штучних нейронів, з'єднаних за допомогою вагових значень та великою кількістю входів (рис. 3.10). Групу нейронів зі спільним вхідним сигналом називають шаром. Елемент Σ множить кожен вхід x на вагу

w і підсумовує зважені входи . Вихід дорівнює одиниці, якщо сума перевищує задане порогове значення, а в іншому випадку - нулю.

Така архітектура простого персептрона використовується для бінарної класифікації, де нейрони приймають велику кількість вхідних сигналів та вирішують, чи належить вхідний об'єкт певному класу. Це нейромережеве утворення володіє здатністю вивчати та адаптуватися до вхідних даних.

У процесі навчання персептрона вагові коефіцієнти змінюються так, щоб максимізувати правильні класифікації. Цей процес може бути узагальнений для різних задач класифікації, зробивши персептрон важливим елементом у вирішенні простих задач машинного навчання.

Така проста структура персептрона відображає його обмеженість у вирішенні складних завдань. Однак це є лише вихідна точка для розвитку більш складних та потужних архітектур штучних нейронних мереж.

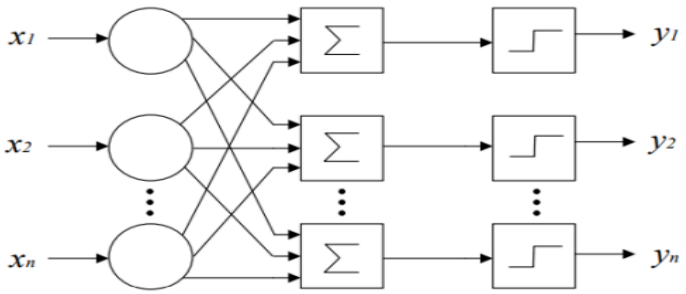


Рис. 3.10. Персептрон

Навчання персептрона відбувається через передавання послідовності багатьох образів по одному на його вхід та адаптацію ваг до досягнення необхідного результату для всіх образів. Такий підхід дозволяє персептрону адаптуватися до різноманітних вхідних даних, оптимізуючи вагові коефіцієнти для досягнення правильних класифікацій.

Проте важливо відзначити, що персептрон доцільно використовувати лише для задач з високою лінійністю. Наприклад, він може успішно розділити точки (0,0) та (1,1) на два класи у двовимірному просторі. Однак він не зможе ефективно розв'язати завдання «виключне або», де потрібно розділити точки (0,0), (1,1) у клас 1 і (0,1), (1,0) у клас 2. Цей приклад відображає нездатність простого персептрона розв'язати завдання, що вимагають нелінійних розділів.

Існує велика кількість функцій, які не можна представити одношаровою мережею. Ймовірність того, що випадково обрана функція буде лінійно роздільною, дуже мала, навіть для помірних розмірів змінних. Це обмеження робить одношарові персептрони придатними лише для рішення простих завдань та обмежує їхню застосовність у вирішенні більш складних проблем.

3.4 Багатошаровий персептрон.

Досить великі обмеження одношарових мереж можна вирішити, добавляючи додаткові шари. Двошарові мережі складаються з одношарових мереж і з’єднуються каскадним типом. Вони можуть робити загальні класифікації. Мережа створює функцію практично будь-якого рівня складності, проте кількість шарів і число елементів у всіх шарах визначають складність функції[. На рис. 2.8 зображена двошарова мережа, яка навчається шляхом функції зворотного поширення.

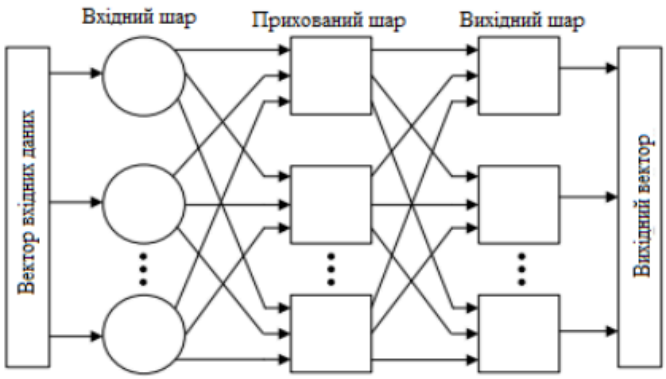


Рис. 3.11 Двошаровий персептрон

Нейрони, які розташовані в одному шарі нейронної мережі, не мають прямих зв'язків між собою, але кожен з них пов'язаний з кожним нейроном наступного шару, за винятком останнього шару, де виходи стають загальними виходами мережі. Перший шар нейронів, який пов'язаний з вхідними даними, відіграє роль розподільчих пунктів, і в ньому не відбуваються жодні математичні операції. Вхідні дані просто проходять через цей шар і подаються на входи ваг на його виходах.

Коли нейрон отримує вхідні дані, наступний шар додає їх з призначеними вагами. Потім ця сума піддається передавальній функції, яка обчислює результат та передає його на один з входів нейрона наступного шару. Цей процес повторюється для всіх нейронів у наступному шарі.

Функціонування мережі прямого типу можна описати за допомогою формули:

$$yj\ k = f\ (\sum wij\ k\ yi\ n(k-1)\ k-1\ i=1\ ),j = 1{:}\ n(k), \quad (3.12)$$

де x - вхідний сигнал;

y k - значення j -го виходу нейрона k -го шару;

w k - вага зв'язку від i -го нейрона (k -1) -го шару до j -му нейрону k -го шару;

f - функція активації;

n(k) - Число нейронів у k -му шарі.

У ролі функції активації в мережах зі зворотним розповсюдженням здебільшого застосовується сигмоїдальна функція. Багатошарові мережі більш продуктивні та потужні, ніж одношарові, лише у разі наявності не лінійних характеристик. стискаюча функція забезпечує необхідну продуктивність . Для старту навчання

багатошарових нейронних мереж використовується алгоритм зворотного розповсюдження похибки. Якщо при роботі прямої функції вхідний сигнал розповсюджується по мережі від вхідного шару до вихідного, то при налаштуванні ваг хиба мережі поширюється від вихідного шару до вхідного.

3.5 Мережі з радіальною базовою функцією (RBF)

Мережі з радіальною базовою функцією (RBF) мають принципово іншу архітектуру, ніж більшість архітектур нейронних мереж. Більшість архітектур нейронної мережі складається з багатьох рівнів і вводить нелінійність шляхом повторюваного застосування нелінійних функцій активації. З іншого боку, мережа RBF складається лише з вхідного рівня, одного прихованого рівня та вихідного рівня. Структура мережі зображено на рис. 3.13

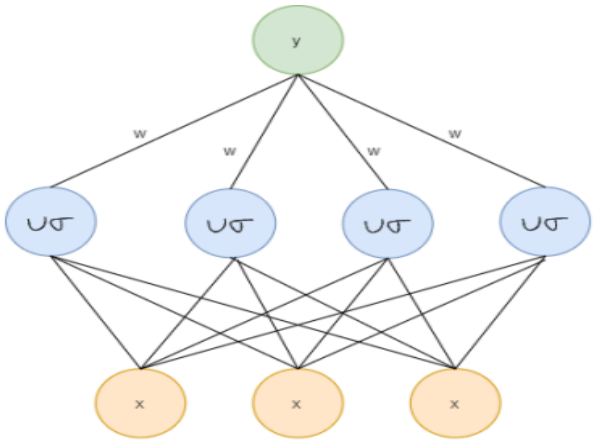


Рис. 3.13. Структура RNN мережі.

Важливо розуміти, що вхідний рівень в мережі RBF не здійснює обчислень; він просто отримує вхідні дані та передає їх на спеціальний прихований рівень мережі RBF. Обчислення, які відбуваються всередині прихованого шару, відрізняються від більшості нейронних мереж, і саме в цьому полягає потужність мережі RBF. Вихідний рівень виконує завдання прогнозування, таке як класифікація або регресія, засноване на обробці прихованим шаром.

Кількість нейронів у вхідному шарі повинна дорівнювати розмірності вхідних даних. На вхідних рівнях не відбуваються обчислення, на відміну від стандартних штучних нейронних мереж. Вхідні нейрони повністю з'єднані з прихованими нейронами та передають свої дані вперед.

Прихований шар призначений для обробки вхідних даних, для яких візерунок може бути не лінійно роздільним, і перетворює його на новий простір, який є більш лінійно роздільним. Зазвичай прихований шар має вищу розмірність, ніж вхідний, оскільки нелінійне перетворення часто потрібне для здійснення лінійного розділення не лінійних шаблонів. Це обгрунтовується теоремою Ковера про роздільність шаблонів, яка показує, що перетворення у простір вищої розмірності часто зроблять шаблон лінійно роздільним.

Обчислення в прихованих шарах ґрунтуються на порівняннях із векторами-прототипами, що є векторами з навчального набору. Кожен нейрон у прихованому шарі обчислює подібність між вхідним вектором і його прототипом, що математично записується так:

$$\Phi_i = e^{\left(\frac{||\bar{X}-\overline{u_i}||^2}{2*\sigma_i^2}\right)}$$

(3.14)

де:

- X як вхідний вектор
- μ як вектор прототипу i^{th} нейрона
- σ як пропускна здатність i^{th} нейрона
- phi як вихід i^{th} нейрона

Параметри μ і σ вивчаються неконтрольованим способом, наприклад, за допомогою певного алгоритму кластеризації. Вихідний рівень використовує функцію лінійної активації як для завдань класифікації, так і для завдань регресії. Обчислення на вихідному рівні виконуються так само, як стандартна штучна нейронна мережа, яка є лінійною комбінацією між вхідним вектором і вектором ваги. Обчислення на вихідному рівні можна математично записати так:

$$y = \sum wi\Phi i \; n \; i \;, \; (3.15)$$

де

- w_i як зв’язок ваги,
- Ф як вихід i^{th} нейрона з прихованого шару а у як результат передбачення

Отриманий прогноз можна використовувати як для завдань класифікації, так і для регресії, це залежить від цільової функції та функції втрат. Параметри w вивчаються контрольованим способом, наприклад градієнтним спуском. Незважаючи на те, що вихідний рівень RBF можна використовувати як кінцевий результат, можна стекувати мережі RBF з іншими мережами, наприклад, ми можемо замінити вихідний рівень мережі RBF багаторівневим сприйняттям і навчити мережу від кінця до кінець.

3.6. Згорточні Нейронні Мережі (CNN):

Згорточні нейронні мережі (CNN) є потужним інструментом для класифікації даних, зокрема для розпізнавання зображень та взаємодії з об'єктами. Цей тип нейронної мережі входить в категорію наглядованого навчання, тобто він потребує набору даних, в якому класи вже класифіковані.

Архітектура CNN можна уявити як набір двовимірних матриць, які накладаються одна на одну. Перший шар представляє вхідне зображення, і наступні шари використовують математичні операції згортки та субдискретизації для зменшення розміру зображення та виділення ключових особливостей. Ці операції виконуються кілька разів, а потім значення передаються через повністю пов'язані шари нейронної мережі, які визначають вихідні дані.

Однією з особливостей CNN є здатність автоматичного визначення важливих функцій та ознак зображення, що робить їх ефективними для роботи з великими обсягами даних. Зокрема, вони знайшли широке застосування в області розпізнавання облич, класифікації об'єктів та розпізнавання паттернів у зображеннях.

На рис. 3.16 зображено приклад градієнтного навчання для розпізнавання документів за допомогою згорточних нейронних мереж.

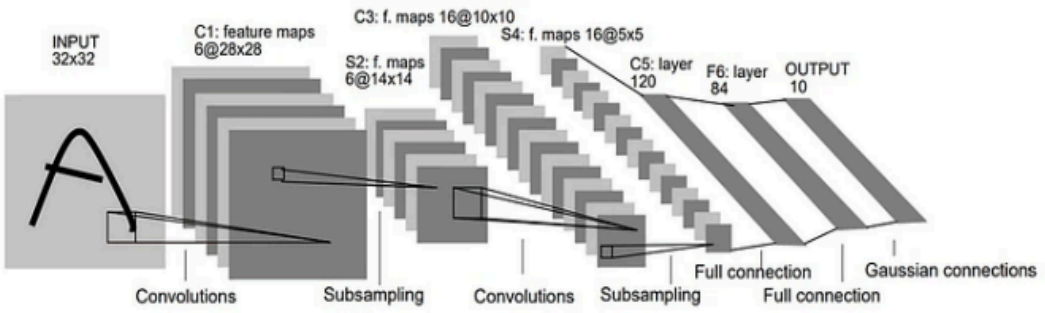


Рис. 3.16. Градієнтне навчання розпізнавання документів

Вихідний результат згорточних нейронних мереж (CNN) представляє собою клас, до якого належать дані, а самі дані виступають у ролі вхідного сигналу. CNN є алгоритмом навчання під наглядом, що передбачає наявність анотованих даних, тобто дані мають бути позначені відповідним класом. Цей підхід є найбільш ефективним, коли маємо справу з графічними даними, які необхідно класифікувати.

Припустимо, що на фабриці з консервації манго направляють у секцію соління, а яблука - у секцію варення. Завданням CNN є визначення цих фруктів, аналізуючи їх зображення. Модель навчається за допомогою набору графічних даних для манго та іншого для яблук, які вже мають відповідні мітки. Після вивчення характеристик кожного фрукта CNN може класифікувати свіжі зображення фруктів, визначаючи їх як манго чи яблука. Такий підхід є ключовим аспектом функціонування CNN.

3.7 RNN Повторювана нейронна мережа (RNN)

— це клас алгоритмів машинного навчання, які підпадають під категорію неконтрольованого навчання. Неконтрольоване навчання – це тип машинного навчання, якому не потрібен набір даних, позначений у необхідних класах. Такі алгоритми використовують вихідні дані одного кроку як частину вхідних даних для наступного кроку.

Оскільки вони можуть використовувати вихідні дані попереднього кроку, вони швидше за все зможуть дізнатися, чи попередні вхідні дані пов’язані з поточними. Встановлення кореляції між останнім введенням і поточним введенням даних є основним завданням RNN . Якщо ви пошукаєте значення слова «повторний» у словнику, ви побачите, що воно означає «повторюваний або часто». Слово відображає те, що існує математична операція, яка виконується кілька разів. У RNN вихідні дані в заданий момент часу оцінюються як функція вихідних даних мережі за попередньою міткою часу. Один важливий момент, який слід зазначити, полягає в тому, що всі вихідні значення використовують однакові правила підвищення градації, оскільки рівні RNN підтримують розподіл ваги. Розгляньте рис. 3.17 , щоб мати більш чітке розуміння RNN, воно представляє роботу RNN.

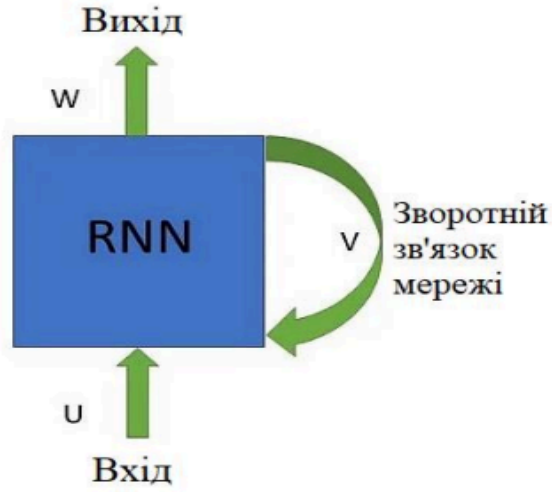


Рис. 3.17. Структура RNN мережі.

Оскільки рекурентні нейронні мережі (RNN) найбільш ефективні для завдань, які вимагають передбачення наступних даних, вони широко використовуються для тимчасових даних, таких як послідовності слів. У випадку введення послідовності слів RNN може передбачити наступне слово у цій послідовності, не потребуючи набору даних із мітками для досягнення цієї мети.

Припустимо, що ми подаємо на вхід RNN речення, яке описує твір мистецтва на виставці. Наприклад: "Митець, здається, занурився в глибини культурного вираження свого часу, щоб створити це вишукане мистецтво. Мазки пензля більш впевнені, ніж…". RNN аналізуватиме кожне слово відносно попереднього і намагатиметься імітувати стиль написання.

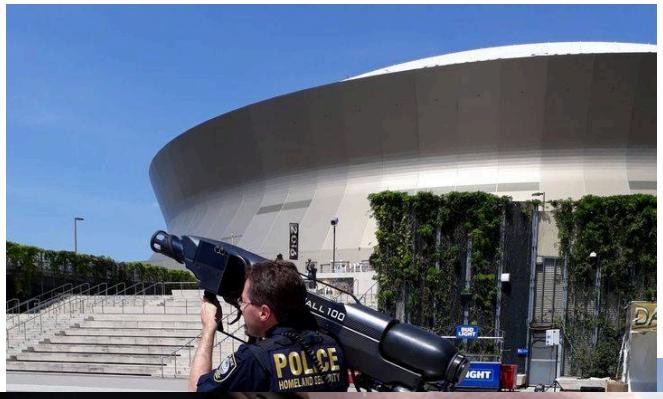
Вихідні дані, передбачені алгоритмом, можуть бути на кшталт "…інші художники свого часу". Однак фактично написаний текст може мати інший вигляд, наприклад, "попередні твори інших художників". Завданням є максимально наблизити передбачені слова до фактичних слів, щоб вони максимально точно відображали стиль та зміст тексту.

3.8. Висновки

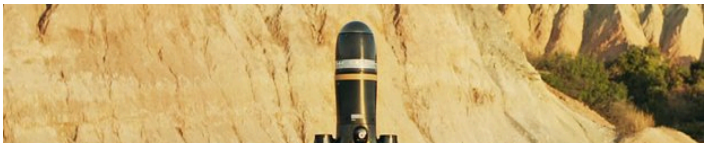
Використання нейромереж в системах виявлення БПЛА відзначається значним потенціалом для підвищення ефективності та точності виявлення. Нейромережі

дозволяють створювати адаптивні моделі, які здатні вчитися та адаптуватися до різноманітних сценаріїв та умов.

Перевагою використання нейромереж для виявлення БПЛА є їхній потенціал у роботі з великим обсягом та високорозмірними даними, такими як зображення та відео. Здатність нейромереж ефективно враховувати контекст та навчатися виявляти складні патерни дозволяє покращити якість виявлення та зменшити ймовірність помилкових сигналів.Однак важливо враховувати високі вимоги до обчислювальних ресурсів для тренування та експлуатації нейромереж. Забезпечення необхідного рівня обчислювальної потужності та врахування витрат часу на тренування може бути важливим фактором при впровадженні таких систем.



Усупереч цьому, впровадження нейромереж у сферу виявлення БПЛА відкриває перспективи для поліпшення систем безпеки, автоматизації та ефективного використання безпілотних систем у різних галузях, таких як військова, цивільна авіація та безпека об'єктів інфраструктури. З кожним новим розвитком технологій



нейромереж та збільшенням обчислювальних можливостей можна очікувати подальшого удосконалення систем виявлення БПЛА за допомогою нейромереж.

4. Існуючи розробки

4.1 OpenWorks Engineering

Оригінальний виріб пропонує британська компанія OpenWorks Engineering - це гранатомет SkyWall 100 (рис 4.1) і сімейство виробів на його базі. Пристрій ґрунтується на добре відомій ідеї лову безпілотника за допомогою сітки. компанія OpenWorks Engineering не припиняє розвиток своїх систем боротьби з БПЛА. На базі переносного гранатомета SkyWall 100 було створено аналогічний виріб SkyWall Patrol. Розроблено автоматизовану турель SkyWall Auto для стаціонарних і мобільних платформ.

Рис. 4.1 - гранатомет SkyWall 100

4.2.REX-1

Це портативний пристрій, що глушить сигнал для дрона, на який буде направлено пристрій. Для використання пристрою потрібна людина, що буде його тримати. Зовні він схожий на ручну зброю та важить приблизно 4 кг (рисунок 4.2). Пристрій здатний блокувати на відстані одного кілометра сигнали GSM, 3G, LTE і ставити перешкоди на частотах 900 МГц, 2,4, 5,2- 5,8 ГГц.

Рис. 4.2 – антидрон рушниця REX-1

4.3. Aerosnare

Це пристрій (рис. 4.3), який забезпечує фізичну можливість захоплення дрона для поліції та силовиків, які вже експлуатують власні дрони. AeroSnare надійно приєднується до будь-якого дружнього дрона. Пристрій виконує постріл по ворожому дрону.Він використовує мотузку та парашут, які прикріплені до дружнього дрону.

Рис. 4.3 - **Aerosnare**

4.4. SkyFence

Це система пов’язаних між собою пристроїв (рис. 4.4), які формують «електронну стіну», що простягається на 500 метрів у небо. Пристрої глушать ворожі дрони і вони не можуть перелетіти через «стіну» до охороняємої території .

Рис. 4.4 - SkyFence

4.5.Kaspersky Antidrone

Це програмне забезпечення, яке можна підключити до обчислювального модулю(рис. 4.5). Також для роботи потрібно підключити будьякий пристрій, що сканує простір над потрібною зоною – камеру, лідар, радар, акустичний сенсор. Додатково можна підключити IPTV-камери, які вже використовуються на охороняємому об'єкті

Рис. 4.5 - Kaspersky Antidrone

4.6. Anduril Roadrunner

Дрон винищувач із двома турбореактивними двигунами (рис 2.25) існує у двох варіантах. Базова версія здатна нести корисне навантаження для виконання різних завдань, а Roadrunner-M призначений для перехоплення безпілотників підривом бойової частини.

Рис. 4.6 Anduril Roadrunner

4.7. DroneShield-DroneSentinel

Одразу дві противодронні системи (рис. 4.7) - DroneSentinel, здатну виявити

БЛА-порушник, і DroneSentry, готову заглушити керуючий сигнал і направити дрон назад до оператора (як варіант - змусити апарат сісти в безпечному режимі).
Дальність дії системи - приблизно 2 км. Власник отримує повідомлення SMS, електронною поштою або за допомогою наявних систем безпеки.

Рис. 4.7 - DroneShield-DroneSentinel

Висновки до розділу

У цьому розділі було проаналізовано найпоширеніші існуючі рішення, що використовуються для боротьби із ворожими дронами. Вони дозволяють виявляти та знешкоджувати їх за різними механізмами.

На даний момент немає універсальної системи, яка гарантувала б стовідсотковий захист від безпілотних літальних апаратів (БПЛА). Кожен об'єкт відрізняється своїми унікальними характеристиками, інфраструктурою та розташуванням на місцевості. Тому для досягнення

максимального рівня захисту від БПЛА необхідно впроваджувати індивідуальні рішення, які враховують розмір об'єкта та різноманітні системи політики безпеки.
Розробка ефективних заходів безпеки передбачає адаптацію до конкретного середовища та особливостей об'єкта. Урахування різноманітних аспектів, таких як географічне положення, фізична конфігурація об'єкта та місцева інфраструктура, дозволяє створювати індивідуальні стратегії захисту.Важливим аспектом є розуміння того, що ідеальний захист від БПЛА непрактичний, і ефективність заходів безпеки може бути досягнута через інтегрований підхід. Використання різних технологій, таких як радіочастотний аналіз, візуальні сенсори та системи машинного навчання, може утворити комплексну систему, яка мінімізує ризик проникнення БПЛА та забезпечує ефективний захист. Однак важливо постійно вдосконалювати ці технології та адаптувати їх до змінюючихся умов і загроз.
На основі аналізу існуючих рішень було вирішено створити систему, яка комбінує режими боротьби із ворожими дронами:
а) використовувати локатор та радіочастотні методи для дистанційного виявлення дрона та використання візуальних сенсорів для розпізнання моделі та траекторії руху, використовуючі методи машинного навчання

б) нейтралізація за допомогою Battelle DroneDefenders.

Користувач системи матиме змогу обирати режим протидії самостійно. Завдяки двом режимам, у випадку, якщо один із них не спрацює
– буде активовано інший режим.

У системі існує два методи виявлення дронів: локатор, та виявлення за допомогою комп’ютерного зору. Для цього камера відсилає до обчислювального центру зображення, яке аналізується комп’ютерним зором. Після цього активується один із режимів протидії дронам.

5.1 Функціональний Розбір системи

Наземний пристрій забезпечує свою роботу за допомогою блока живлення, який постачає електроенергію для обчислювального модулю, камери, модуля глушіння та локатора.
Передавач локатору ініціює надсилання керуючого сигналу до магнетрону, який виробляє високочастотні імпульси. Дуплексер перемикає локатор в режим антени, дозволяючи передати

високочастотні імпульси через неї. При отриманні відбитого сигналу антеною, дуплексер в режимі передавача направляє цей сигнал до демодулятора. Демодулятор передає отриманий сигнал обчислювальному блоку, що далі передає дані про знайдені локатором повітряні об'єкти процесору.

Камера відправляє відеопотік до процесора, який аналізує його, розкладаючи на зображення. За допомогою комп'ютерного зору процесор розпізнає на цих зображеннях літаючі об'єкти. Далі нейтралізація за допомогою напрвленного пострілу Battelle DroneDefenders.

5.2 Опис системи

Наземний пристрій включає в себе компоненти, такі як обчислювальний модуль, камера, локатор, модуль глушіння та блок живлення. Обчислювальний модуль відповідає за виконання обчислювальних операцій за допомогою процесора, передачу та прийом сигналів, а також вміщує в собі WiFi-модуль. Він також виконує сканування зображень, які отримує від камери за допомогою комп'ютерного зору.

Камера використовується для трансляції зображень небесного простору до обчислювального центру.

Локатор використовується для виявлення повітряних об'єктів, а також для визначення їхньої дальності та геометричних параметрів. Метод роботи локатора ґрунтується на випромінюванні радіохвиль та реєстрації їх віддзеркалень від об'єктів. Складається з передавача, дуплексера, антени та приймача.

Модуль глушіння використовується для переривання зв'язку між ворожими дронами та їхнім пультом управління. Він передає інтенсивний білий шум на тих же радіочастотах, на яких дрони спілкуються. Складається з керуючого пристрою, джерела перешкод, підсилювача та антени.

DroneDefenders протидіє БПЛА, використовуючи руйнівні радіохвилі для нейтралізації дрону. Противодронні рушниці нешкідливі для будь-яких пристроїв, крім дронів. Ультрасучасний дизайн дозволяє їм безпечно і під контролем відключати дрони.

Сервер відповідає за зберігання даних про знешкодження дронів . Складається з мережевої карти, процесору та бази даних.

5.3 ОПИС АЛГОРИТМУ РОБОТИ СИСТЕМИ

1. Ініціалізація системи:

Запуск наземного пристрою та всіх компонентів, включаючи локатор, обчислювальний модуль,

камеру, модуль глушіння та блок живлення.

2. Виявлення повітряних об'єктів локатором:

Локатор відправляє сигнал у небесний простір та сприймає відбитий сигнал, визначаючи наявність літаючих об'єктів.

3. Передача інформації від локатора до обчислювального модуля:

Приймач передає інформацію щодо відлуння до обчислювального модуля, який вирішує, чи виявлено літаючий об'єкт.

4. Робота камери та передача зображень до обчислювального модуля:

Камера надсилає зображення небесного простору до обчислювального модуля.

5.Аналіз зображень та розпізнавання об'єктів:

Обчислювальний модуль активує нейромережу, яка аналізує зображення та розпізнає об'єкти на ньому.

6. Рішення щодо того, чи знайдений об'єкт є дроном:

Нейромережа вирішує, чи ідентифікований об'єкт є дроном.

7. Перевірка режиму знешкодження за замовчуванням:

Система перевіряє, який режим знешкодження встановлено за замовчуванням.

8. Якщо знешкодження не автоматичне:

Система отримує від користувача відповідь.

9.Перевірка згоди користувача на знешкодження:

Система перевіряє, чи користувач надав згоду на знешкодження.

10. Застосування методу знешкодження:

Система вирішує, як нейтралізує БПС.

11. Прийняття рішення щодо знешкодження:

Система приймає рішення щодо того, чи було дрон знешкоджено.

12. Завершення роботи:

Якщо дрон успішно знешкоджено, це означає завершення роботи системи.

5.3.1 Реалізація виявлення БПС

Впровадження системи розпізнавання дронів включає важливий компонент, що реалізований за допомогою комп’ютерного зору та локатора. Локатор проводить сканування небесного простору, працюючи паралельно з камерою, яка здійснює обертання, робить знімки простору та передає

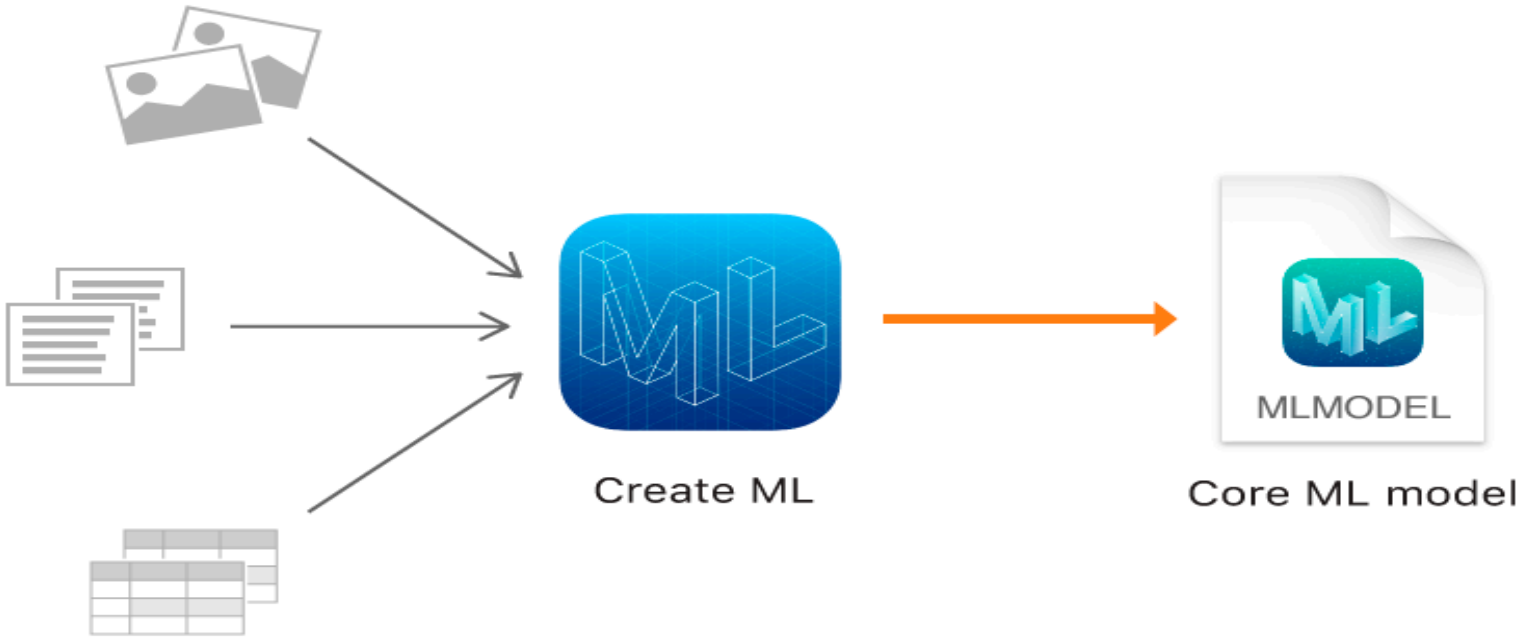
інформацію обчислювальному модулю. Отримані зображення аналізуються за допомогою комп’ютерного зору. Такий підхід сприяє підвищенню точності виявлення, оскільки два модулі працюють одночасно.

5.3.1.1 Локатор

Локатор (рис. 5.1) складається з наступних елементів:

а) передавача;

б) антени;

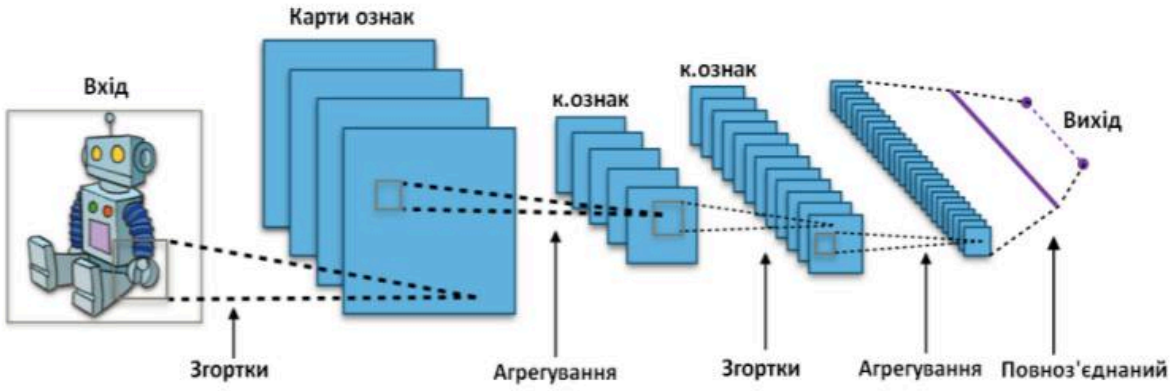


в) дуплексера;

г) приймача.

Основні частини магнетрона:

1 — катод; 2 — анодний блок, 3 — вивід високочастотної енергії



Архітектура згорткової нейронної мережі

Рис. 5.1 - локатор

Функція передавача полягає у створенні високочастотних імпульсів, здійснюючи їх генерацію за допомогою внутрішнього магнетрону. Дуплексер взаємодіє з передавачем та антеною, дозволяючи антені висилати напрямок радіохвиль. Радіохвилі відбиваються від дрона, а їхнє відлуння повертається назад. Антена виконує функції як передавача, так і приймача, черговою відправкою та прийманням радіохвиль. Робота дуплексера полягає в перемиканні між режимами передачі сигналів та прийому відлуння. Сигнал, що був прийнятий, демодулюється та передається до обчислювального центру, де визначаються координати об'єкта.

5.3.1.2 Магнетрон

Локатор використовує радіохвилі, які генеруються за допомогою магнетрона. Ці радіохвилі подібні до світлових, але мають довшу довжину і нижчі частоти. Магнетрон генерує мікрохвилі, які використовуються для виявлення дронів.Магнетрон є потужною електронною лампою, яка виробляє мікрохвилі при взаємодії електронного потоку з магнітним полем. Він є великим і потужним у порівнянні з мікрохвильовою піччю, оскільки повинен посилати хвилі на більшу відстань.Магнетрон складається з анодного блока, який включає товстий полий мідний циліндр з порожнинами, що створюють кільцеву систему резонаторів. Катод, що проходить уздовж центральної осі аноду, підключений до джерела живлення. Магнетрон генерує мікрохвилі, що випромінюються в простір через антену(схема 5.2).За допомогою магнетрона локатор створює мікрохвилі, які використовуються для виявлення та визначення координат дрона.

Схема 5.2 – основні частини магнеторна

5.3.1.3 Антена

Антена складається з металевих струмопровідних елементів, які з'єднані з магнетроном. У режимі передачі струм протікає по антені, створюючи електромагнітне поле. Це поле утворює електромагнітну хвилю, яка випромінюється в простір.У режимі прийому антена отримує електромагнітні хвилі, які потім підсилюються та демодулюються приймачами.

Використовується параболічна антена, яка володіє властивістю відбивати електромагнітні хвилі від рефлектора.

Параболічна антена обертається на 360 градусів, що дозволяє виявляти ворожі дрони на великій площі. Коли сигнали контактують з дронами, вони відбиваються або розсіюються, а деякі поглинаються і проникають у ціль.

5.3.1.4 Дуплексер

Дуплексер забезпечує перемикання антени між режимами передачі сигналів та прийому відлуння. У режимі передачі антена не може приймати, і навпаки .Дуплексер має три порти для підключення антени, радіоприймача і передавача, що широко використовується для створення дуплексних ретрансляторів.Робота дуплексера (схема 5.3) ґрунтується на принципі пропускання сигналу однієї частоти та блокування іншої.

Таким чином, в приймальному плечі антени корисний сигнал вільно проходить до приймача, інший сигнал блокується. У передавальному плечі сигнал від передавача досягає антени, а його шуми в області прийомних частот блокуються.

Схема 5.3 – схема роботи дуаплексеру

5.3.1.5 Приймач

Приймач виконує функцію підсилення та демодуляції отриманих антеною відбитих сигналів. Після обробки сигналу, приймач направляє його до обчислювального модулю, який визначає відстань до дрону. Визначення відстані здійснюється на основі часу, який пройшов між відправленням імпульсу та отриманням відлуння. Це визначення точно розраховується за допомогою формули, враховуючи, що швидкість розповсюдження радіолокаційного сигналу є постійною.

$$s = (c*t)/2, \quad (5.4)$$

де s – відстань від локатору до дрону (м), c – швидкість світла (м/с), t – час, що пройшов між передачею імпульсу та отриманням відлуння (с).

5.3.2. Комп’ютерний зір

Глибиною у контексті роботи модуля комп’ютерного зору є відстань між розпізнаними об’єктами та камерою безпілотного літального апарату. Відстань можна буде вичислити за допомогою нейронної мережі, що буде повертати прогноз відстаней базуючись на зсуві зображення попіксельно між двома кадрами відеопотоку. Таким чином модуль комп’ютерного зору повинен вирішувати задачу розпізнання глибини оточення БПЛА. Тобто алгоритм роботи модуля має виконувати наступні кроки:

1. Отримання відеопотоку.
2. Оброблення відеопотоку таким чином, щоб на виході отримувати карту глибини зображення.
3. Виведення оброблених зображень.

Алгоритм роботи модуля комп’ютерного зору представлено на рис. 5.5.

рис. 5.5 Алгоритм роботи модуля комп’ютерного зору

Камера високої роздільної здатності з оглядом у 360° надсилає зображення простору до обчислювального модулю. Застосовуючи комп'ютерний зір, модуль аналізує зображення для виявлення рухливих об'єктів на небі, визначаючи, чи є серед них дрон.Для навчання обчислювального модулю розпізнавання об'єктів, що передаються камерою, проведено аналітичну роботу зі збору даних для тренування моделі. Використовується технологія нейромережі, що реалізує програмну імплементацію структур людського мозку. Нейромережі представляють собою систему взаємодіючих штучних нейронів. Кожен нейрон мережі опрацьовує сигнали, які отримує та надсилає іншим нейронам. Ці процесори, об'єднані великою мережею, здатні вирішувати складні завдання завдяки керованій взаємодії.Нейромережі не програмуються, а навчаються. Можливість навчання полягає в встановленні оптимальних зв'язків між нейронами. Внаслідок цього мережа здатна розпізнавати об'єкти, навіть якщо їхні дані відсутні в навчальній вибірці, або якщо дані частково спотворені чи "зашумлені".

Для успішного навчання нейромережі у розпізнаванні об'єктів та зображень потрібно велике число прикладів з правильними відповідями або спеціальної структури нейронної мережі, яка враховує особливості завдання. Система виявлення дронів використовує згорткову нейронну мережу, оскільки цей тип мережі продемонстрував найкращі результати у цій сфері. Це пов'язано

з тим, що згорткові нейронні мережі ефективно обробляють зображення великих розмірів, такі як високоякісні знімки від камер. Такі камери важливі для можливості системи розглядати дрони у небесному просторі.Згорткові нейронні мережі (схема 5.6) забезпечують часткову стійкість до змін масштабу, зсувів, поворотам, зміні ракурсу і іншим спотворень.

Схема 5.6 – Архітектура згорткової нейронної мережі

Згорткові нейронні мережі об'єднують три архітектурні ідеї, для забезпечення інваріантності до зміни масштабу, повороту зрушення і просторовим спотворенням:

а) локальні рецепторні поля (забезпечують локальну двовимірну зв'язність нейронів);

б) загальні вагові коефіцієнти синапсів (забезпечують детектування деяких рис в будь-якому місці зображення і зменшують загальне число вагових коефіцієнтів); в) ієрархічну організацію з просторовими підвибірками

Група методів для виявлення та надійного визначення об'єктів на зображеннях, зокрема

безпілотних літальних апаратів (БПЛА).
Один із передових методів виявлення об'єктів, зокрема БПЛА, - Метод Віоли-Джонс (Viola-Jones object detection). Цей метод використовує каскадний класифікатор для оперативного та точного визначення об'єктів у реальному часі. Він відомий своєю високою швидкодією та точністю, навіть при різних умовах освітлення та поворотах об'єкта.
Метод гнучкого порівняння на графах (Elastic graph matching) є ще однією важливою технікою для виявлення об'єктів, яка базується на порівнянні графів для опису їх біометричних особливостей. Цей метод дозволяє враховувати зміни в структурі об'єкта, забезпечуючи високу точність визначення.
Метод опорних векторів (Support Vector Machines, SVM) є ефективною технікою для виявлення об'єктів на зображеннях. Він володіє високою стійкістю до перенавчання та швидкодією, забезпечуючи точне розпізнавання об'єктів.Нейромережеві методи, хоча вимагають складної процедури налаштування, можуть досягти високої точності виявлення об'єктів, включаючи БПЛА. Однак вони також відрізняються високою обчислювальною складністю.
Обрання конкретного методу виявлення БПЛА залежить від конкретних вимог системи та умов експлуатації. Враховуючи високу обчислювальну складність деяких методів, важливо збалансувати точність та ефективність для досягнення оптимальних результатів у конкретних сценаріях використання

5.3.3 Тренування моделі

Тренування моделі комп'ютерного зору для розпізнання безпілотних літальних апаратів (БПЛА або дронів) включає декілька етапів. Нижче наведено загальний опис процесу та можливі інструменти, які можуть бути використані:
Збір та Підготовка Даних:
Зібрати набір даних, який містить зображення дронів та можливої області їхньої розташованості.
Розмітити області, де знаходяться дрони (bounding boxes) на зображеннях.
Формування Структури Даних:
Перетворити дані у формат, придатний для використання в обраному інструменті, наприклад, у формат TFRecord для TensorFlow.
Вибір Архітектури Моделі:
Вибрати архітектуру моделі. Залежно від розміру та складності ваших даних, ви можете

використовувати вже популярні архітектури, такі як Faster R-CNN, YOLO (You Only Look Once), або SSD (Single Shot Multibox Detector).

Вибір та Налаштування Інструменту для Тренування:

Використовуйте інструменти для тренування моделі, такі як TensorFlow Object Detection API або PyTorch, якщо ви використовуєте TensorFlow чи PyTorch, відповідно.

Налаштуйте конфігураційні файли, вказуючи архітектуру моделі, шляхи до даних, гіперпараметри тощо.

Тренування Моделі:

Здійсніть тренування моделі, використовуючи підготовлені дані та конфігурації.

Використовуйте GPU, якщо це можливо, для прискорення процесу тренування.

Оцінка та Валідація:

Використовуйте валідаційний набір для оцінки ефективності моделі, звертаючи увагу на показники, такі як точність та втрати.

Тонка Налагодження та Оптимізація:

Використовуйте тонке налаштування гіперпараметрів для покращення результатів моделі.

Тестування та Впровадження:

Тестуйте модель на тестовому наборі даних.

Розгорніть модель для використання в реальних умовах для розпізнавання дронів.

Моніторинг та Підтримка:

Моніторте ефективність моделі в реальному часі та вчасно проводьте оновлення.

Застосовуючи інструменти, такі як TensorFlow, PyTorch, або вже готові API для розпізнавання об'єктів, ви зможете спростити процес тренування моделі для розпізнавання безпілотних літальних апаратів.

Для тренування нейронної мережі, що використовується в системі, було використано програму CreateML – потужний інструмент для роботи з машинним навчанням.

Результатом є навчена модель, яка виникає внаслідок застосування алгоритму машинного навчання до набору навчальних даних. Моделі є компактними (близько 3 Мб), що дозволяє їх легко вбудовувати в проекти.Під час навчання з використанням зображень доступні два основних шаблони: Image Classifier (класифікатор зображень) і Object Detector (детектор об'єктів).Image Classifier використовується для класифікації зображень за їх вмістом. Після навчання моделі

можна ідентифікувати окремий об'єкт на зображенні та призначити його конкретному класу. Наприклад, це може бути використано для розпізнавання видів тварин або різних видів рослин на фотографіях. У шаблоні Image Classifier від CreateML використовується техніка трансферного навчання (схема 5.5).

Трансферне навчання дозволяє комбінувати заздалегідь навчену модель з новими даними, що дозволяє навчати моделі на обмеженій кількості зображень.Зображення для Image Classifier повинні мати розмір не менше 299 на 299 пікселів. Набори для навчання повинні включати не менше 10 зображень для кожного класу, бажано більше. Приблизно 80% зображень використовуються для навчання, а решта 20% – для тестування. Крім того, зображення для навчання не повинні дублюватися серед тих, що використовуються для тестування. Назви папок

для навчання використовуються як ідентифікатори для відповідних класів при використанні моделей.

Схема 5.5 – техніка навчання Create ML

Для тренування моделі комп'ютерного зору створено набір даних з 296 фотографій літаючих об'єктів, таких як гелікоптери, дрони, літаки, планери та дирижаблі. Зображення у шаблоні Image Classifier завантажувалися із використанням анотацій, які містять інформацію про розташування літаючого об'єкта на зображенні. Для цього використовувався сервіс IBM Cloud Annotations, який дозволяє позначати певні об'єкти на фотографіях шляхом обведення їх прямокутником та надання їм назви.

Файл із зображеннями та анотаціями було експортовано як архів для подальшого використання в програмі CreateML.

Після підготовки теки з зображеннями та анотацією, можна приступати до тренування моделі в середовищі CreateML. Для цього обирається шаблон Image Classifier, та створюється новий проект.

У вікні проекту в інспекторі ліворуч відображається інформація про проект та його назву, що можна редагувати. Далі в Model Sources містяться всі моделі, що використовуються в проекті. У секції Training Data додаються зображення для тренування, у Validation Data можна включити зображення для перевірки моделі, а в Testing Data додаються зображення для тестування моделі,

які не використовувалися під час тренування.
Розділ Parameters дозволяє встановити максимальну кількість ітерацій, виконаних над одним зображенням під час тренування моделі. У секції Augmentations можна вибрати ефекти, які застосовуються до зображень.
Після налаштувань кнопкою Train запускається процес тренування. В розділі Results можна переглядати оцінку ефективності моделі після завершення тренування. У данному випадку, модель добре класифікувала зображення з тренувального набору (93%) та перевірочного набору (54%). Загальна точність після тестування склала 81%.
Для візуалізації роботи моделі, створено застосунок на iOS в середовищі XCode, який використовує попередньо натреновану модель. Застосунок аналізує зображення з камери в режимі реального часу та відображає результат аналізу на екрані.Наприклад, застосунок може розпізнати дрон на зображенні, обведений червоним кольором. Результати можуть відрізнятися в залежності від розпізнаних об'єктів, таких як літак, гелікоптер, планер чи дирижабль, які будуть позначені зеленим кольором.Для альтернативного методу розпізнавання використовується локатор, що генерує радіохвилі та виявляє ворожі дрони на основі їх відбивань. Також використовується комп'ютерний зір, де камера з високим розширенням та кутом огляду у 360° надсилає зображення на обчислювальний модуль, який аналізує його для визначення рухомих об'єктів, таких як БПС.

5.4 Ралізація нейтралізації БПС

Ми використовуємо антидронову рушницю Battelle DroneDefenders, яка є ефективним методом глушіння і безпечною для всіх пристроїв, окрім БПС. БПС має приймально-передавальний пристрій, який використовується для визначення місцезнаходження та установки зв'язку з пультом керування. Пульт передає команди, а дрон надсилає відео. Рушниця генерує сигнали на тих самих частотах, але із щільнішою хвилею, ніж зв'язок між дроном та пультом. При потраплянні дрона у зону впливу рушниці він втрачає можливість передавати інформацію та отримувати команди. Це може призводити до аварійної посадки дрона або його зіткнення з вітром, особливо в погіршених погодних умовах.Усі БПС, будь то заводські чи виготовлені з фабричних компонентів, працюють у певному діапазоні частот та відповідають стандартам, що надає можливість нейтралізувати різні типи БПС, включаючи літакоподібні дрони. Додатково, здійснення перешкодження сигналу GPS за допомогою окремого тригера може бути використано

для блокування руху БПЛА або для захоплення його під час повернення додому.Система використовує простий інтерфейс — всього лише одну кнопку, і для її використання не потрібні високі навички стрільця. Точність важлива лише у межах приблизно 30° кута хвилі, і діапазон впливу становить до 3,5 км. Після використання рушниці вона надає тактильні вібрації для сигналізації режиму заглушення, а також має функцію логування для збору інформації. Дрон після впливу переходить до протоколу безпеки та виконує посадку, а в разі активного протоколу "повернутися додому" блокується GPS сигнал і чекається вимушена посадка. За потреби можна вилучити або вивчити дані з ворожого БПС для подальшого аналізу та вдосконалення.

ВИСНОВКИ

У даному розділі була детально розглянута робота локатору та впроваджено ефективний метод розпізнавання дронів - за допомогою комп'ютерного зору. Передавач локатору, використовуючи магнетрон, генерує імпульсні радіохвилі, а антена обертається на 360%, дозволяючи виявляти дрони на великих площах. Дуплексер ефективно перемикає антену між режимами передачі та прийому, забезпечуючи надійну роботу системи.

Унікальний підхід до розпізнавання дронів за допомогою комп'ютерного зору дозволяє виявляти рухомі об'єкти на небі та ефективно розпізнавати їх як дрони чи інші об'єкти. Важливо відзначити, що розроблений застосунок, який використовує цей метод, може служити як практичний інструмент для виявлення та моніторингу дронів у реальному часі.

Такий комплексний підхід до виявлення дронів, поєднуючи радіолокаційні та оптичні методи, створює надійну та ефективну систему безпеки. Інтеграція цих технологій покликана підвищити точність та швидкість виявлення дронів, роблячи систему високоефективною в реальних умовах експлуатації.

Проект успішно розроблено, представляючи систему повітряної боротьби із дронами. У процесі виконання роботи було здійснено порівняльний аналіз різних аналогів системи, сформовано концепцію, детально розглянуто принципи роботи та вибрано компоненти системи.

Описано процес тренування нейромережі, яка здатна розпізнавати об'єкти у зоні огляду камери системи. Розроблено систему, що включає наземну установку (обчислювальний модуль, локатор, модуль глушіння, акумулятор та камера), сервер та антидрон-рушницю.

Відзначається передовістю системи через повну автономність виявлення, протидії за допомогою антидрон рушниці та використання комп'ютерного зору для розпізнавання. Гнучкість

використання, яка дозволяє встановлювати систему як стаціонарну або на транспорт, робить її відмінною. Можливості вдосконалення в майбутньому з урахуванням особливостей новітніх БПС, а також покращення моделі комп'ютерного зору, роблять цю систему ефективною та захищеною.

Майбутні вдосконалення можуть стати фундаментом для подальшого розвитку системи повітряної боротьби із дронами, що надасть їй ще більшу ефективність у протистоянні передовим та різноманітним загрозам.

1)Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В., Анохин М.А. Информационные характеристики звукового излучения малых беспилотных летательных аппаратов// Радиотехника. (Харьков). 2017. Вып. 191. С. 181-187.

2)V. Kartashov, V. Oleynikov, O. Zubkov, S. Sheiko, "Optical detection of unmanned air vehicles on a video stream in a real-time"; The Fourth International Conferenceon Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2019), 9-13 September 2019, Odessa, Ukraine, 4 p.

3)Oleksandr Sotnikov, Vladimir Kartashov, Oleksandr Tymochko, Oleg Sergiyenko, Vera Tyrsa, Paolo Mercorelli, Wendy Flores-Fuentes. Methods for Ensuring the Accuracy of Radiometric and Optoelectronic Navigation Systems of Flying Robots in a Developed Infrastructure. Chapter 16// Machine Vision and Navigation; Editors: Sergiyenko**,** Oleg, Flores-Fuentes**,** Wendy**,** Mercorelli**,** Paolo; pp.537-578.

4)Oleynikov V. N , Zubkov O. V., Kartashov V. M., Korytsev I. V., Babkin S. I., Sheiko S. A. Investigation of detection and recognition efficiency of small unmanned aerial vehicles on their acoustic emission; Telecommunications and Radio Engineering, 2019, Volume 78, Issue 9; pp. 759-770.

5)Kartashov, V., Oleynikov, V., Koryttsev, I., Zubkov, O., Babkin S., Sheiko, S. Processing and Recognition of Small Unmanned Vehicles Sound Signals. 2018 International Scientific-Practical Conference on Problems of Infocommunications. Science and Technology (PIC S and T 2018) – Proceedings, 31 January 2019; pp. 392-396.

6) Kartashov V., Oleynikov V., Koryttsev I., Sheyko S., Zubkov O., Babkin S., Selieznov I. Use of Acoustic Signature for Detection, Recognition and Direction Finding of Small Unmanned Aerial Vehicles; 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 25-29 Feb. 2020; pp. 1-4.

7) https://www.google.com/imgres?imgurl=https%3A%2F%2Fupload.wikimedia.org%2Fwikipedia%2Fcommons%2Fthumb%2F3%2F3c%2FAirship_designed_by_Jean-Baptiste_Marie_Meusnier_de_La_Place.jpg%2F220px-Airship_designed_by_Jean-

8)https://ep3.nuwm.edu.ua/6254/1/05-04-77.pdf

9)https://sprotyvg7.com.ua/wp-content/uploads/2022/04/ВП-7-0003.01-Боротьба-з-БПЛА.pdf

10)https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D0%B8%D0%BE%D0%BB%D0%BE%D0%BA%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D1%82%D0%B0%D0%BD%D1%86%D0%B8%D1%8F

11) Kaspersky Antidrone. URL: https://go.kaspersky.com/antidrone.html (дата звернення: 29.03.2020).

12) Rex-1. URL: https://zala-aero.com/production/means-of-ew/rex-1/ .

13) SkyWall Auto. URL: https://openworksengineering.com/skywall-auto/

14) SkyWall Auto. URL: https://www.unmannedsystemstechnology.com/wpcontent/uploads/2017/09/OpenWorks-Engineering-Skywall300-dronecapture-system-326x159.jpg

15) Aerosnare. URL: https://www.dronedefence.co.uk/products/aerosnare/

16) Sky Fence. URL: https://www.dronedefence.co.uk/products/skyfence/

17)Baptiste_Marie_Meusnier_de_La_Place.jpg&tbnid=shF5PH-4hrYzIM&vet=12ahUKEwip5pf2vJ6DAxVvi_0HHfWLB5UQMygFegQIARBQ..i&imgrefurl=https%3A%2F%2Fru.wikipedia.org%2Fwiki%2F%25D0%2598%25D1%2581%25D1%2582%25D0%25BE%25D1%2580%25D0%25B8%25D1%258F_%25D0%25B2%25D0%25BE%25D0%25B7%25D0%25B4%25D1%2583%25D1%2585%25D0%25BE%25D0%25BF%25D0%25BB%25D0%25B0%25D0%25B2%25D0%25B0%25D0%25BD%25D0%25B8%25D1%258F&docid=P4m_dEe1UZKX2M&w=220&h=147&q=%D0%B0%D0%B5%D1%80%D0%BE%D1%81%D1%82%D0%B0%D1%82&hl=ru&ved=2ahUKEwip5pf2vJ6DAxVvi_0HHfWLB5UQMygFegQIARBQ

18)What is radar and how is it used to track aircraft? URL: https://www.abc.net.au/science/articles/2014/03/17/3964782.html

19)Радіоглушіння. URL: https://uk.wikipedia.org/wiki/Радіоглушіння

20) Шумотрон. URL: https://uk.wikipedia.org/wiki/Шумотрон

21) Усилитель. URL: https://ru.wikipedia.org/wiki/Усилитель

22) Нейронні мережі https://www.ibm.com/cloud/learn/neural-networks

23) Neural Network Models Explained https://www.seldon.io/neural-network-models-explained

24) 9 Types of Neural Networks: Applications, Pros, and Cons https://www.knowledgehut.com/blog/data-science/typesof-neural-networks

25) TensorFlow – однослойный персептрон https://coderlessons.com/tutorials/mashinnoe-obuchenie/vyuchittensorflow/tensorflow-odnosloiny

i-perseptron
26)Що таке багатошаровий перцептрон https://uk.theastrologypage.com/multilayer-perceptron
27) What are Radial Basis Functions Neural Networks?
https://www.simplilearn.com/tutorials/machine-learningtutorial/what-are-radial-basis-functions-neural-networks
28) 5 Different Types of Neural Networks
https://www.projectpro.io/article/5-different-types-of-neural-networks/431
29)Introduction to Recurrent Neural Network
https://www.geeksforgeeks.org/introduction-to-recurrent-neural-network
30) Electronic or Mechanical: Which Paintball Gun Is Right for You? URL:
https://www.liveabout.com/electronic-versus-mechanical-guns2565831
31) Cavity magnetron. URL: https://en.wikipedia.org/wiki/Cavity_magnetron
32) Основні частини магнетрона. URL:
http://ed.kpi.ua/wpcontent/uploads/Mastertheses/2019/Ichenskyi_V.pdf
33) Antenna. URL: https://en.wikipedia.org/wiki/Antenna_(radio)
34) Зеркальная антенна. URL: https://ru.wikipedia.org/wiki/Зеркальная_антенна
35) When and where to use a duplexer. URL:
https://blog.taitradio.com/2014/05/13/when-and-where-to-use-a-duplexer/
36) Зображення схеми роботи дуплексеру у локаторі. URL:
https://upload.wikimedia.org/wikipedia/commons/thumb/a/af/Bsp_Duplexeng.svg/440px-Bsp_Duplex-eng.svg.png
37) Штучна нейронна мережа. URL: https://uk.wikipedia.org/wiki/Штучна_нейронна_мережа
38) Згорткова нейронна мережа. URL: https://uk.wikipedia.org/wik