

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Інфокомунікацій

(повна назва)

Кафедра

Інформаційно-мережної інженерії

(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)

(рівень вищої освіти)

(позначення документа)

«Дослідження засобів протидії безпілотним літальним апаратам»

(тема)

Виконав: студент II курсу, групи ІМІм 21-1

Коновалова К.Ю.

(прізвище, ініціали)

Спеціальність 172 «Телекомунікації та

радіотехніка»

(код і повна назва напрямку)

Тип програми освітньо-професійна

(освітньо-професійна або освітньо-наукова)

Освітня програма інформаційно-мережна
інженерія

(повна назва освітньої програми)

Керівник доц. Іваненко С. А.

(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри

(підпис)

Безрук В.М.

(прізвище, ініціали)

2022 р.

Не містить відомостей заборонених до відкритого публікування.

Студент

/Коновалова К.Ю./

Керівник

/Іваненко С.А./

Харківський національний університет радіоелектроніки
(повна назва вищого навчального закладу)

Факультет Інфокомунікацій
Кафедра інформаційно-мережної інженерії
Рівень вищої освіти другий (магістерський)
Спеціальність 172 «Телекомунікації та радіотехніка»
Тип програми освітньо-професійна
Освітня програма інформаційно-мережна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри ІМІ

проф. Безрук В.М.
“ ” 2022 року

**З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Коноваловій Катерині Юріївні

(прізвище, ім'я, по батькові)

1. Тема роботи «Дослідження засобів протидії безпілотним літальним апаратам»

керівник роботи к.т.н. доц. Іваненко Станіслав Андрійович

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ВНЗ від « 21 » жовтня 2022 року № 1376Ст

2. Строк подання студентом роботи 22 грудня 2022 р.

3. Вихідні дані до роботи Провести аналіз та загальну характеристику БпЛА на сучасному етапі розвитку. Розглянути демаскуючі ознаки, методи виявлення та протидії БпЛА. Провести порівняльну характеристику цих методів. Дослідити пристрої протидії таким літальним апаратам, котрі керуються за допомогою протоколу WI-FI, та використовують супутникове позиціонування.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Вступ

1. Аналіз та загальна характеристика БпЛА

2. Аналіз методів виявлення БпЛА

3. Аналіз методів протидії БпЛА

4. Запропоновані методи для протидії БпЛА

Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Слайди у форматі Power Point (назва та мета роботи, визначення БпЛА, управління БпЛА, демаскуючі ознаки БпЛА, основні методи виявлення БпЛА, малогабаритні, радіомоніторинг БпЛА, глушіння БпЛА, GPS-spoofing, перехоплення управління, протидія квадрокоптерам із керуванням за WI-FI, генератор завад GPS, результати роботи, спрямована антена, висновки тощо).

КАЛЕНДАРНИЙ ПЛАН

№ з/П	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	24.10 – 26.10.22	
2	Аналіз літератури за темою роботи.	27.10 – 30.10.22	
3	Виконання розділу 1	01.11 – 06.11.22	
4	Виконання розділу 2	07.11 – 15.11.22	
5	Виконання розділу 3	16.11 – 24.11.22	
6	Виконання розділу 4	25.11 – 15.12.22	
7	Оформлення пояснювальної записки	16.12 – 20.12.22	
8	Оформлення презентаційного матеріалу,		
9	підготовка до захисту у ЕК	21.12 – 22.12.22	

Дата видачі завдання 24.10.2022 р.

Студент _____ (підпис) _____ (Коновалова К.Ю.) (прізвище та ініціали)

Керівник роботи _____ (підпис) _____ (Іваненко С.А.) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 59с., 27 рис., 4 табл., 16 джерел, 1 додаток

Об'єкт роботи – засоби протидії безпілотним літальним апаратам.

Мета роботи – розробка та дослідження ефективності відносно простих засобів протидії безпілотним літальним апаратам, для приватного користування.

В роботі виконаний аналіз методів виявлення та протидії безпілотним літальним апаратам, визначені демаскуючі ознаки останніх. На практиці були перевірені два засоби протидії даним пристроям: WI FI-джаммер, та постановник завад супутникової навігації. Отримані результати їхньої роботи, свідчать про ефективність їхнього використання.

БпЛА, ПРОТИДІЯ, WI-FI, GPS, ГЛУШІННЯ, DJI SPARK.

THE ABSTRACT

Explanatory note: 59p., 27 fig., 4 tables, 16 sources, 1 appendix

The object of research is means of countering unmanned aerial vehicles.

The purpose of the work is to develop and study the effectiveness of relatively simple countermeasures against unmanned aerial vehicles for private use.

The work analyzes the methods of detecting and countering unmanned aerial vehicles. Unmasking signs of the latter are identified. In practice, two means of combating these devices were tested: a WI FI jammer and a satellite navigation jammer. The obtained results of their work testify to the effectiveness of their use.

UAV, COUNTERACTION, WI-FI, GPS, JAMMING, DJI SPARK.

ЗМІСТ

	С.
ПЕРЕЛІК СКОРОЧЕНЬ	8
ВСТУП	9
1 АНАЛІЗ ТА ЗАГАЛЬНА ХАРАКТЕРИСТИКА БпЛА.....	10
1.1 Класифікація та галузі застосування.....	10
1.2 Базова конструкція та принципи управління	12
1.3 Нормативна база, щодо використання у світі	15
2 АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ БпЛА	20
2.1 Демаскуючі ознаки БпЛА	20
2.2 Методи виявлення БпЛА.....	22
3 АНАЛІЗ МЕТОДІВ ПРОТИДІЇ БпЛА	26
3.1 Глушіння БпЛА	26
3.2 Підміна GPS-координат.....	29
3.3 перехоплення управління	30
3.4 Фізична протидія.....	31
3.5 Порівняльна характеристика методів	31
4 ЗАПРОПОНОВАНІ МЕТОДИ ДЛЯ ПРОТИДІЇ БПЛА.....	32
4.1 Протидія квадрокоптерам із керуванням за Wi-Fi ...	32
4.2 Пристрій для глушіння GPS	37
4.3 Розробка спрямованої антени для підвищення якісних характеристик запропонованих пристроїв	41
4.4 Вибір оптимального пристрою протидії квадрокоптерам для приватного використання.....	Ошибка! Закладка не определена. 42
ВИСНОВКИ.....	45
ПЕРЕЛІК ПОСИЛАНЬ	46
ДОДАТОК А СЛАЙДИ ПРЕЗЕНТАЦІЇ.....	48

ПЕРЕЛІК СКОРОЧЕНЬ

БпЛА – безпілотний літальний апарат;
ЕМВ – електромагнітне випромінювання;
ЕПР – ефективна площа розсіювання;
РМ – радіомоніторинг;
РЛС – радіолокаційна станція;
ППРЧ – програмна перебудова радіочастоти;
AFIZ – Аеродромна зона польотної інформації;
ATCA – Air Traffic Control Association;
GPS – Global Positioning System;
RTH – Return to Home;
VLOS – Visual Line of Sight;
Wi-Fi – Wireless Fidelity.

ВСТУП

Безпілотні літальні апарати – одні з багатьох пристроїв, котрі об'єднали значну кількість винаходів людства і уособлюють його поточний стан розвитку.

Даний пристрій може виконувати багато різноманітних задач. У сфері розваг дрони за останні два роки стали набагато доступніші і отримали набір серйозних інструментів – камери, диктофон, автопілот. Даний пристрій може проникнути навіть в найбільш важкодоступні місця. За останні роки було продано декілька сот тисяч дронів. Вартість їх стала прийнятною, функціонал виріс, управління стало простішим.

З кожним роком кількість безпілотних літаючих апаратів (БпЛА) суттєво збільшується. Окрім безумовних переваг від їхнього користування ми також отримуємо і певні ризики пов'язані з цим. Перед усім мова йде про безпеку життя та здоров'ю людей, цілісність майна та інфраструктури.

Саме через свою масовість, простоту в керуванні дані пристрої набувають все більшого розповсюдження, а отже і потенційна шкода від них також зростає. Тепер такі апарати все частіше можна спостерігати в приватних руках в тому числі і звичайних споживачів електроніки.

Саме тому у цій роботі з метою захисту, в тому числі і персональної інформації, пропонується дослідження та розробка пристроїв, які реалізують методи протидії БпЛА.

1 АНАЛІЗ ТА ЗАГАЛЬНА ХАРАКТЕРИСТИКА БпЛА

1.1 Класифікація та галузі застосування

Розглянемо в цілому, що являє собою даний тип літальних апаратів.

Безпілотний літальний апарат (англ. unmanned aerial vehicle, скор. UAV; або англ. remotely piloted vehicle скор. БпЛА або дрон) — літальний апарат, який може злітати, здійснювати політ і сідати без фізичної присутності пілота на його борту [1].)

Кількість різновидів БпЛА дійсно вражає, оскільки вона визначається тим різноманіттям задач, котрі вони можуть вирішувати та технічними рішеннями, щодо їх реалізації.

Але, не дивлячись на цей факт, в цілому існує два основних типи таких літальних апаратів за принципом польоту:

- літакового типу;
- роторного типу.

До БпЛА літакового типу відносять летюче крило (рис.1.1 (а)) та класичну літакову конструкцію. Дані БпЛА доволі економічні з точки зору витрат енергії для виконання польоту завдяки використанню підйомної сили крила. Час польоту може дорівнювати десятки годин. Використовуються переважно для аеророзвідки, спортивних змагань, виконання польотів за місіями в сільському господарстві і т.д.

ZOHD



Рисунок 1.1 БпЛА типу летюче крило ZOHD Dart 250G (а), та квадрокоптер DJI Mavic 3 (б)

Переважним за кількістю представником роторних БпЛА є квадрокоптер. На поточний час кількість таких пристроїв просто вражає завдяки використанню у багатьох галузях.

Квадрокоптер – БпЛА, що має чотири гвинти, швидкість обертання яких регульована спеціальним польотним контролером, який має стабілізуючі системи для забезпечення аеродинамічної стійкості.

Окрім квадрокоптерів відомі й такі види роторних БпЛА:

- трикоптер (три гвинти) – мультикоптер з специфічною конструкцією, що використовується для розваг, трюків, зйомки на легких камерах;
- гексакоптер (шість гвинтів) та октокоптер (вісім гвинтів) – є найбільш стабільними, важкі і дороговартісні апарати, використовуються для аерозйомок, доставки вантажів, спеціальних задач.

Серед інших типів БпЛА квадрокоптер має наступні переваги:

- краща плавність руху, можливість зависання;
- значна маневреність відносно літакових варіантів;
- значна кількість режимів управління польотами та гнучкість функцій.

Час роботи та дальність польоту дрона залежать від багатьох показників: маси, потужності і енергоспоживання двигунів, ємності батареї, потужності передавачів та чутливості приймача, якості використовуваних антен, тощо. Середній час польоту для роторних БпЛА – це 15-30 хвилин. Середня дальність – 2-3 км. Середня висота – декілька кілометрів.

Галузі застосування БпЛА:

- порятунок людей;
- побутові задачі та розваги;
- комунальні підприємства та заклади (контроль споруд та моніторинг агрегатів);
- військова галузь;
- наука та дослідження;
- картографія за допомогою аерозйомки;

- Захист дикої природи;
- дослідження та попередження негативних природних явищ;
- сільське господарство та будівництво.

БПЛА завжди були надбанням військових, проте останнім часом такі їх представники, як квадрокоптери, завойовують своє місце у різних сферах і цивільного життя. Щодня людство знаходить їм нові застосування, роблячи певні вдосконалення літаючих помічників. Дрони можуть стати такими супутниками людства як і мобільні телефони, тобто в найближчому майбутньому вони можуть стати незамінним атрибутом нашого життя.

1.2 Базова конструкція та принципи управління

Оскільки БПЛА не мають на своєму борту пілота, котрий міг би регулювати параметри літального апарата і таким чином здійснювати пілотування, то розглянемо яким чином відбувається цей контроль. Як правило, керування виконуються дистанційно за допомогою радіоканалу, який пов'язує борт та пульт управління.

На даний час існують наступні можливості з пілотування БПЛА:

- через морські станції управління (розташоване на водній поверхні);
- через мобільні станції (зазвичай автомобільний транспорт);
- стаціонарні пункти управління.

Зазначимо, що різні типи БПЛА (залежно від класу, конструкції, призначення), мають різні можливості щодо навігації та контролю.

До складу безпілотного комплексу входять такі підсистеми регулювання, координації польотів (комплекс Pioneer ВМС США) [2]:

1. Сама станція зазвичай включає такі компоненти:

- лінія «вниз» від БПЛА до пункту управління;
- лінія «вгору» від пункту управління до БПЛА;
- системи прийому та обробки зображення на дисплеї;

- системи прийому тепловізійного та інфрачервоного зображення
- пульт керування пілота (включаючи системи програмування польотів та польотного завдання)

2. До комплексу підсистем управління на стороні БпЛА входять:

- пристрої одержання відео та фото інформації;
- системи отримання сигналів від супутників (глонас/GPS);
- пристрої телеметрії та передачі на пункт управління інформації щодо параметрів положення судна у просторі, швидкості польоту, тривалості польоту тощо;
- бортовий комп'ютер;
- підсистеми для зберігання польотної інформації, а також відео та фото інформації [2].

Існують наступні режими радіокерування БпЛА: ручний режим, напіваавтоматизований режим, автоматизований режим.

Ручний режим керування БпЛА – повністю здійснюється оператором за допомогою дистанційного пульта управління. Управління дронами в ручному режимі застосовується в певних умовах при великій кількості непередбачуваних факторів. Даний режим можна активувати наприклад при відмові автоматики БпЛА.

Напіваавтоматизований режим керування – використовується у сприятливих умовах, коли ситуація є передбачуваною, і присутня мінімальна кількість позаштатних ситуацій та факторів. Автоматизувати можна частину польоту, якісь окремі елементи польоту (наприклад – зліт та посадки), а також можна автоматизувати процеси відео- та фотозйомки.

Автоматизований режим управління – застосовується коли ситуація повністю прораховується, середовище польоту є сприятливим. Тут можна повністю автоматизувати політ, позначити завдання, після закінчення яких БпЛА повернеться на вихідну точку вильоту. Також при втраті каналу зв'язку є інерційна навігаційна система на волоконно-оптичних гіроскопах і кварцових

акселерометрах. Даний режим дозволяє виробити оптимальне навігаційне рішення за часткового, повного або періодичного зникнення зв'язку з наземною станцією управління.

Керування польотом здійснюється за допомогою пульта дистанційного керування, позиціонування у просторі обумовлено використанням супутникових систем навігації або інерціальних систем.

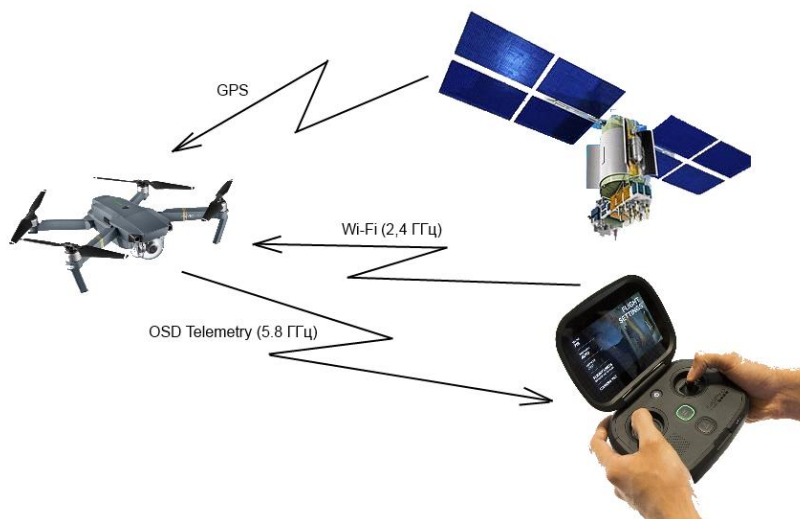


Рисунок 1.2 – Візуалізація каналів управління та позиціонування БПЛА

Різні моделі квадрокоптерів мають різну кількість каналів управління, що відповідають за певні команди та функції, такі як зйомка відео, запис звуку, управління та інші.

Сукупність елементів квадрокоптера разом із програмним забезпеченням формують якість та сукупність функцій квадрокоптера, зокрема кількість режимів управління, які суттєво впливають на вартість обладнання квадрокоптера. Розглянемо основні їхні види:

- «Headless mode» (GPS) – найбільш простий режим управління, коли не важливо де саме у квадрокоптера знаходиться ніс, дрон буде вважати за перед той бік, яким було розпочато політ.
- «Follow Me» (GPS) - режим, що дозволяє дрону рухатись за людиною, що управляє апаратом.

- «Acro» режим - найбільш складний для освоєння режим, в цьому режимі дрон не використовує систему стабілізації.
- «Flight to point» (GPS) GPS-режим - в цьому режимі літальний апарат пересувається відповідно з точками, визначеними системою супутникової навігації GPS.
- «Return To Home» (GPS) – функціональний режим, основна задача якого - повернення квадрокоптера на вказану точку. Наприклад можна запрограмувати коптер повертатися додому.
- «Active Track» (GPS) – інтелектуальний режим, що дозволяє керуючому апаратом розпізнавати небезпечні предмети і виключати ситуації зіткнення з ними.

Польотні режими, які включають в себе режими за асистуванням GPS значно облегшують управління квадрокоптерами, в результаті чого його можуть успішно використовувати навіть малопідготовлені пілоти.

Слід зазначити, що коли сигнал GPS зникає – більшість квадрокоптерів втрачають можливість функціонування в автоматичних режимах і переходять в режим лише утримання висоти. Через це вони стають сприйнятливими до таких дестабілізуючих факторів як, наприклад, бічний вітер – через це можуть бути втрачені через відліт поза зону зв'язку із наземним пунктом управління, автоматичні режими повернення також в цьому випадку не допоможуть, якщо тільки дрон не оснащений інерціальними системами позиціонування, котрі на великих відстанях мають суттєву помилку, схильну до наколювання.

1.3 Нормативна база, щодо використання квадрокоптерів у світі

Велика популярність БпЛА, зокрема квадрокоптерів, що викликана їхньою доступністю і технологічністю, приводить до різних інцидентів: починаючи від падіння на людей під час масових заходів, закінчуючи зіткненнями із літаками пасажирської авіації.

Для уникнення подібного роду випадків, які можуть призвести до небезпечних результатів, у світі розроблюються правові норми стосовно використання такого типу літальних апаратів.

Відповідно до вимог пункту 4 розділу II Правил використання повітряного простору, польоти безпілотних повітряних суден масою до 20 кг включно виконуються без подання заявок на використання повітряного простору, без отримання дозволів на використання повітряного простору, без інформування органів управління Повітряних Сил Збройних Сил України та органів об'єднаної цивільно-військової системи організації повітряного руху України (ОЦВС), органів Державної прикордонної служби України, органів обслуговування повітряного руху (ОПР) та відомчих органів управління повітряним рухом (УПР), за умови дотримання таких вимог [3]:

- 1) польоти виконуються без перетинання державного кордону України;
- 2) польоти виконуються поза межами встановлених заборон та обмежень використання повітряного простору, крім випадків, установлених Положенням про використання повітряного простору;
- 3) польоти виконуються не ближче 5 км від зовнішніх меж злітно-посадкових смуг аеродромів або не ближче 3 км від зовнішніх меж злітно-посадкової смуги вертодромів, крім випадків узгодження з експлуатантом аеродроме/вертодрому;
- 4) польоти виконуються не ближче 500 м від пілотованих повітряних суден;
- 5) польоти не виконуються над:
 - скупченням людей на відкритому просторі та над місцями щільної забудови;
 - об'єктами (зонами), які визначені Міністерством оборони України, Міністерством інфраструктури України, Міністерством внутрішніх справ України, Державною прикордонною службою України, Службою безпеки України, Національною поліцією України, Національною гвардією України, Державною фіскальною службою України, Службою зовнішньої розвідки

України, Управлінням державної охорони України, іншими військовими формуваннями та правоохоронними структурами, утвореними відповідно до законів України, та відносно яких здійснюється охорона / державна охорона (за умови позначення території навколо цих об'єктів інформаційними знаками про заборону польотів безпілотних повітряних суден та/або шляхом оприлюднення меж такої заборони), крім випадків виконання польотів за дозволом зазначених вище повноважних органів [3];

6) польоти виконуються в межах прямої видимості (VLOS);

7) максимальна висота польоту не вище:

- 120 м над рівнем земної (водної) поверхні поза межами CTR, AFIZ , ATCA, ATCZ, спеціально встановлених зон, іншого спеціально зарезервованого повітряного простору;

- 50 м над рівнем земної (водної) поверхні в межах CTR, AFIZ, ATCA, ATCZ, спеціально встановлених зон, іншого спеціально зарезервованого повітряного простору, якщо інформація про фактичний статус елементів структури повітряного простору на час виконання польоту відсутня;

- 50 м над статичними перешкодами на горизонтальній відстані не більше 100 м від таких перешкод, як відхилення від зазначених вище обмежень по висоті, на запит власника такого об'єкту;

8) швидкість польоту безпілотного повітряного судна складає не більше 160 км/год [3].

В інших випадках польоти безпілотного повітряного судна масою до 20 кг включно та усі без винятку польоти безпілотного повітряного судна масою більше 20 кг виконуються у межах спеціально встановлених зон та маршрутів з дотриманням вимог щодо подання заявок на використання повітряного простору, отримання дозволів та умов використання повітряного простору, інформування органів управління Повітряних Сил Збройних Сил України, органів Державної прикордонної служби України, органів ОЦВС, органів ОПР/УПР [3].

Нормативна база в інших країнах світу доволі сильно відрізняється в різних країнах, проте є загальні моменти, котрі можна звести до розглянутих нижче.

Польоти, котрі здійснюються в комерційних цілях – реєструються у відповідних органах..

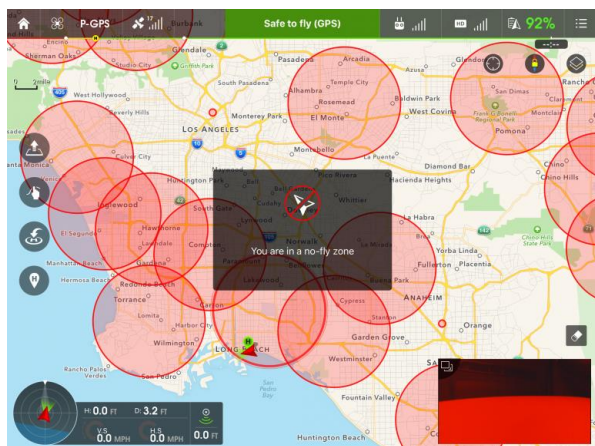
Якщо дрон важить менше 2-х кг і польоти здійснюються в приватних цілях (хобі/розвага), додаткової реєстрації не потрібно, але існує список обов'язкових умов, що вимагають дотримання [4]:

- - ви не можете здійснювати польоти ближче, ніж 30 м від транспортних засобів, човнів, будинків, які розташовані не на вашій приватній власності або ви не володієте дозволом від власника приватної власності;
- - ви не можете літати над населеними пунктами і над територіями скупчення людей, такими як публічні пляжі, чужі двори / ділянки, парки і громадські зони відпочинку, спортивні заходи та ігрові зони [4];
- ви не можете працювати в радіусі 5.5 км від будь-якого аеродрому, аеропорту, в зонах зльоту і посадки вертольотів, які можуть бути розташовані в лікарнях, поліцейських ділянках і інших місцях, які не очевидні при першому розгляді, перед плануванням польоту необхідно обов'язково враховувати дані локації (незнання не звільняє від відповідальності);
- - польоти дозволено здійснювати виключно в світлий час доби. Тільки в гарну погоду і в межах видимості пілота;
- - дальність польоту не повинна перевищувати 400 футів (123 м).

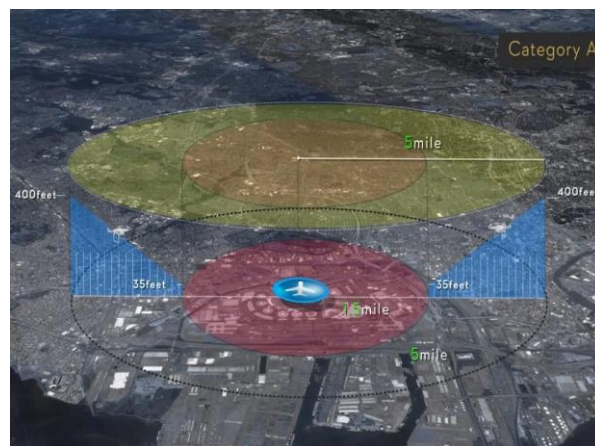
Як можна побачити на законодавчому рівні майже у всіх розвинених країнах світу виконується регулювання польотів із використанням БПЛА. Слід зазначити, що і самі виробники такого обладнання слідкують за дотриманням загальних вимог і рекомендацій, щодо польотів. Наприклад фірма DJI, на рівні програмного забезпечення своєї продукції вводить так звані «безпілотні зони»,

в яких заборонено виконувати польоти на квадрокоптерах. У цих зонах БПЛА злітати не буде, і залітати до них також.

На рис. 1.3 наведені візуалізації заборонених зон для польотів на комерційних дронах.



а)



б)

Рисунок 1.3 – а) Карта безпілотних зон на карті місцевості; б) Безпілотна зона у вигляді вирви

2 АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ БпЛА

Не секретом є і той факт, що активним чином розвивається і такий напрямок як протидія БпЛА. Це викликано через непоодинокі випадки появи малорозмірних літальних апаратів у закритих зонах аеропортів, а також використання в цілях промислового шпигунства і втручання в особисте життя громадян. До того ж БпЛА дуже активно використовуються у військових діях у якості розвідників, коригувальників, ретрансляторів зв'язку, атакуючої техніки як самостійно так і у складі комплексів військового обладнання.

Все це викликає суттєву увагу щодо рішень, спрямованих на боротьбу із подібного роду літальними апаратами. У розробці таких технологій зацікавлені не тільки збройні сили, а й органи безпеки, поліція і приватні охоронні фірми.

Боротьба з БпЛА є комплексом заходів щодо їх виявлення, розпізнавання, прицілювання, захоплення й ураження.

2.1 Демаскуючі ознаки БпЛА

Для того, щоб протидіяти БпЛА в першу чергу їх необхідно виявити та за можливістю ідентифікувати, для того щоб забезпечити більш ефективну протидію. Це пов'язано з тим, що самі методи протидії можуть бути неоднаково ефективними для різних типів БпЛА.

Для виявлення літальних апаратів використовується набір технічно-організаційних заходів щодо їх виявлення. Саме виявлення можливе завдяки існуванню у БпЛА демаскуючих ознак, класифікація котрих зображена на рис.2.1.

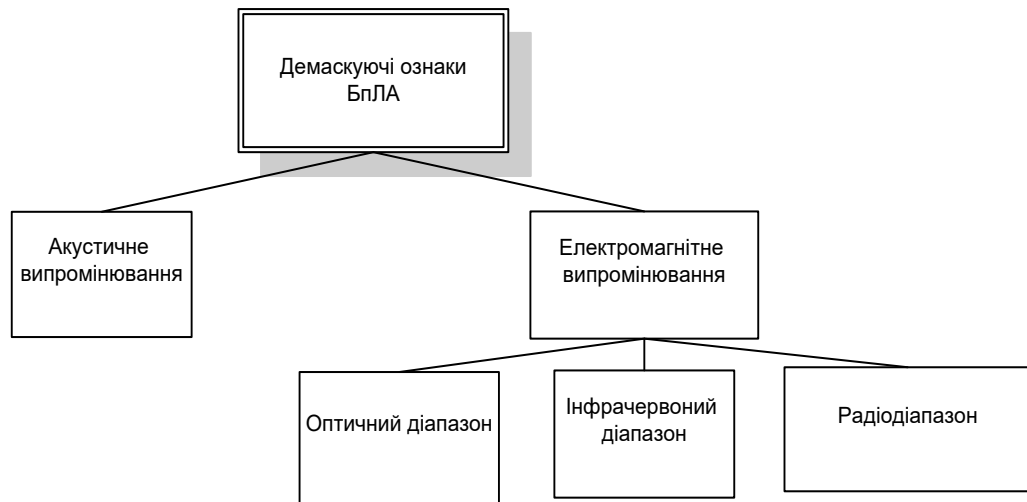


Рисунок 2.1 – Демаскуючі ознаки БПЛА

Акустичне випромінювання як правило викликано роботою рушійних агрегатів – гвинтомоторними групами або реактивними двигунами. Гучність звуку від них може бути доволі високою, вони можуть бути чутні від декількох десятків метрів до кількох кілометрів.

Фактори котрі впливають на гучність та якість акустичних коливань:

- тип двигуна (ДВС або електричний);
- розмір та форма гвинтів, частота їхніх обертів.

ДВС, реактивні двигуни та електричні двигуни імперного типу як правило більш гучні, ніж електричні двигуни із пропелерами.

До електромагнітних демаскуючих ознак можна віднести наступні:

- сигнали бортового відповідача;
- сигнали РЛС, відбиті від корпусу та елементів БПЛА;
- сигнали телевізійних станцій та ретрансляторів, базових станцій стільникового зв'язку, що відбиваються від БПЛА;
- лінія зв'язку каналу управління дроном;
- сигнали бортових РЛС. [1].

Якщо розглядати демаскуючі ознаки в оптичному діапазоні – то це можуть бути бортові вогні, та власне саме дрон, який відбиває сонячне світло.

2.1 Демаскуючі ознаки БПЛА

Основні методи виявлення БПЛА, які зображено на рис. 2.2.

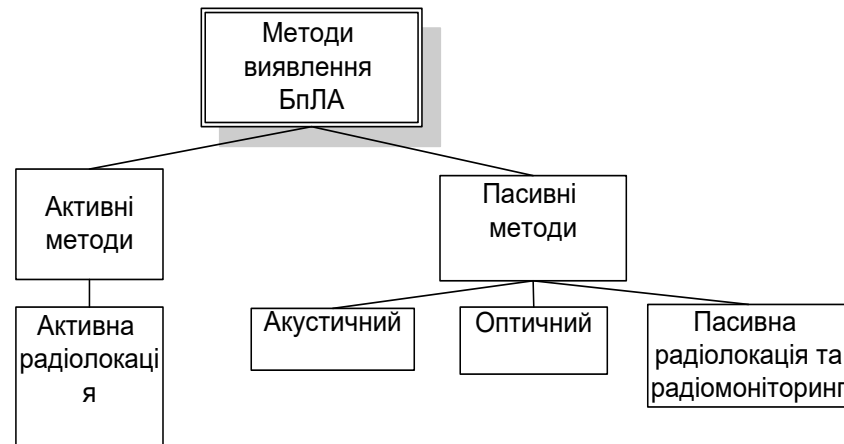


Рисунок 2.2 – Основні методи виявлення БПЛА

Застосування методів та дальність їхньої дії може суттєво відрізнятися для конкретних БПЛА, в залежності від наявності в них тих чи інших демаскуючих ознак, якими вони володіють.

Активні методи радіолокації ефективні для великих за розмірами БПЛА, оскільки вони володіють доволі значними ефективними площами розсіювання (ЕПР) та висотами польоту, що робить їх виявлення за допомогою РЛС доволі ефективним [5].

Найбільшу складність виявлення представляють малогабаритні БПЛА (МБПЛА). Приклад такого літального апарату наведено на рис. 2.3.



Рисунок 2.3 – Малогабаритний МБПЛА DJI Spark (вага 300 г, час польоту 15 хв.)

Хоча даний пристрій і являє собою комерційний пристрій із наявністю в його програмному забезпеченні безпольотних зон – їх доволі легко можна обійти.

Сукупність ознак МБпЛА:

- нано-БпЛА маса складає менше 1 кг, тривалістю польоту менше 1 години і висота польоту до 300 м;
- мікро-БпЛА – маса до 10 кг, часом польоту 1 година, висота польоту до 1 км;
- міні-БпЛА – маса до 50 кг, час польоту до кількох годин, висота польоту до 3–5 км [5].

У ряді випадків МБпЛА є складними цілями для РЛС. Дані апарати мають малу ЕПР, це призводить до того, що їхнє виявлення стає досить складною задачею. Зокрема через це знижується максимальна дальність виявлення [3]. А враховуючи факт встановлення на них спеціальних антирадарних покриттів, найбільшу ефективність дає застосування двочастотних імпульсних радіолокаторів. Перша група частот у дециметровому діапазоні, друга в сантиметровому дозволяє покращити результати виявлення МБпЛА [6].

Слід зазначити, що МБпЛА виготовляють із композитних матеріалів та особливого пластику зі спеціальним кольоровим оформленням, що ускладнює їхнє оптичне виявлення за допомогою камер, а їх невеликі бензинові, а ще більш електричні двигуни мало випромінюють в інфрачервоному спектрі та працюють майже безшумно [5].

Тому для ефективного виявлення таких приладів необхідне одночасне використання декількох методів виявлення.

Найбільша вразливість МБпЛА обумовлена наявністю електромагнітного випромінювання (ЕМВ). Основними інструментами виявлення МБпЛА в електромагнітному діапазоні є:

- тепловізор інфрачервоного діапазону ЕМ хвиль;

- камери оптичного діапазону ЕМ хвиль;
- РЛС;
- радіомоніторинг.

Радіомоніторинг (РМ) дозволяє отримати інформацію щодо об'єкту за його електромагнітним випроміненням із використанням технічних засобів.

РМ включає діяльність з оцінки радіообстановки, пошуку, виявлення та контролю різних каналів зв'язку, та визначення інших джерел радіовипромінювання.

Завдання РМ:

- панорамний спектральний аналіз у поточному часі;
- пошук випромінювання від БпЛА, оцінка та вимірювання їх параметрів, порівняння з базою даних та визначення їх приналежності тим чи іншим різновидам БпЛА;
- запис радіосигналів зі службовими параметрами (частота, час, рівень сигналу, спектрограма тощо) та подальше їх відтворення;
- технічний аналіз радіосигналів у реальному часі та в пост-обробці;
- пеленг БпЛА.

Приклад роботи результатів РМ можна побачити на рис.2.4 , де можна побачити сигнал управління дронів із використанням ППРЧ.

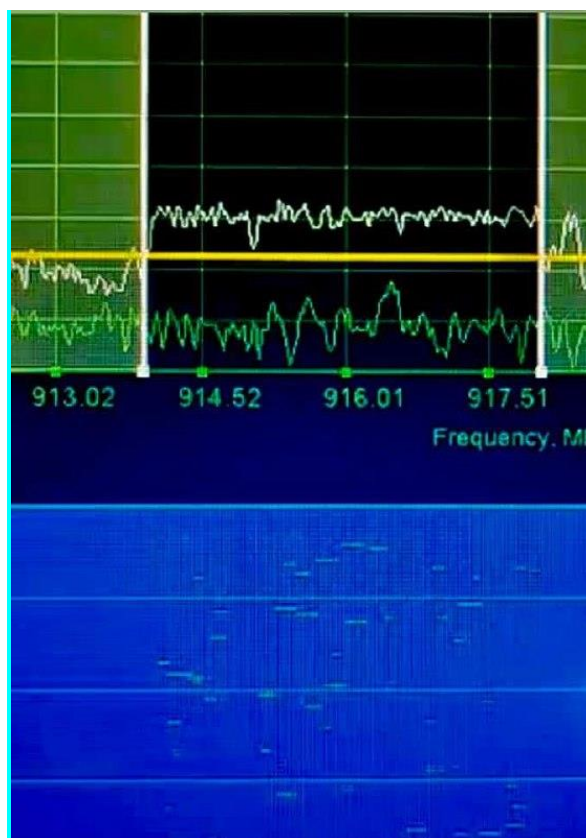


Рисунок 2.4 – Приклад сигналів управління дронів, які використовують ППРЧ 913-918 МГц

Прийом подібного сигналу може свідчити про те, що комплекс РМ виявив БпЛА. Якщо навчити систему виявляти та розпізнавати такі і подібні сигнали, то можна виявляти БпЛА шляхом радіомоніторингу повітряного простору.

3 АНАЛІЗ МЕТОДІВ ПРОТИДІЇ БпЛА

Розглянемо більш детально різні методи протидії, які є більш фінансово доступними та універсальними.

3.1 Глушіння БпЛА

Більшість сучасних БпЛА використовують канали зв'язку та передачі відео або зображення, що працюють в частотних діапазонах 2.4 ГГц та 5.8 ГГц. Більшість з них використовують навігаційні системи GPS і ГЛОНАСС, які працюють в частотних діапазонах 1575,42 МГц и 1224,60 МГц.

Проте із використанням різного обладнання ці частоти можуть суттєво відрізнятися одна від одної, наприклад радіоканал управління може бути на частотах 430 МГц, 960 МГц, 1,2 ГГц. Як можна побачити ці частоти нижче аніж 2,4 ГГц – це пов'язано з тим що, за рахунок властивостей радіохвиль нижчі частоти менше згасають під час розповсюдження, тому дані частотні діапазон зазвичай використовуються для дальніх польотів.

Для забезпечення позиціонування у просторі БпЛА як правило використовують барометричні висотоміри, акселерометри, ультразвукові, інфрачервоні датчики та сигнали GPS.

Частоти роботи супутників GPS [7] :

- L1 (1575.42 МГц) частота використовується старими супутниками;
- L2 (1227.60 МГц) частота використовується сучасними супутниками;
- L3 (1381.05 МГц): застосовується для виявлення ядерних вибухів і інших високоенергетичних явищ в інфрачервоному діапазоні;
- L4 (1379.913 МГц): для вивчення процесів, котрі перебігають в іоносфері;
- L5 (1176.45 МГц): для цивільної безпеки життя.

Отже, щоб позбавити квадрокоптер керування та навігації потрібно заблокувати ці канали передачі.

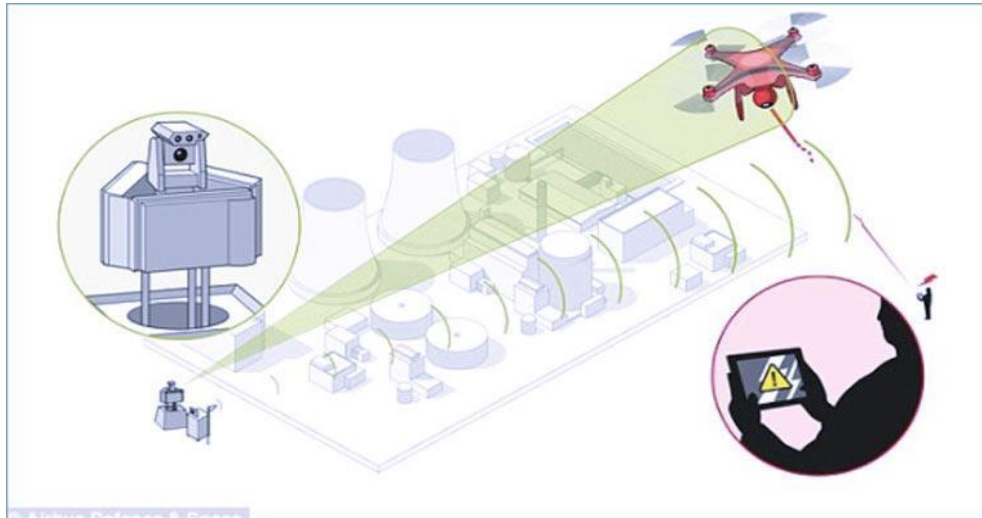


Рисунок 3.1 – Візуалізація глушіння БПЛА

Саме на придушення таких сигналів орієнтуються комерційні прилади постановки перешкод. За допомогою таких пристроїв можна створити навколо дрона зону радіомовчання, завдяки потужному радіосигналу, який обриває подачу сигналів з боку оператора. При цьому, порушується і позиціонування за GPS або ГЛОНАСС.

Але слід враховувати, що чим коротше довжина хвилі, тим слабкіше виявляється дифракція радіохвиль. З цієї причини хвилі діапазонів УВЧ-СВЧ, із використанням яких і працюють БПЛА, дуже слабо діфрагують навколо земної поверхні і дальність їх поширення визначається здебільшого відстанню прямої видимості (прямі хвилі) .

Тобто, для того щоб заглушити такі канали має бути організована умова прямої видимості «цілі» та джерела завади.

На рис. 3.2 наведений пристрій комплексного глушіння гармата ANTIDRON KVSG-6.



Рисунок 3.2 – Антидронна гармата ANTIDRON KVSG-6

ANTIDRON G-6 виробляє українська компанія Kvertus Technology. На офіційному сайті зазначено, що комплекс вражає більшість видів дронів, блокуючи частоти дистанційного радіоуправління, відеопередачі, навігації GPS у радіусі до 3 км, на відстань впливає сила сигналу та місце розташування оператора. Однією батареї вистачає на 25-30 хвилин роботи, рівень заряду, що залишився, відображається на спеціальному індикаторі. Загальна вихідна потужність 80 Вт [8].

Але треба враховувати той факт, що деякі дрони оснащені суттєвими засобами боротьби із завадами завдяки спеціальним антенним системам та організації радіоприйому.

Але глушіння GPS та каналів управління малодоцільне коли БпЛА використовує інерціальну систему навігації і летить в автоматичному режимі без супроводження пілота.

3.2 Підміна GPS-координат

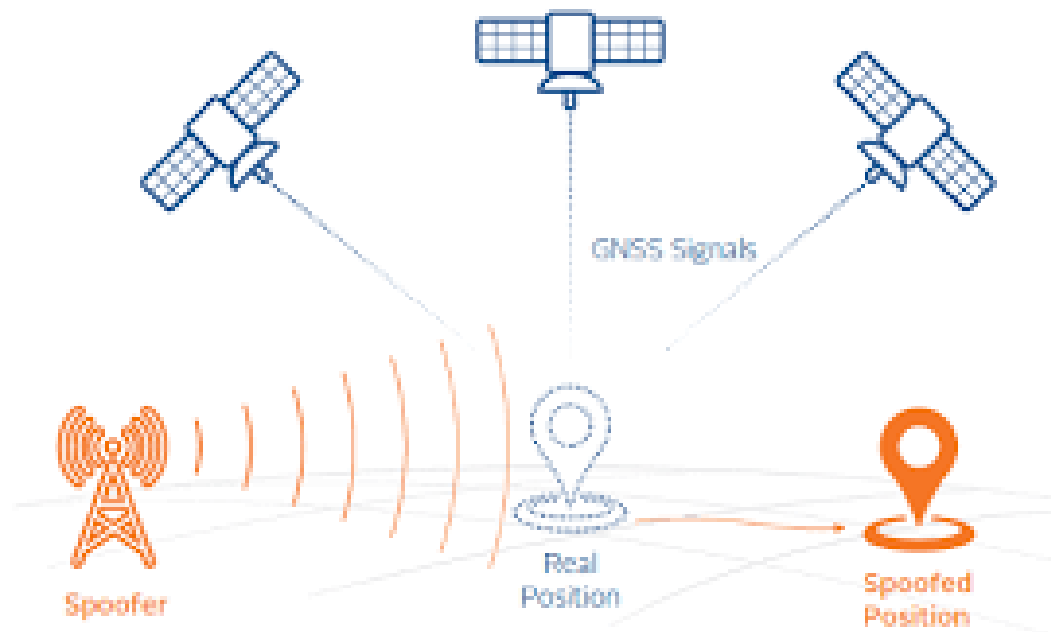


Рисунок 3.3 – Spoofing атака для сигналу GPS

У цьому методі відбувається не просто глушіння каналу GPS, а підміна просторових координат, які отримуються завдяки цій процедурі.

Spoofing атака на GPS – атака, яка намагається обдурити GPS-приймач, широкомовно передаючи трохи більш потужний сигнал, ніж отриманий від супутників GPS, такий, щоб бути схожим на ряд нормальних сигналів GPS. Ці імітовані сигнали, змінені таким способом, щоб змусити одержувача не визначити своє місце розташування, вважаючи його таким, яке відправить атакуючий. Оскільки системи GPS працюють вимірюючи час, який потрібен для сигналу, щоб дійти від супутника до одержувача, успішний спуфінг вимагає, щоб атакуючий точно знав, де його ціль – така, щоб імітуючий сигнал міг бути структурований з належними затримками сигналу. Атака спуфінга GPS починається, передаючи трохи більш потужний сигнал, який вказує коректну позицію, і потім повільно відхиляється далеко до позиції, заданої атакуючим, тому що переміщення занадто швидко призведе до втрати

сигнальної блокування, і в цій точці spoofer стане працювати тільки як передавач перешкод [9].

Таким чином можливо посадити дрон у хибній точці «домашньої позиції», або змусити його зупинятися, блокуючий подальший політ.

3.3 Перехоплення управління

Цей метод є найбільш складним. За мету ставиться отримання самого дрону, та інформації, яка міститься на ньому.

Для здійснення перехоплення необхідно знати протоколи управління дроном, які можуть бути відкритими і закритими, залежати від виробника. Це суттєво ускладнює задачу перехоплення.

Серед відомих способів можна відзначити наступні:

- атаку за часом (timing attack), синхронізуючи частоту випромінювача свого пульта з частотою радіомодуля дрона в автоматичному режимі, після цього на дрон відправляється шкідливий пакет, який змушує чужий апарат ігнорувати команди з «рідного» контролера, і почати слухати команди з контролера зломисника [10];

Можна відзначити, що для перехоплення фірма DJI реалізувала комплекс, який дозволяє вести неперервний контроль поруч із об'єктом, біля якого заборонені польоти [11].



Рисунок 3.4 – Зовнішній вид комплексу DJI Aeroscope

Даний комплекс дозволяє ідентифікувати всі повітряні борти цього виробника, і може виконати екстрену посадку, або перехоплення управління «дрона-зловмисника». Проте вартість такого комплексу складає декілька тисяч доларів і дозволити його придбання можуть не всі структури. До того ж, дрони інших виробників не можуть бути зупинені даним пристроєм.

3.4 Фізична протидія

Фізична протидія квадрокоптерам являє собою не лише спроби збити його з якоїсь зброї. Для реалізації цього методу може використовуватись «дрон мисливець», заряджений сіткою. Як тільки ціль ідентифікована, коптер піднімається в повітря і стріляє сіткою в порушника. Для цих цілей також можуть бути використані спеціально навчені птахи. Також для боротьби із БпЛА можуть бути використані протизенітні ракетні комплекси, або стрілецька зброя.

3.5 Порівняльна характеристика методів

Таблиця 3.1 – Переваги та недоліки різних методів боротьби з квадрокоптером

	Переваги	Недоліки
Глушіння	Невелика вартість, простота реалізації	Мала селективність атаки та низька енергетична ефективність
Фізична протидія	Висока ефективність протидії	Складність реалізації
Підміна GPS-координат	Висока ефективність, можливість посадки дрона в заданній точці	Значна складність реалізації, висока вартість обладнання
Перехоплення управління	Висока ефективність, отримання доступу до всіх функцій дрон	Висока вартість, мала універсальність, складність реалізації

Можна відзначити, що не один з методів на практиці не застосовується відокремлено від інших. Це залежить від конкретного випадку, дивлячись на ресурси, та моделі конкретного БпЛА.

4 ЗАПРОПОНОВАНІ МЕТОДИ ДЛЯ ПРОТИДІЇ КВАДРОКОПТЕРАМ

Не дивлячись на те, що існує нормативна база, яка регулює використання квадрокоптерів, не зрозуміло які саме органи мають слідкувати за їх виконанням. Цей факт призводить до вразливості приватної інформації. Для її захисту пропонується два методи протидії квадрокоптерам, які були реалізовані на практиці.

4.1 Протидія квадрокоптерам із керуванням за Wi-Fi

Велика кількість квадрокоптерів може керуватися із використанням технології Wi-Fi. Саме використовуючи особливості цієї технології можливо виконати протидію керування квадрокоптера.

Стандарт Wi-Fi 802.11 визначає різні типи фреймів, які точки доступу і мережеві карти для користувача пристроїв з Wi-Fi використовують для комунікацій, управління та контролю бездротового лінка [12].

Другий рівень (Data Link) моделі OSI/ISO в 802.11 розділений на два підрівні:

1. LLC (Logical Link Control) – ідентичний для всіх мереж платформи 802;
2. MAC (Media Access Control) – ідентичний для всіх мереж платформи 802.11.

Стандарт 802.11 визначає операції саме на MAC-підрівні другого рівні моделі OSI. Цей стандарт визначає три типи фреймів: фрейми Управління (Management frames), фрейми Контролю (Control frames), фрейми Даних (Data frames) [12].

Кожен фрейм має контрольне поле, яке визначає версію протоколу 802.11, тип фрейму і різні індикатори, наприклад: WPA включений, управління енергозбереженням активно і т.д. Додатково до цього все фрейми містять MAC-адреси джерела і одержувача, номер фрейма в послідовності, тіло фрейма і перевірючу послідовність фрейму для корекції помилок. Фрейми 802.11 переносять протоколи і дані більш високих рівнів моделі OSI/ISO всередині

тіла фрейма. Наприклад фрейм даних може транспортувати HTML-код будь-якої веб-сторінки (з усіма необхідними заголовками TCP/IP), що використовується далі для відображення. Інші фрейми, які станції використовують для управління і контролю несуть специфічну інформацію про бездротовому лінк в тілі фрейма. Наприклад, тіло фрейма бікона містить ідентифікатор мережі WLAN: SSID, тимчасові позначки (timestamp) і іншу інформацію про точку доступу [12].

Фрейми управління Wi-Fi (Management Frames) 802.11 – дозволяють встановлювати і підтримувати комунікації в мережі стандарту Wi-Fi.

Фрейм деаутентифікації (Deauthentication frame) користувача пристрою відправляє кадр деаутентифікації Wi-Fi до іншого пристрою, якщо хоче закінчити безпечне з'єднання. Фрейм деаутентифікації це нотифікація, а не запит. При отриманні повідомлення деаутентифікації жодна приймаюча сторона не може відмовитися його виконати, за винятком випадку коли включений режим захисту фреймів (802.11w: MFP або Management Frame Protection) і не вдалося успішно виконати контроль від підробки фрейма MIC (Message Integrity Check). Якщо фрейм повідомлення деаутентифікації не почуте на іншому кінці, то правила управління на MAC-рівні дозволяють трактувати такий стан як втрату комунікацій [12].

Таким чином, щоб виконати від'єднання пульта від квадрокоптера треба використати фрейм деаутентифікації. Це приведе до того, що зв'язок за каналом управління буде перерваний і це призведе до активації режиму RTH - квадрокоптер примусових має вернутися до точки зльоту.

Wi-Fi jammer – це пристрій, який призначений для відключення бездротових пристроїв від точки доступу, він є апаратним деаутентифікатором. Ця процедура виконується за допомогою фрейма деаутентифікації, який використовується для безпечного підключення клієнтів від бездротової мережі. Оскільки ці керуючі пакети незашифровані, з'ясувати MAC-адресу маршрутизатора Wi-Fi і клієнтського пристрою між якими треба виконати

роз'єднання нескладно. Для виконання цієї процедури не обов'язково бути в мережі або знати пароль, цього достатньо, щоб бути в його діапазоні [13].

На даний момент великої популярності набули недорогі і мініатюрні плати з підтримкою програмної платформи NodeMCU. Вони побудовані на модулі ESP8266, який реалізує роботу з Wi-Fi за стандартом 802.11 b / g / n на частоті 2,4 ГГц. Зараз зустрічається два варіанти подібних плат: з чіпом CP2102 американської компанії Silicon Labs або з китайським CH340 [14].



а)



б)

Рисунок 4.1 – а) Зовнішній вигляд модулю NodeMCU; б) Модуль ESP8266

ESP8266 - дешевий мікроконтролер із вбудованим Wi-Fi. Він містить 160 МГц процесор і може бути запрограмований з використанням Arduino або без неї. Дані плати позиціонуються як пристрої для прототипування: на їх основі створюються автоматизовані системи, які підлягають контролю за Wi-Fi. Тема сама по собі дуже цікава, але наразі нас цікавить інше - можливість застосування NodeMCU для проведення атак. У ESP8266 і є режими роботи в якості клієнта (P2P) і точки доступу (soft-AP). Управляти платою можна з телефону або будь-якого іншого пристрою з Wi-Fi. За допомогою відповідної прошивки його можна використовувати в якості деаутентифікатора. Для прошивки використане середовище Arduino IDE [14].

Види атак, які можна здійснити за допомогою утиліти

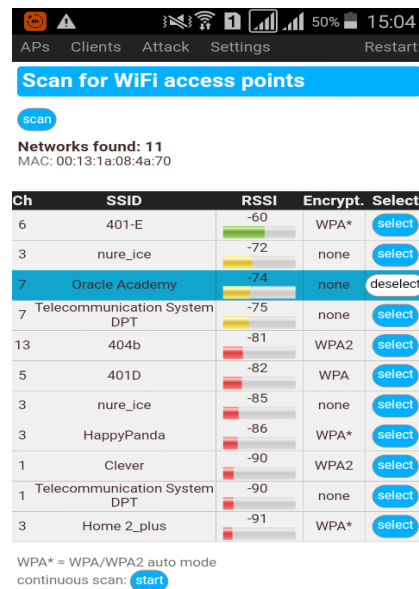
- Deauth (deauthentication attack) – посилає фрейм деаутентифікації і роз'єднання обраних клієнту обраної точки доступу.
- Beacon (Beacon flood attack) – Виконує клонування обраної мережі або мереж із списку.

Алгоритм запуску пристрою:

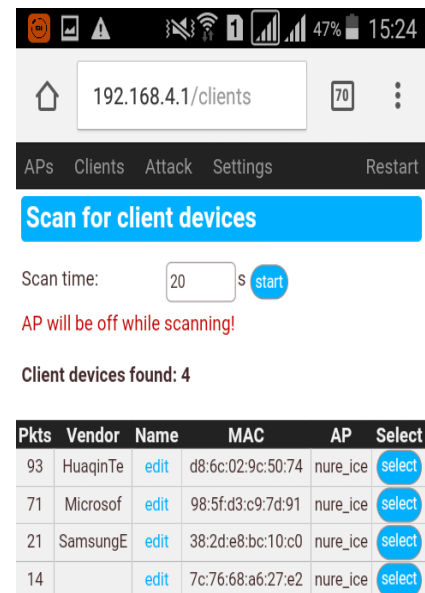
- 1) Спочатку необхідно запустити ESP8266, подавши живлення.
- 2) Включити Wi-Fi на пристрої та з'єднуватись з сервером ESP8266;
- 3) Після підключення необхідно відкрити браузер і перейти до 192.168.4.1;
- 4) Необхідно зробити сканування мереж WI-FI з метою виявлення мережі квадрокоптера, котрому потрібно вчинити протидію.



Рисунок 4.2 – Обладнання для протидії БПЛА, які керуються за допомогою Wi-Fi



а)



б)

Рисунок 4.3 – а) Результаты мониторингу Wi-Fi мереж; б) Виявлення підключеного клієнта (пульт керування) керування до квадрокоптера

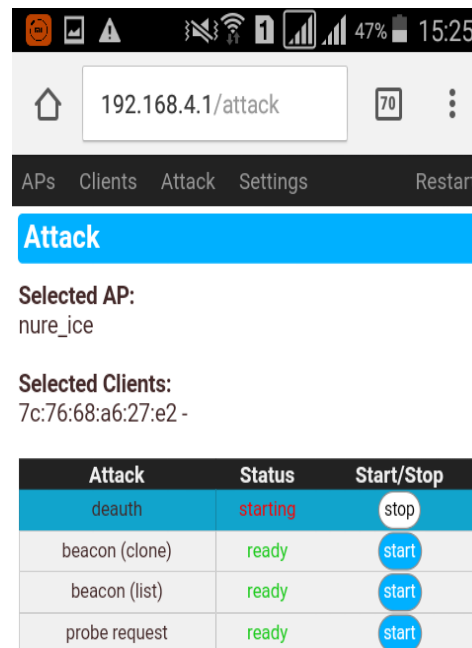


Рисунок 4.4 – Виконання атаки типу «деаутентифікація»

Визначення точки доступу, яка організована квадрокоптером можна виконати завдяки особливостям MAC адреси, яка специфічна для даного виду пристроїв. Крім того, даний вид атаки може бути частиною комплексної атаки

по перехопленню квадрокоптера. Наприклад для цих цілей може бути використана атака типу Beacon, або за допомогою утиліти aircrack-ng, завдяки вразливості WPS.

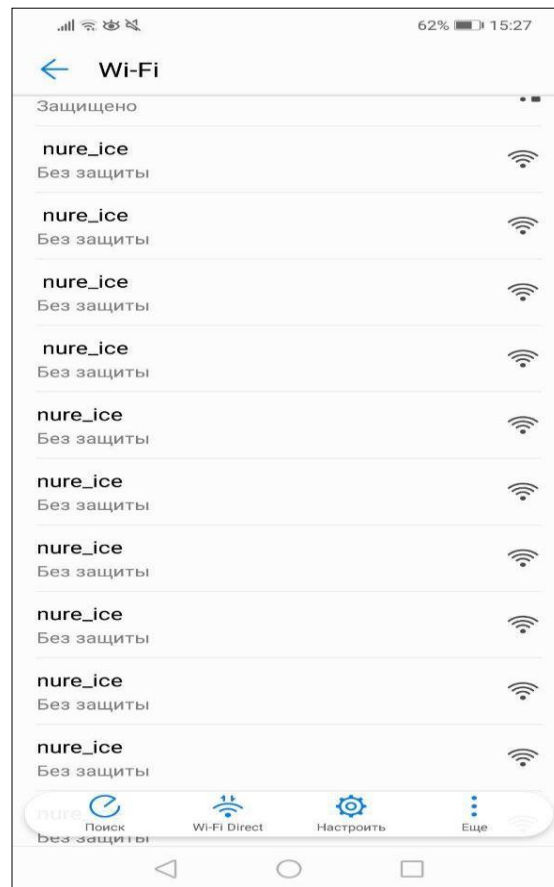


Рисунок 4.5– Результат виконання атаки типу Beacon

4.2 Пристрій для глушіння GPS

Атака за Wi-Fi є досить ефективною враховуючи кількість квадрокоптерів, які керуються за допомогою цього протоколу. Проте досить популярні і інші методи керування, які дозволяють керувати квадрокоптером на значній відстані без використання Wi-Fi. Саме для цього випадку пропонується пристрій, який має більшу універсальність – це генератор завад для GPS. При постанові завад за цим каналом вразливими є всі типи квадрокоптерів, які керуються за допомогою інтелектуальних режимів із використанням GPS. Виключенням є лише спортивні квадрокоптери, які не досить розповсюджені.

Принципова електрична схема даного пристрою зображена на рис. 4.6.

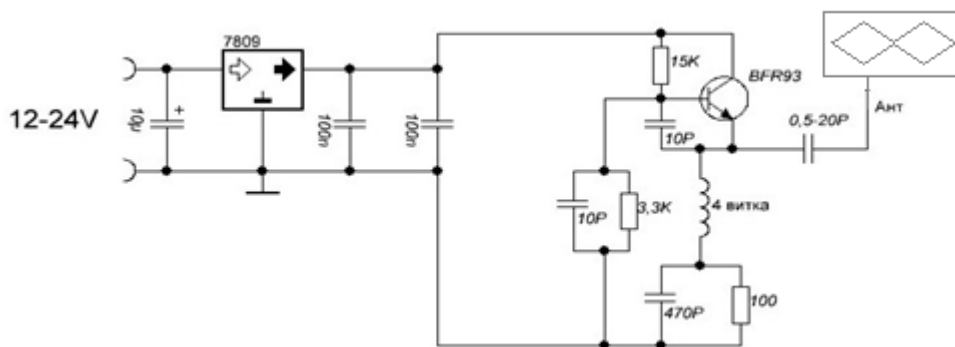


Рисунок 4.6 – Принципова електрична схема генератора завод для GPS

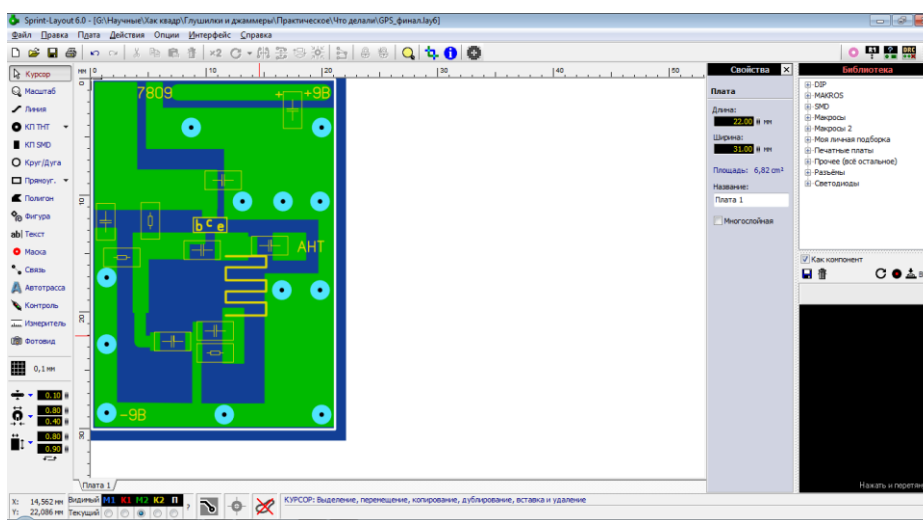
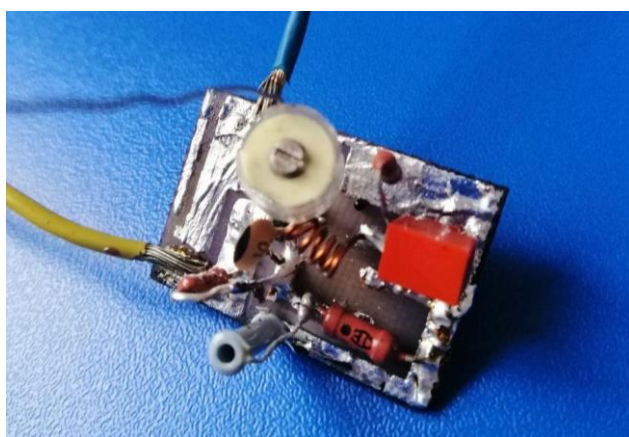


Рисунок 4.7 – Друкована плата генератора завод у програмі Sprint-Layout



а)



б)

Рисунок 4.8 – а) Генератор завод; б) Спектр сигналу, що формується генератором завод

Формально використання подібного роду пристроїв потребують дозволу відповідних органів.

Для проведення експерименту використовувався квадрокоптер Hubsan-501S, який зображений на рис. 4.9.



Рисунок 4.9 – Квадрокоптер Hubsan-501S

Для проведення експерименту із глушінням GPS була зібрана лабораторна установка (рис 4.10), яка включала квадрокоптер, пульт дистанційного керування, спектроаналізатор HMS-3000 і пристрій глушіння.



а)



б)

Рисунок 4.10 – а) Експериментальна установка з виключеним генератором завад;

б) Експериментальна установка з включеним генератором завад

Результат роботи запропонованої схеми видно на телеметрії, що зображена на екрані пульта квадрокоптера рис.4.11. Рожевим кольором знизу екрану зображено кількість супутників, що бачить квадрокоптер, а нижче жовтим кольором зображено кількість супутників, що бачить пульт. З рисунку видно, що сигнал від супутників зник.



а)



б)

Рисунок 4.11 – а) Екран квадрокоптера з виключеним генератором завад;
б) Екран квадрокоптера з включеним генератором завад.

4.3 Розробка спрямованої антени для підвищення якісних характеристик запропонованих пристроїв

Пристрої, які були розглянуті вище мають певне обмеження на радіус дії. Крім того, генератор завад для GPS працює за всіма напрямками у просторі, що може створювати завади не лише обраному пристрою, а й іншим, на відміну від Wi-Fi jammer, який виконує селективну атаку.

Дальність дії каналу радіозв'язку визначається за наступною формулою [15]:

$$r = \lambda \frac{\sqrt{A \cdot G_1 \cdot G_2 \cdot \eta_1 \cdot \eta_2 \cdot \nu^2}}{4 \cdot \pi} \quad (4.1)$$

Збільшення радіусу дії пропонується виконати завдяки підвищенню коефіцієнта підсилення антени G на стороні пристрою протидії. Для цих цілей була виготовлена антена Харченка, яка є простою у виготовленні та має коефіцієнт підсилення близько 10-12 дБ.

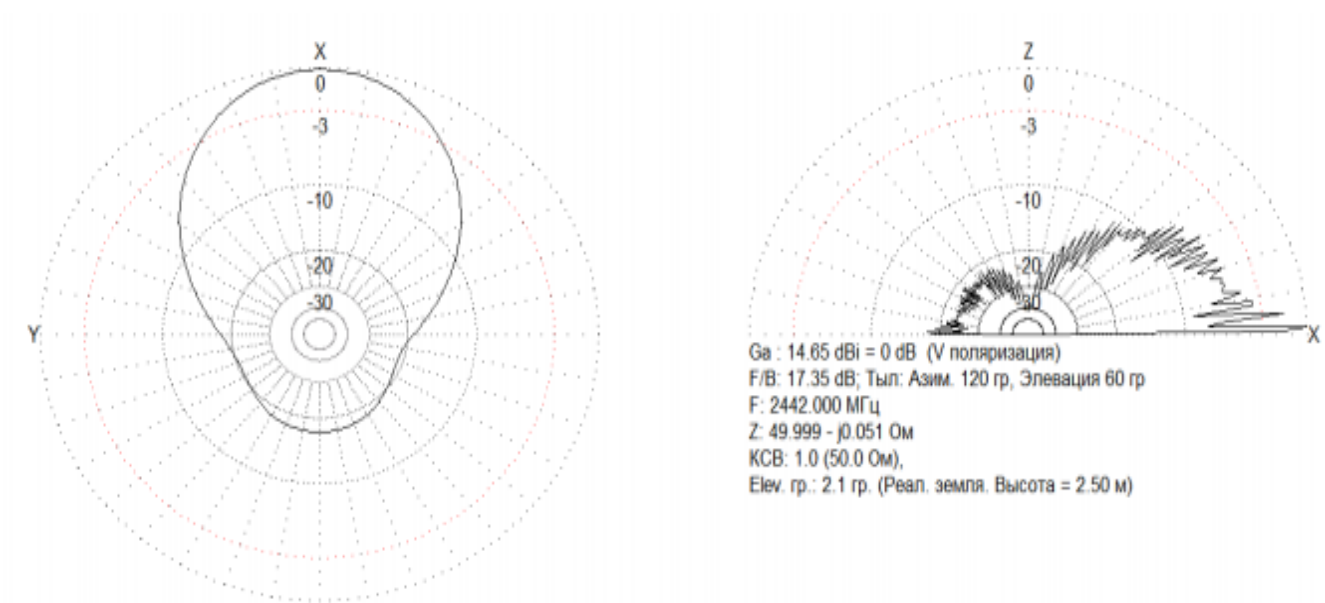


Рисунок 4.12 – Діаграма спрямованості антени Харченка



Рисунок 4.12 – Антена Харченка

Використання спрямованої антени замість штатних дозволить збільшити дальність дії за розрахунками, отриманими із формули 4.1, у 2.8 разів, за тих же самих умов. Та організувати селективність атаки у просторі у випадку застосування генератора завад GPS.

4.4 Вибір оптимального пристрою протидії квадрокоптерам для приватного використання

Для вибору кращого пристрою для приватного використання окрім запропонованих було взято ще два комерційних: DJI аероскоп та "KVS ANTIDRON-M". Вибір виконувався за допомогою методу багатокритеріальної оптимізації за сукупністю показників якості.

Таблиця 4.1 – Показники якості пристроїв протидії квадрокоптерам

Пристрій Параметр	Генератор завад GPS	Модуль NODEMCU	DJI аероскоп	"KVS ANTIDRON- M"
Радіус дії, м	9	150	5000	600 — 1200
Складність реалізації	2	3	10	10
Можливість використання без ліцензії	5	5	10	10
Вартість, грн	200	250	84 000	560 000
Час автономної роботи, години	20	30	1,5	0,6
Маса, кг	50 · 10-3	150 · 10-3	6.8	11.5
Енергоспоживання, Вт	0,45	0,4	70	380
Селективність за напрямом дії	10	10	7	9

Таблиця 4.2 – Нормовані показники якості обраних пристроїв

Пристрій Параметр	Генератор завад GPS	Модуль NODEMCU	DJI аероскоп	"KVS ANTIDRON- M"
Радіус дії	0,0018	0,03	1	0,24
Складність реалізації	0,2	0,3	1	1
Можливість використання без ліцензії	0,5	0,5	1	1
Вартість	0,0003	0,00044	0,15	1
Час автономної роботи	0,66	1	0,05	0,02
Маса	0,0004	0,001	0,6	1
Енергоспоживання	0,0011	0,0010	0,18	1
Селективність за напрямом дії	1	1	0,7	0,9

Таблиця 4.3 – Нормовані порівнянні показники якості протидії

Пристрій Параметр	Генератор завад GPS	Модуль NODEMCU	DJI аероскоп	"KVS ANTIDRON- M"
Радіус дії	0,0018	0,03	1	0,24
Складність реалізації	0,8	0,7	0	0
Можливість використання без ліцензії	0,5	0,5	1	1
Вартість	0,9997	0,99956	0,85	0
Час автономної роботи	0,66	1	0,05	0,02
Маса	0,9996	0,999	0,4	0
Енергоспоживання	0,9989	0,999	0,82	0
Селективність за напрямом дії	1	1	0,7	0,9

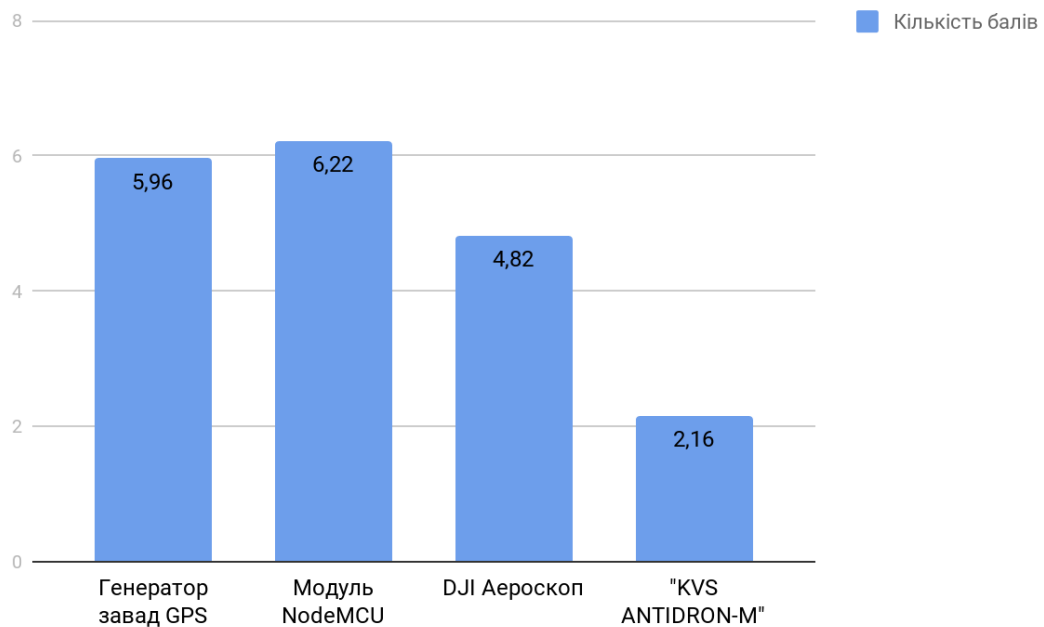


Рисунок 4.13 – Сума балів за сукупністю обраних показників якості

Як можна побачити з рис. 4.13 модуль NodeMCU є переважним для протидії дронам, які керуються за допомогою WI FI.

ВИСНОВКИ

1. В роботі розглянуті місце БпЛА в сучасному світі, галузі їх використання і в водночас ризики безпеці, які вони несуть.
2. Розглянута нормативна база, щодо використання літальних апаратів у різних країнах світу. Крім того виявлена небезпека щодо витоку приватної інформації, безпеці життю та майну людей.
3. Для вирішення проблеми захисту від БпЛА в тому числі, приватної інформації, був проведений аналіз вразливостей каналів управління квадрокоптерів та запропоновані два пристрої: WI FI джамер та генератор завад системам супутникового позиціонування дронів.
4. Дані пристрої були реалізовані практично, ефективність їх використання підтверджена шляхом експериментальних досліджень.
5. Крім того запропонована їх модернізація завдяки використанню спрямованої антени, яка була виготовлена. Її використання дозволяє збільшити радіус протидії запропонованих пристроїв та організувати селективність атаки за напрямом у випадку генератора завад GPS.
5. Проведений багатокритеріальний вибір оптимального пристрою для приватного використання. Запропоновані пристрої є достатньо ефективними та прості у виготовленні та експлуатації при менших фінансових затратах для приватного використання.

ПЕРЕЛІК ПОСИЛАНЬ

1. Unmanned aerial vehicle: сайт URL: https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle
2. RQ-2 Пионер: сайт URL: https://ru.frwiki.wiki/wiki/RQ-2_Pioneer
3. БЕЗПІЛОТНІ ПОВІТРЯНІ СУДНА: сайт URL: <https://avia.gov.ua/bezpilotni-povitryani-sudna-2/>
4. Подготовка БПЛА к геодезическим миссиям. Что нужно знать?: сайт URL: <https://skymec.ru/pravila-ispolzovaniya-dronov-v-stranah-mira/news/>
5. Малоразмерные беспилотники – новая проблема для ПВО: сайт URL: <http://army-news.ru/2015/02/malorazmernye-bespilotniki-novaya-problema-dlya-pvo/>
6. Годунов А. И., Шишков С. В., Юрков Н. К. Комплекс обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Надежность и качество сложных систем. 2014. № 2 (6). С. 62–70.
7. Поваляев Е., Хуторной С. Системы спутниковой навигации ГЛОНАСС и GPS //Ч. 3. Борьба с многолучевостью.- "Инженерная микроэлектроника". – 2002. – №. 2. – С. 23.
8. ЗСУ отримали українські гармати ANTIDRON KVSG-6 для боротьби з російськими БПЛА: сайт URL: <https://focus.ua/digital/529717-vsu-poluchili-ukrainskie-pushki-antidron-kvsg-6-dlya-borby-s-rossiyskimi-bpla-foto-i-video>
9. What is GPS Spoofing?: сайт URL: <https://www.everythingrf.com/community/what-is-gps-spoofing>
10. Timing Attack: сайт URL: <https://ropesec.com/articles/timing-attacks/>
11. DJI Aeroscope: сайт URL: <http://4vision.ru/products/dji-aeroscope.html>
12. WI FI frames: сайт URL: <http://wi-life.ru/tehnologii/wi-fi/wi-fi-frames-management-control-data>
13. Що таке вай-фай Джаммер і як зробити його своїми руками: сайт URL: <https://texnogid.biz.ua/pidkluchennya/vaj-faj-dzhammer.html>

14. Джаммери - що це? Сфера застосування глушилок зв'язку. WiFi Jammer. Спосіб установки ПО Принцип роботи: сайт URL: <https://hddrecover.ru/different/dzhammery-cto-eto-sfera-primeneniya-glushilok-svyazi-wifi-jammer/>

15. Ємельянов В.В. Конспект лекцій з дисципліни «Системи мобільного зв'язку»: конспект лекцій/В.В. Ємельянов [Електронний документ] – 48 с.

16. Рекомендації до оформлення кваліфікаційної роботи: сайт URL: https://cn.nure.ua/wp-content/uploads/2021/05/129-test_compressed.pdf