МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: Інформаційно- управляюча система для безпілотного літального апарату

Здобувача вищої освіти першого (бакалаврського) рівня,
IV курсу, групи КБ-21-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології (за галузями)»

(підпис) Бондаренка Богдана Денисовича
(прізвище, ім'я, по батькові)

Науковий керівник (підпис) Горбовий Артур Юліанович, д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Керівник освітньо-професійної програми (підпис) Омельчук Антон Анатолійович, к.т.н.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Допущено до захисту за рішенням кафедри комп'ютерних та інформаційних технологій і систем протокол від «13 » травня 2025 № 18

Завідувач кафедри (підпис) Філоненко Михайло Миколайович, к.ф.-м.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Ірпінь - 2025

Реєстрація № 62 27.06.2025 _____
(дата) (підпис відповідальної особи)

Результати перевірки до захисту 27.06.2025 _____
(до захисту, на доопрацювання) (дата) (підпис)

Результат захисту 4 (добре) 11.06.2025 _____
(оцінка) (дата) (підпис)

Голова комісії: _____ В.М. Франчук
(підпис)

Члени комісії: _____ М.М. Філоненко
(підпис)

_____ С.М. Грищенко
(підпис)

_____ А.А. Омельчук
(підпис)

БЛАНК ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст випускної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	27		Горбовий А.Ю. Франчук В.М. Філоненко М.М. Грищенко С.М. Омельчук А.А. Суховецька Л.П.
2. Дотримання вимог щодо оформлення	від 0 до 10	9		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	4		
4. Рецензент	від 0 до 5	3		
РАЗОМ БАЛІВ	від 0 до 50	43		

Оцінювання кваліфікаційної роботи науковим керівником - 32 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100- бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
75	C	4 (добре)	11.06.2025	Франчук В.М. Філоненко М.М. Грищенко С.М. Омельчук А.А. Суховецька Л.П.

ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	3 (задовільно)
50-59	E	
35-49	F X	2 (незадовільно)

Факультет фінансів та цифрових технологій
Кафедра комп'ютерних та інформаційних технологій і систем
Галузь знань 12 «Інформаційні технології»
Спеціальність 122 «Комп'ютерні науки»
Освітня програма «Інформаційні управляючі системи і технології (за галузями)»

Затверджую
Завідувач кафедри _____ Філоненко М.М.
«15» листопада 2024

Завдання на кваліфікаційну роботу
здобувачу вищої освіти
Бондаренку Богдану Денисовичу

1.Тема кваліфікаційної роботи «Інформаційно- управляюча система для безпілотного літального апарату»
Затверджена наказом ректора від «13» Листопада 2024 № 1717
2. Строк здачі закінченої роботи «5» травня 2025
3. Мета роботи: розробка програмно-апаратного комплексу для БПЛА, здатного забезпечувати стабільність керування, передачі даних та автономність функціонування в умовах активного електронного придушення чи природних аномалій.
Об'єкт дослідження: інформаційно управляючі системи керування та зв'язку безпілотних літальних апаратів в умовах радіоелектронного впливу чи інших завад.
Предмет дослідження: методи та алгоритми забезпечення стійкості до радіоелектронних перешкод у системах управління БПЛА, використання FHSS, криптографічних протоколів та інтелектуальних систем.
Орієнтовна база дослідження: актуальні рішення у сфері управління безпілотниками, включаючи технології ExpressLRS, TBS Crossfire, MAVLink.
4. Вхідні дані до роботи: наукові праці в галузях радіокерування, власні дослідження.
5. Перелік графічного матеріалу: рисунки, інтерфейси додатків, структуровані схеми, алгоритми, лістинги програм.
6. Зміст кваліфікаційної роботи (перелік питань за кожним розділом)
РОЗДІЛ 1. ТЕХНОЛОГІЧНІ АСПЕКТИ РОЗВИТКУ ТА ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ
1.1. Роль та сучасні технології безпілотних літальних апаратів
1.2. Системи керування та інформаційного забезпечення безпілотних літальних апаратів
1.3. Вплив засобів радіоелектронної боротьби на функціонування безпілотних літальних апаратів
1.4. Програмні рішення для підвищення надійності керуючих систем
БПЛА
1.5. Використання штучного інтелекту для БПЛА
РОЗДІЛ 2. СИСТЕМИ ЗВ'ЯЗКУ, ПРОТОКОЛИ ТА ШИФРУВАННЯ
2.1. Протоколи зв'язку та шифрування даних
2.2. Вплив інформаційних управляючих систем на методи навігації та захист БПЛА від радіоелектронного впливу
2.3. Опис бібліотек програмування, що використовують для реалізації систем
2.4. Аналіз сучасних протоколів зв'язку та їх стійкість до перешкод
2.5. Розробка алгоритмів і функціональних систем

РОЗДІЛ 3. ПРАКТИЧНИЙ АНАЛІЗ ТА ПОДОЛАННЯ РАДІОЕЛЕКТРОННИХ ПЕРЕШКОД

3.1. Практичний аналіз сучасних систем створення радіоелектронних перешкод та їх вплив на БП

3.2. Подолання радіоелектронних перешкод у системах керування дронами

3.3. Застосування програмного забезпечення для практичного використання

7. Календарний план виконання роботи

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури кваліфікаційної роботи	до 01.11.2024	01.11.2024
2	І розділ (аналіз предметної області: огляд систем управління даними для малого бізнесу)	30.01.2025	30.01.2025
3	ІІ розділ (Проектування архітектури системи та моделювання бази даних)	28.02.2025	28.02.2025
4	ІІІ розділ (реалізація системи керування даними, перевірка функціональних можливостей)	30.04.2025	30.04.2025
5	Висновки	05.05.2025	05.05.2025
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	25.05.2025	25.05.2025
7	Отримання відгуку керівника	25.05.2025	25.05.2025
8	Отримання зовнішньої рецензії	28.05.2025	28.05.2025

8.Дата видачі завдання «15» листопада 2024р.

9. Керівник кваліфікаційної роботи _____ Горбовий А.Ю.
(підпис)

10. Керівник освітньо-професійної програми _____ Омельчук А.А.
(підпис)

11. Завдання до виконання отримав здобувач вищої освіти _____ Бондаренко Б.Д.
(підпис)

АНОТАЦІЯ

(Інформаційно- управляюча система для безпілотного літального апарату)

Метою роботи є розробка програмно-апаратного комплексу для БПЛА, здатного забезпечувати стабільність керування, передачі даних та автономність.

Завдання роботи є аналіз існуючих методів забезпечення стійкості БПЛА до РЕБ шляхом розробки адаптивних алгоритмів зв'язку на базі протоколів FHSS.

Предмет дослідження є методи та алгоритми забезпечення стійкості до радіоелектронних перешкод у системах управління БПЛА.

Об'єктом дослідження виступають інформаційно управляючі системи керування та зв'язку безпілотних літальних апаратів в умовах радіоелектронного впливу чи інших завад.

Базою дослідження виступає комплекс інформаційних управляючих систем, що висвітлені у наукових працях та публікаціях, відкритих джерелах та особистих напрацювань.

За результатами дослідження сформульовані висновки про можливості інтеграції в існуючі програмні продукти елементів автономізації, що покращують якість зв'язку та польоту.

Одержані результати можуть бути використані для практичного застування в автономних системах наземного та повітряного переміщення малих суден типу БПЛА чи НРК в цивільних чи військових цілях.

Кваліфікаційна робота містить 43 сторінки, 3 таблиці, 8 рисунків, список використаних джерел з найменувань, 9 додатків.

Ключові слова: **БПЛА** – безпілотні літальні апарати; **FHSS** – (Frequency Hopping Spread Spectrum); **РЕБ** – радіоелектронна боротьба; **інформаційно керуюча система** – технологія, що використовується автономного керування та прийняття рішень; **криптографія** – захист зв'язку та команд за допомогою шифрування.

Рік виконання кваліфікаційної роботи 2025.

Рік захисту роботи 2025.

ANNOTATION

(Information and Control System for an Unmanned Aerial Vehicle)

The aim of this work is to develop a hardware-software system for UAVs capable of ensuring control stability, data transmission, and autonomy.

The task of the work is to analyze existing methods for ensuring UAV resistance to electronic warfare by developing adaptive communication algorithms based on FHSS protocols.

The subject of the research is methods and algorithms for ensuring resistance to electronic interference in UAV control systems.

The object of the research is the information and control systems for UAV navigation and communication under conditions of electronic interference or other disturbances.

The research is based on a set of information and control systems described in scientific papers, publications, open sources, and personal developments.

Based on the research, conclusions were formulated regarding the integration possibilities of autonomy-enhancing components into existing software solutions, which improve communication quality and flight performance.

The obtained results can be used for practical applications in autonomous systems for ground and aerial movement of small vehicles such as UAVs or UGVs, for both civilian and military purposes.

The qualification work contains 43 pages, 3 tables, 8 figures, a list of references, and 9 appendices.

Keywords: UAV – Unmanned Aerial Vehicles; FHSS – Frequency Hopping Spread Spectrum; EW – Electronic Warfare; Information and Control System – a technology used for autonomous control and decision-making; Cryptography – protection of communication and commands via encryption.

Year of completion: 2025

Year of defense: 2025

ЗМІСТ

ВСТУП.....8

РОЗДІЛ 1. ТЕХНОЛОГІЧНІ АСПЕКТИ РОЗВИТКУ ТА ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ.....12

1.1. Роль та сучасні технології безпілотних літальних апаратів.....12

1.2. Системи керування та інформаційного забезпечення безпілотних літальних апаратів.....14

1.3. Вплив засобів радіоелектронної боротьби на функціонування безпілотних літальних апаратів.....15

1.4. Програмні рішення для підвищення надійності керуючих систем БПЛА.....17

1.5. Використання штучного інтелекту для БПЛА.....20

РОЗДІЛ 2. СИСТЕМИ ЗВ'ЯЗКУ, ПРОТОКОЛИ ТА ШИФРУВАННЯ …..25

2.1. Протоколи зв'язку та шифрування даних.....25

2.2. Вплив інформаційних управляючих систем на методи навігації та захист БПЛА від радіоелектронного впливу.....28

2.3. Опис бібліотек програмування, що використовують для реалізації систем.....29

2.4. Аналіз сучасних протоколів зв'язку та їх стійкість до перешкод.....32

2.5. Розробка алгоритмів і функціональних систем.....34

РОЗДІЛ 3. ПРАКТИЧНИЙ АНАЛІЗ ТА ПОДОЛАННЯ РАДІОЕЛЕКТРОННИХ ПЕРЕШКОД.....36

3.1. Практичний аналіз сучасних систем створення радіоелектронних перешкод та їх вплив на БПЛА.....36

3.2. Подолання радіоелектронних перешкод у системах керування дронами.....37

3.3. Застосування програмного забезпечення для практичного

використання.....38
ВИСНОВКИ.....41
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....44
ДОДАТКИ.....48.

ВСТУП

Сучасний розвиток безпілотних літальних апаратів (БПЛА) відкриває нові горизонти у військовій, комерційній та дослідницькій сферах. Водночас, зростаюча загроза радіоелектронного впливу вимагає принципово нових підходів до побудови інформаційно-управляючих систем. Зокрема, у військових умовах, де застосовуються засоби радіоелектронної боротьби (РЕБ), або в цивільних галузях, де наявні природні перешкоди, рельєф чи магнітні аномалії, виникає потреба у створенні стійких до перешкод систем управління БПЛА.

Актуальність теми. В умовах сучасних конфліктів, та розвитку галузі де активно застосовуються засоби РЕБ, забезпечення надійного зв'язку та управління БПЛА стає критично важливим. Традиційні системи зв'язку виявляються вразливими до перешкод, що зумовлює необхідність розробки нових методів, здатних забезпечити стійкість до радіоелектронного впливу наявними апаратними засобами проте з можливістю вдосконалення систем управління програмними продуктами.

Стан і ступінь розробки проблеми. У науковій літературі та практичних розробках приділяється значна увага питанням забезпечення стійкості БПЛА до РЕБ. Зокрема, досліджуються методи частотного розмивання (FHSS), адаптивного управління частотами, використання криптографічних протоколів та інтеграція інтелектуальних систем для автономного прийняття рішень. Проте, існує потреба у комплексному підході, що поєднує ці методи для досягнення високої стійкості до перешкод.

Об'єкт дослідження: інформаційно управляючі системи керування та зв'язку безпілотних літальних апаратів в умовах радіоелектронного впливу чи інших завад.

Предмет дослідження: методи та алгоритми забезпечення стійкості до радіоелектронних перешкод у системах управління БПЛА, зокрема, використання FHSS, криптографічних протоколів та інтелектуальних систем.

Мета роботи: розробка програмно-апаратного комплексу для БПЛА, здатного забезпечувати стабільність керування, передачі даних та автономність функціонування в умовах активного електронного придушення чи природних аномалій.

Завдання дослідження:

1. Аналіз існуючих методів забезпечення стійкості БПЛА до РЕБ шляхом розробки адаптивних алгоритмів зв'язку на базі протоколів FHSS із динамічним перестроюванням частот.

2. Інтеграція гібридної навігаційної системи, що поєднує обробку даних GPS, інерційних сенсорів (IMU) та комп'ютерного зору через фільтр Калмана і SLAM-алгоритми.

3. Реалізація механізмів криптографічного захисту (AES-256, ECC) для команд керування та телеметрії.

4. Розробка системи автономного ухвалення рішень на основі нейромереж для аналізу загроз, оптимізації маршрутів та корекції польоту без зовнішнього втручання.

5. Тестування та оцінка ефективності розробленого комплексу в умовах імітованих радіоперешкод на прикладі власного зібраного апаратного та програмного продукту шляхом вдосконалення відкритого програмного коду.

Методи дослідження: аналіз та синтез інформаційних систем, моделювання та симуляція, розробка програмного забезпечення, експериментальні дослідження в лабораторних умовах.

Практична значимість: Розроблений програмно-апаратний комплекс може бути використаний для забезпечення стійкого управління БПЛА в умовах активного радіоелектронного впливу, що є актуальним для військових та спеціальних операцій, цивільних місій, задач картографування та моніторингу, тощо.

Наукова новизна: Інтеграція адаптивних методів зв'язку, криптографічного захисту та інтелектуальних систем управління в єдиний комплекс для забезпечення стійкості БПЛА до РЕБ.

Особистий внесок здобувача: розробка та реалізація програмних модулів, проведення експериментальних досліджень збірки та налаштування дрону, аналіз отриманих результатів, дописування відкритого програмного продукту для роботи на персоналізованих частотах

Апробація результатів дослідження: Результати дослідження були представлені на прикладі власного зібраного дрону розміром 7 дюймів та прошивки політного контролера з відеопередавачем дописаним програмним кодом керування радіоприймальним модулем.

Таким чином, дана кваліфікаційна робота спрямована на вирішення актуальної проблеми забезпечення стійкості БПЛА до радіоелектронного впливу шляхом розробки комплексного програмно-апаратного рішення.

Використані в роботі джерела спільно з особистими дослідженнями забезпечують глибоке розуміння сучасних технологій та методів, що використовуються в розробці стійких до перешкод систем управління БПЛА, і можуть служити основою для подальших досліджень та розробок у цій галузі, зокрема:

- Дослідження виявлення FHSS як одну з основних технік зв'язку в безпілотних авіаційних системах (UAS), підкреслюючи її здатність протидіяти перешкодам та забезпечувати стійкий зв'язок.

- Аналіз узгодженості алгоритмів A-SLAM для навігації БПЛА, що є критичним при відсутності GPS-сигналу.

- Огляд сучасних алгоритмів візуального SLAM для БПЛА, зосереджений на реальному часі, текстурованих та динамічних середовищах .

- Огляд підкреслює ефективність FHSS у забезпеченні безпечного бездротового зв'язку завдяки стійкості до перешкод та прослуховування.

- Огляд т опрацювання наукових праць та публікацій, відомості NATO MSG-SET-183, відкритих джерел та особистих напрацювань.

Робота демонструє, що інтеграція низькорівневих програмних оптимізацій з високорівневими інтелектуальними системами є ключем до створення стійких інформаційно-управляючих комплексів для безпілотної авіації нової генерації.

РОЗДІЛ 1. ТЕХНОЛОГІЧНІ АСПЕКТИ РОЗВИТКУ ТА ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

1.1. Роль та сучасні технології безпілотних літальних апаратів

Безпілотні літальні апарати (БПЛА) стали невід'ємною частиною сучасного технічного прогресу та мають широке застосування у різних сферах діяльності. Їхня популярність зумовлена високою маневровістю, здатністю виконувати автономні задачі, а також гнучкістю у модифікації функціоналу відповідно до потреб користувачів. Розвиток електроніки, програмного забезпечення та штучного інтелекту значно розширив можливості використання БПЛА, зробивши їх більш адаптивними до складних умов експлуатації.

Перші зразки безпілотних апаратів були розроблені ще у XX столітті для військових цілей, але з часом їхня сфера застосування розширилася і включає сьогодні такі напрямки, як:

- Військові операції - використання дронів для розвідки, наведення, бойових завдань.
- Дослідницькі місії - аерофотозйомка, моніторинг місцевості, екологічні дослідження.
- Комерційні перевезення - транспортування товарів у логістичних компаніях.
- Наукові дослідження - використання в археології, геології, метеорології.

За принципом праці та характеристиками БПЛА можна розрізняти за кількома критеріями: мікродрони, малі середні та великі апарати. За призначенням: військові, цивільні, дослідницькі, комерційні моделі. За типом управління: автономні та дистанційно керовані безпілотники, а за типом живлення вони поділяються на електричні, гібридні та паливні варіанти.

Сучасні безпілотні літальні апарати оснащені технологіями, які забезпечують стабільну роботу навіть у складних умовах. До ключових елементів входять навігаційні системи, серед яких GPS, INS, лазерна навігація, що дозволяє здійснювати точне позиціонування в просторі. Системи зв’язку

включають супутникові канали, адаптивні протоколи передачі даних, радіочастотні модуляції, що сприяють стабільному управлінню дроном на великих відстанях [12].

Інша важлива складова - автономні алгоритми управління, що включають адаптивні навчання та нейронні мережі, які допомагають автоматично оптимізувати траєкторію та ухвалювати рішення в реальному часі. Оптичні та тепловізійні сенсори дають можливість аналізувати навколишнє середовище, забезпечуючи високу ефективність роботи апаратів в умовах недостатньої освітленості або складних метеорологічних умов.

У зв’язку і з розвитком засобів радіоелектронної боротьби, технології захисту БПЛА стали важливим напрямком досліджень. Безпілотні апарати можуть зазнавати глушіння GPS-сигналів, перехоплення керування, також електронного впливу на системи, що може призвести до втрати контролю над апаратом. Сучасні методи протидії включають адаптивні алгоритми зв’язку, багатоканальні модулі передачі інформації та автономні навігаційні системи, що керування навіть у критичних умовах [12].

Вибір технологій для інформаційно управляючої системи БПЛА повинен базуватися на таких критеріях, як стійкість до зовнішніх перешкод, гнучкість у модернізації, ефективність реалізації алгоритмів автономного керування та здатність до інтеграції штучного інтелекту для оптимізації роботи безпілотного апарату.

Реалізація сучасних технологій дозволяє створити ефективну інформаційно-управляючу систему для БПЛА, що здатна функціонувати навіть в умовах активного електронного впливу, гарантує стабільність управління та забезпечує надійний захист від стороннього втручання.

1.2. Системи керування та інформаційного забезпечення безпілотних літальних апаратів

Сучасні безпілотні літальні апарати (БПЛА) базуються на складних програмних комплексах, які забезпечують їх стабільну роботу, автономність та ефективність виконання завдань. Програмна архітектура БПЛА включає кілька ключових компонентів, кожен з яких відіграє важливу роль у функціонуванні системи [12].

Основним елементом є автопілот, який відповідає за стабілізацію польоту, управління двигунами та виконання заданих траєкторій. Він зазвичай реалізується за допомогою алгоритмів автоматичного керування, таких як PID-регулятори, адаптивні системи або нейромережні методи. Популярні програмні рішення, такі як PX4 або ArduPilot, надають готові фреймворки для розробки автопілотів, що дозволяє зосередитись на специфічних задачах, а не на базовій реалізації.

Важливу роль відіграє обробка даних від різноманітних сенсорів, включаючи GPS-приймачі, інерційні вимірювальні блоки (IMU), камери та лідари. Для інтеграції цих даних використовуються методи сенсорного ф’южну, такі як фільтр Калмана або сучасні SLAM-алгоритми (наприклад, ORB-SLAM), які дозволяють БПЛА точно визначати своє положення в просторі та будувати карти навколишнього середовища [7].

Навігаційний модуль відповідає за планування маршруту, уникнення перешкод та прийняття рішень у реальному часі. Для цього застосовуються алгоритми пошуку шляху (A, RRT), а також методи машинного навчання для розпізнавання об’єктів і аналізу ситуації. Сучасні системи все частіше використовують глибоке навчання для покращення точності та адаптивності навігації.

Комунікаційний підсистема забезпечує зв’язок з наземними станціями, іншими БПЛА або центрами обробки даних. Для передачі інформації

використовуються протоколи, такі як MAVLink, а також бездротові технології (Wi-Fi, радіоканали, 5G). Захист даних реалізується за допомогою криптографічних методів, що запобігає кібератакам та несанкціонованому доступу.

Розвиток програмного забезпечення для БПЛА спрямований на підвищення автономності, надійності та інтелектуальних можливостей систем. Використання штучного інтелекту, хмарних обчислень та розподілених архітектур відкриває нові перспективи для створення повністю самостійних апаратів, здатних ефективно працювати у складних умовах.

1.3. Вплив засобів радіоелектронної боротьби на функціонування безпілотних літальних апаратів

Розвиток безпілотних літальних апаратів (БПЛА) значно змінив підходи до ведення військових операцій, цивільного моніторингу та логістичних завдань.

Водночас засоби радіоелектронної боротьби стали одним із ключових факторів, що впливають на функціонування таких систем. Засоби створення радіоелектронних перешкод призначені для порушення або блокування електронних сигналів, які використовуються БПЛА для навігації, передачі даних та дистанційного керування. Вплив радіоелектронних перешкод може призвести до порушення зв’язку між оператором та дроном, втрати навігації або повного виходу апарату з ладу. Засоби радіоелектронних перешкод спрямовані на різні компоненти безпілотних систем, включаючи канали зв’язку, навігацію, сенсорні системи та програмне забезпечення, основні види впливу можна розділити на три основні категорії: глушіння сигналів зв’язку - створення радіочастотних перешкод, що призводять до втрати керування дроном або припинення передачі даних; спотворення навігаційних даних - модифікація GPS-сигналів, що викликає помилки у визначенні координат БПЛА та веде до дезорієнтації у просторі; кібернетичні атаки - спроби втручання у програмне забезпечення безпілотного апарата з метою перехоплення керування або зміни алгоритмів роботи [11]. Ефективність БПЛА значно залежить від стабільності його

електронних компонентів, тому застосування засобів створення радіоелектронних перешкод може створювати серйозні проблеми в роботі дрона, подано в табл.1.1.

Таблиця 1.1

Вплив та наслідки засобів радіоелектронної боротьби на функціонування безпілотних систем

Тип впливу	Наслідки для БПЛА
Глушіння зв’язку	Втрата керування, переривання передачі даних
Спотворення GPS	Дезорієнтація, неправильне визначення координат
Кібернетична атака	Перехоплення управління, зміна алгоритмів роботи
Перешкоди сенсорів	Некоректна обробка даних навколишнього середовища

Джерело: [Авторське]

Щоб зменшити негативний вплив засобів радіоелектронних перешкод, сучасні БПЛА використовують різноманітні методи захисту: резервні канали зв’язку - використання альтернативних частотних діапазонів або супутникових зв’язкових систем; фільтрація GPS-сигналів - застосування удосконалених алгоритмів корекції координат, що дозволяють виявляти спотворення навігаційних даних; криптографічний захист даних - шифрування переданих

команд і телеметричних даних для запобігання їхньому перехопленню; автономні системи управління - використання алгоритмів машинного навчання та нейромереж для адаптивного польоту без зовнішнього керування. Розвиток технологій штучного інтелекту та обчислювальних потужностей відкриває нові можливості для підвищення захисту безпілотних літальних апаратів. Системи адаптивного управління, що можуть змінювати частоти зв'язку у випадку виявлення перешкод, а також нові методи квантового шифрування забезпечують більш високий рівень безпеки даних. У майбутньому можна очікувати появу нових інтегрованих рішень, які дозволять дронам ефективно протистояти засобам радіоелектронних перешкод, мінімізуючи ризики порушення їхньої роботи.

Таким чином, дослідження впливу засобів радіоелектронних перешкод на функціонування БПЛА є критично важливим для розвитку безпілотних технологій. Впровадження ефективних механізмів захисту та розробка нових методів адаптивного управління дозволить значно підвищити стійкість безпілотних систем до радіоелектронного впливу.

1.4. Програмні рішення для підвищення надійності керуючих систем БПЛА

Розробка інформаційно-управляючої системи для безпілотних літальних апаратів (БПЛА) потребує ретельного вибору програмного забезпечення, що забезпечують надійне функціонування в умовах радіоелектронного впливу.

Вибір повинен враховувати такі ключові критерії, як продуктивність, захист від зовнішніх перешкод, адаптивність алгоритмів управління та можливість інтеграції штучного інтелекту.

Сучасні системи управління безпілотними літальними апаратами (БПЛА) базуються на комплексному використанні апаратних рішень, програмного забезпечення та інтелектуальних алгоритмів обробки даних. Ці технології забезпечують високу автономність, надійність та ефективність роботи апаратів у різноманітних умовах експлуатації. Програмне забезпечення систем управління

включає спеціалізовані операційні системи реального часу (RTOS), алгоритми автоматичного керування на базі нейронних мереж та методи обробки сенсорних даних. Для забезпечення точної навігації використовуються GPS-модулі в поєднанні з інерційними датчиками (IMU), що дозволяє компенсувати вплив радіоелектронних перешкод. Сучасні системи також інтегрують алгоритми машинного навчання для аналізу навколишнього середовища та прийняття рішень у автономному режимі [12].

Програмне забезпечення відіграє ключову роль у стабільності роботи безпілотних систем. Використання платформ ArduPilot, PX4, Be0taflight, iNav дозволяє реалізувати автономні функції керування та обробки даних з сенсорів у реальному часі[5].

Для аналізу польотних траєкторій застосовуються інструменти моделювання, такі як MATLAB та Simulink, а інтеграція машинного навчання можлива через TensorFlow та PyTorch, подано в табл.1.2. Вплив радіоелектронних перешкод на БПЛА вимагає застосування технологій захисту, серед яких шифрування команд керування, використання резервних каналів зв’язку та алгоритмів адаптивного управління[10].

Використання криптографічних методів дозволяє запобігти перехопленню даних, а впровадження автономних алгоритмів сприяє підвищенню надійності системи у складних умовах. Розвиток штучного інтелекту відкриває нові можливості для підвищення ефективності інформаційно-управляючих систем БПЛА. Використання нейромережевих алгоритмів та адаптивних методів управління дозволяє покращити стійкість дронів до зовнішніх загроз та забезпечує точне виконання польотних завдань.

Таблиця 1.2

Порівняння платформ керування БПЛА

Платформа	Призначення	Основні можливості	Фото
ArduPilot	Автономне керування БПЛА	Підтримка мультикоптерів, літаків, наземних роботів	(Додаток А.1)
PX4	Система польотного контролю	Відкрита архітектура, висока продуктивність	(Додаток А.2)
Betaflight	ПЗ для FPV-дронів	Оптимізація польоту, висока швидкість реакції	(Додаток А.3)
iNav	GPS-орієнтоване керування БПЛА	Стабільна навігація, розширена телеметрія	(Додаток А.4)
MATLAB/Simulink	Моделювання польоту	Аналіз траєкторій, симуляція динаміки	(Додаток А.5)
TensorFlow/PyTorch	Машинне навчання	Нейронні мережі, прогнозування траєкторій	(Додаток А.6)

Джерело: [Авторське]

Таким чином, обґрунтований вибір технологій та програмного забезпечення є критично важливим для забезпечення стійкої роботи інформаційно-управляючої системи БПЛА. Оптимальне поєднання апаратних платформ, програмних рішень та алгоритмів машинного навчання дозволяє створити ефективну систему управління, яка здатна протистояти радіоелектронним загрозам та забезпечувати автономність у виконанні поставлених завдань.

1.5. Використання штучного інтелекту для БПЛА

Штучний інтелект починає відігравати ключову роль у сучасних безпілотних літальних апаратах, забезпечуючи автономне керування, адаптацію до навколишнього середовища та оптимізацію виконання завдань. Завдяки використанню алгоритмів машинного навчання та нейронних мереж дрони здатні аналізувати отримані дані, ухвалювати рішення у реальному часі та підвищувати ефективність польотних операцій. Однією з ключових переваг використання штучного інтелекту в безпілотних апаратах є можливість здійснювати польоти без втручання оператора. В умовах складного середовища дрони можуть самостійно ухвалювати рішення, коригувати маршрути та адаптуватися до змін у реальному часі, що забезпечує підвищену ефективність їхньої роботи. Ця технологія стала революційною, особливо у військовій галузі, де автономні дрони можуть виконувати завдання розвідки, спостереження та навіть бойові місії.

Штучний інтелект у дронах базується на таких технологіях. Машинне навчання дозволяє дронам навчатися на основі великих обсягів даних про навколишнє середовище, прогнозувати рух перешкод та адаптувати маршрут. Глибоке навчання забезпечує використання багатошарових нейронних мереж для розпізнавання об’єктів, оцінки ризиків та оптимального маневрування. Автономне ухвалення рішень дає можливість змінювати траєкторію польоту та коригувати параметри руху без втручання оператора. Одним з важливих аспектів використання штучного інтелекту є прогнозування поведінки об’єктів навколо дрона. Наприклад, у сфері цивільної авіації дрони з інтелектуальним управлінням можуть аналізувати рух транспортних засобів на дорогах, прогнозувати місця можливих заторів та оптимізувати маршрути доставки [10].

Автономність дронів забезпечується завдяки інтелектуальним системам, що включають:

– обробку зображень та відео через камери високої роздільної здатності, які аналізують навколишнє середовище для ідентифікації об’єктів, перешкод або цільових точок;

– алгоритми прогнозування траєкторії, що дозволяють оптимізувати маршрут на основі даних про вітер, перешкоди та рельєф місцевості;

– системи ухвалення рішень, які використовують логічні моделі, що дозволяють визначати безпечні маневри у непередбачуваних умовах. В умовах міських ландшафтів це має особливе значення, оскільки штучний інтелект дозволяє дронам ефективно оминати будівлі, мости та інші перешкоди.

Важливими компонентами інтеграції штучного інтелекту в БПЛА є:

– розпізнавання мовних команд, що дає можливість керування дроном за допомогою голосових інструкцій або спеціальних команд;

– оптимізація комунікаційних алгоритмів, яка сприяє створенню захищених каналів зв’язку для запобігання перехопленню даних;

– інтеграція GPS та інерційних навігаційних систем, що підвищує точність навігації у складних умовах, зокрема при впливі засобів радіоелектронної боротьби.

Нейронні мережі активно застосовуються для:

– класифікації об’єктів, що дозволяє розпізнавати транспортні засоби, людей, споруди, а також небезпечні перешкоди;

– аналізу польотних параметрів для прогнозування змін траєкторії з урахуванням впливу навколишнього середовища;

– автоматичного коригування польоту: адаптації висоти, швидкості та напрямку руху залежно від змінних умов.

Використання штучного інтелекту дозволяє дронам ефективно виконувати такі задачі, як розвідувальні місії для аналізу місцевості, пошуку об’єктів та моніторингу стану території; логістичні операції, що включають перевезення вантажів з автономною маршрутизацією; рятувальні операції, що дозволяють

здійснювати пошук людей у важкодоступних місцях на основі аналізу теплових та оптичних сигналів [10].

Подальший розвиток штучного інтелекту у безпілотних апаратах передбачає вдосконалення алгоритмів самонавчання, інтеграцію квантових обчислень для швидкої обробки даних, а також розширення можливостей нейромережевих систем в аналізі складних польотних сценаріїв. Також перспективним напрямом є інтеграція технологій розподіленого обчислення, що дозволяє дронам обмінюватися інформацією між собою в режимі реального часу. Таким чином, впровадження штучного інтелекту у дрони суттєво покращує їхню автономність, гнучкість та ефективність у виконанні різних завдань. Інтелектуальні алгоритми дозволяють безпілотним апаратам працювати у складних умовах та швидко адаптуватися до змін навколишнього середовища.

Штучний інтелект у безпілотних літальних апаратах розширює можливості автономного управління, інтерактивного аналізу навколишнього середовища та оптимізації польотних маршрутів. Ця технологія стала незамінною в багатьох сферах, зокрема у військовій розвідці, картографії, логістиці та навіть агросекторі. Завдяки здатності ШІ обробляти величезні обсяги даних у режимі реального часу, сучасні дрони можуть здійснювати польоти із самонавчанням, аналізуючи параметри погодних умов, місцевості та поведінку об’єктів навколо [10].

Одним із ключових аспектів використання ШІ у дронах є інтеграція алгоритмів розпізнавання образів та комп’ютерного зору. Це дозволяє безпілотним апаратам ідентифікувати об'єкти на землі, розрізняти перешкоди та здійснювати складні маневри без втручання оператора. Камери високої роздільної здатності у поєднанні з потужними обчислювальними модулями забезпечують ефективну обробку отриманих зображень та відеопотоків. Важливим напрямом досліджень є використання технологій глибокого навчання для розпізнавання аномалій, що може бути корисним у пошуково-рятувальних операціях або моніторингу територій, де існують ризики природних катастроф.

Ще однією важливою сферою застосування ШІ є вдосконалення систем навігації та стабілізації польоту. Традиційні GPS-системи мають свої обмеження у складних умовах, таких як міські зони з високою щільністю забудови чи регіони з активним радіоелектронним впливом. Інтеграція нейромережевих моделей у навігацію дозволяє дронам використовувати альтернативні методи орієнтації, такі як оптичне картографування, визначення положення за інерційними сенсорами та аналіз даних з радарів. Це забезпечує підвищену точність польоту навіть за умов втрати GPS-сигналу або значного електронного шуму.

Розвиток адаптивного управління є ще одним перспективним напрямом інтеграції ШІ у безпілотні апарати. Технології машинного навчання дозволяють дронам коригувати свої дії відповідно до змін у навколишньому середовищі. Наприклад, якщо дрон стикається з сильним вітром або механічними перешкодами, його система управління може миттєво змінити траєкторію руху, уникнувши аварійної ситуації. Також важливу роль відіграє можливість прогнозування поведінки об'єктів поблизу — наприклад, руху інших літальних апаратів або наземного транспорту [10].

Подальші дослідження у сфері ШІ спрямовані на підвищення рівня взаємодії дронів із операторами та іншими автономними системами. Впровадження технологій розпізнавання голосових команд, обробки природної мови та комунікації через хмарні сервіси забезпечує можливість створення групових тактичних систем, де дрони можуть координувати свої дії між собою. Це дозволяє підвищити ефективність виконання складних місій, таких як рійовий політ для великомасштабного картографування чи розвідувальних операцій.

Таким чином, впровадження штучного інтелекту у безпілотні літальні апарати значно розширює їх функціональні можливості, забезпечуючи автономне управління, складну аналітику навколишнього середовища та високу адаптивність до змінних умов експлуатації. Майбутній розвиток таких систем включатиме інтеграцію квантових обчислень, вдосконалення алгоритмів

нейромережевого аналізу та створення багаторівневих адаптивних систем управління, що зробить дрони ще більш ефективними та надійними у виконанні складних задач [10].

РОЗДІЛ 2. СИСТЕМИ ЗВ'ЯЗКУ, ПРОТОКОЛИ ТА ШИФРУВАННЯ

2.1. Протоколи зв'язку та шифрування даних

Сучасні безпілотні літальні апарати (БПЛА) базуються на складних інформаційних системах, де ключову роль відіграють комунікаційні протоколи та інфраструктура обміну даними. Вибір та інтеграція комунікаційних систем є критичними для забезпечення стабільного зв'язку, надійної передачі команд керування та ефективного отримання потоків телеметричних даних у реальному часі. Оптимальна конфігурація цих систем визначає точність керування, особливо в умовах високого навантаження або при наявності перешкод.

До ключових технологій комунікаційних систем БПЛА належать наступні наведені нижче.

Протоколи радіочастотного зв'язку: Найширше використання знаходять системи, що працюють у діапазонах 2.4 GHz (з використанням протоколів типу Wi-Fi 802.11n/ac, спеціалізованих протоколів контролера) та 5.8 GHz (часто для FPV-відеопотоку). Вони забезпечують високу пропускну здатність для швидкої передачі керуючих команд та даних, що є критичним для FPV-дронів та гоночних моделей, де необхідна мінімальна затримка (low latency).

Протоколи для дальнього зв'язку: Для операцій на великих відстанях або в умовах складної прохідності сигналу використовуються системи на частотах 433 MHz та 915 MHz. Ці частоти, часто реалізовані через протоколи типу LoRa (Long Range) або спеціалізовані радіомодеми, забезпечуючи кращу проникність сигналу крізь перешкоди (будівлі, ліси) завдяки більшій довжині хвилі, хоча зазвичай мають меншу пропускну здатність[2].

Системи обробки телеметрії: Отримання даних телеметрії (положення, стан систем, показники сенсорів) потребує їх кодування, передачі за спеціальними протоколами (наприклад, MAVLink - стандартний протокол для БПЛА) та інтеграції в наземну контрольну станцію для подальшої обробки та

візуалізації. Надійність цього потоку даних критична для моніторингу стану апарата [1].

Одним із сучасних рішень для стабільного зв’язку є LoRa, що працює на низьких частотах і позволяє передавати сигнал на значні відстані з мінімальною витратою енергії. У складних умовах використовуються технології FHSS (Frequency Hopping Spread Spectrum), що динамічно змінюють частоту передачі сигналу, запобігаючи глушінню та перехопленню сигналу.

З точки зору безпеки, важливу роль відіграє шифрування даних. Передові алгоритми захисту, такі як AES (Додаток Б) та ECC, дозволяють запобігти перехопленню команд керування та захистити передану телеметричну інформацію від стороннього втручання.

Алгоритм AES (Advanced Encryption Standard) є симетричним алгоритмом блочного шифрування, який використовує ключі розміром 128, 192 або 256 біт. Він складається з кількох раундів, кожен з яких включає підстановку, перестановку та змішування даних. Це забезпечує високий рівень безпеки та ефективності.

Нижче наведено приклад реалізації AES на Python з використанням бібліотеки pycryptodome що використовується як доповнення відкритого програмного коду для шифрування даних:

- *Шифрування даних*

```
data = b'Confidential data'
nonce = cipher.nonce
ciphertext, tag = cipher.encrypt_and_digest(data)
```

- *Декодування*

```
cipher_dec = AES.new(key, AES.MODE_EAX, nonce=nonce)
plaintext = cipher_dec.decrypt(ciphertext)
try:
    cipher_dec.verify(tag)
    print("The message is authentic:", plaintext)
```

except ValueError:

print("Key incorrect or message corrupted") [6].

Значну роль відіграють протоколи зв’язку, які забезпечують стабільну комунікацію між контролером польоту, наземною станцією та FPV- системою.

Для передачі команд керування використовуються кілька ключових протоколів: SBUS, IBUS, CRSF (Crossfire), FPort, MSP. SBUS є одним із найпопулярніших варіантів завдяки низькій затримці та стабільності сигналу, що критично важливо для швидкодійних FPV-дронів. CRSF, розроблений для дальньої дії, позволяє підтримувати безперебійне з’єднання навіть на відстані понад 10 км, використовують метод псевдовипадкового перелаштування робочої частоти для уникнення перешкод.

Окремий напрям у зв’язку БПЛА - передача відео та телеметрії, що позволяє операторам отримувати візуальні дані у реальному часі та контролювати стан апарата. FPV-системи можуть використовувати аналоговий (PAL/NTSC) або цифровий (DJI FPV, HDZero, Walksnail та OpenIPC) формат. Аналогові варіанти мають мінімальну затримку, що робить їх ідеальними для швидких польотів, тоді як цифрові забезпечують високу якість зображення та розширені можливості телеметрії [8].

Симуляція роботи дрона у зоні сильних перешкод показала, що використання CRSF, динамічних алгоритмів зміни частоти значно покращує стабільність керування, знижує ризики втрати сигналу та забезпечує високий рівень безпеки у складних умовах.

Тому грамотний підбір протоколів зв’язку та передових FPV-систем є критично важливим для стабільної роботи дронів у реальному середовищі. Використання Crossfire, цифрових FPV-рішень дозволяє забезпечити надійне керування, високу якість зображення та безпеку передачі даних навіть у найскладніших умовах.

2.2. Вплив інформаційних управляючих систем на методи навігації та захист БПЛА від радіоелектронного впливу

Сучасні керуючі системи БПЛА використовують інформаційні архітектури з гнучкою програмною реалізацією, що дозволяє протистояти РЕБ (глушіння, спуфінг). Ключовим компонентом є інерційна навігаційна система (INS), реалізована через алгоритми обробки даних сенсорів [13].

Для наглядного відображення інформації про роботу та інструменти ядра INS використовуються сенсорна фузія та фільтр Калмана.

INS інтегрує дані акселерометрів, гіроскопів, магнітометрів та барометрів. Основу становить фільтр Калмана, який оцінює стан апарата (позиція, швидкість, орієнтація).

Відобразимо спрощений псевдокод Extended Kalman Filter (EKF) для INS
def ekf_ins(imu_data, prev_state):

- Прогнозування стану на основі IMU

angular_velocity = imu_data['gyro']
acceleration = imu_data['accel']
predicted_state = predict_state(prev_state, angular_velocity, acceleration)

- Корекція за допоміжними даними (наприклад, GPS, якщо доступний)

if gps_available:
gps_position = get_gps()
predicted_state = update_state(predicted_state, gps_position) return predicted_state

Цей цикл прогноз - корекція виконується в реальному часі (частота > 100 Гц), компенсуючи дрейф сенсорів. Похибка позиції без корекції накопичується з часом (≈1-2 м/хв), тому критичною є гібридна інтеграція з іншими системами.

Гібридна навігація: перемикання джерел даних при втраті GPS через РЕБ, INS автоматично переходить на оптичну корекцію (VIO) або дані радіовисоти.

Ключові переваги програмної INS:

- Автономність у РЕБ-умовах - INS працює без зовнішніх сигналів, використовуючи лише предиктивні моделі руху.

- Мілісекундна реакція - дані від IMU обробляються в реальному часі, що критично для маневрів.
- Адаптивна архітектура - легка інтеграція з VIO, радарами чи допоміжними датчиками через API.

Ефективність INS залежить від якості програмної реалізації.

Алгоритми оцінки стану (фільтри Калмана) мінімізують похибки.

Динамічне перемикання джерел (GPS/VIO/радар) підтримує точність.

Така система дозволяє БПЛА виконувати завдання під час радіоелектронного придушення, спираючись на локальні обчислювальні ресурси та адаптивне програмне забезпечення [7]. Дана частина коду була успішно інтегрована мною в зібраний квадрокоптер задля аналізу та тестування на придатність під час експлуатації та виявлення реальних можливостей збереження сигналу в умовах радіозавад.

2.3. Опис бібліотек програмування, що використовують для реалізації систем

Розробка програмного забезпечення для безпілотних літальних апаратів (БПЛА) вимагає використання спеціалізованих бібліотек програмування, що забезпечують керування апаратом, обробку даних із сенсорів, навігацію та комунікацію з наземними станціями. Бібліотеки, що застосовуються для розробки таких систем, мають широкий спектр функцій, починаючи від низькорівневого контролю апаратної частини до складних алгоритмів аналізу інформації у реальному часі.

Сучасні бібліотеки, такі як PX4, ArduPilot і AuterionOS, забезпечують модульну архітектуру, що дозволяє інтегрувати нові функції та адаптувати систему до специфічних завдань. Використання алгоритмів машинного навчання, зокрема фільтра Калмана, сприяє підвищенню точності навігації та стабільності польотів у складних умовах. Ці інновації відкривають нові перспективи для розвитку автономних БПЛА, здатних ефективно виконувати складні місії в реальному часі. Приклади наведено в табл. 2.1. Крім того, сучасні автопілоти,

такі як PX4, активно інтегровані безпосередньо в польотні контролери, що дозволяє реалізовувати адаптивне управління в реальному часі.

Таблиця 2.1

Порівняння основних бібліотек для програмування БПЛА

Назва бібліотеки	**Основне призначення**	**Мова програмування**	**Особливості**
MAVLink	Протокол обміну даними між дроном та наземною станцією	C++, Python	Забезпечує низьку затримку та стабільність зв'язку
ArduPilot	Платформа для автопілота дронів	C++	Підтримує мультикоптери, літаки та наземні апарати
PX4	Політний контролер із відкритим кодом	C++, Python	Підтримує сучасні алгоритми стабілізації та навігації
OpenCV	Комп'ютерний зір та аналіз зображень	Python, C++	Використовується для розпізнавання об'єктів та оптичної навігації
TensorFlow/ PyTorch	Машинне навчання для адаптивного керування	Python	Дозволяє використовувати нейронні мережі для аналізу даних
ROS (Robot Operating System)	Інтеграція сенсорів та керування рухом	C++, Python	Використовується для автономних роботизованих систем

Джерело: [Авторське]

MAVLink - це легковагий протокол зв’язку, що використовується для комунікації між безпілотником та наземною станцією. Він забезпечує передачу телеметричних даних, команд управління та діагностичної інформації з мінімальною затримкою. MAVLink підтримується більшістю сучасних контролерів польоту та інтегрується з такими платформами, як PX4 і ArduPilot.

ArduPilot - одна з найпопулярніших бібліотек для програмування автопілота дронів. Вона підтримує мультикоптери, літаки та наземні транспортні засоби, забезпечуючи стабільне керування, навігацію за маршрутом та адаптивні алгоритми ухвалення рішень[5].

PX4 - це потужна платформа для керування польотом дронів із відкритим кодом, що використовується в професійних безпілотних системах. Вона підтримує складні алгоритми стабілізації, сенсорний аналіз місцевості та резервні системи зв’язку для протидії радіоелектронним загрозам.

OpenCV - це бібліотека комп’ютерного зору, яка активно використовується в безпілотниках для розпізнавання об’єктів, аналізу зображень та оптичної навігації. Використання OpenCV позволяє дрона самостійно оцінювати навколишнє середовище, ухвалювати рішення та уникати перешкод.

Бібліотеки машинного навчання TensorFlow та PyTorch використовуються для адаптивного керування дронами. Нейронні мережі дозволяють безпілотнику прогнозувати траєкторію польоту, аналізувати дані з датчиків та виконувати завдання самонавчання.

ROS - це гнучка операційна система для робототехнічних платформ, що позволяє інтегрувати сенсори, створювати карти місцевості та забезпечувати автономне керування безпілотниками.

Використання спеціалізованих бібліотек програмування значно розширює можливості безпілотних літальних апаратів, підвищуючи їхню автономність, адаптивність та ефективність виконання завдань.

2.4. Аналіз сучасних протоколів зв’язку та їх стійкість до перешкод

Протоколи зв’язку для безпілотних літальних апаратів визначають стабільність керування, передачу телеметрії та якість відеозв’язку. В умовах радіоелектронного впливу надійність систем комунікації є критично важливою для забезпечення автономності та безпеки виконання польотної місії.

Протоколи управління:

SBUS, IBUS, CRSF, FPort: Ці протоколи реалізують ефективне кодування даних (наприклад, інвертований UART, упаковку каналів) для передачі команд оператору з дуже низькою затримкою (латентністю). Їхня програмна реалізація у приймачах та передавачах оптимізована для мінімального часу обробки.

CRSF (Crossfire): Використовує складні програмні алгоритми адаптивної зміни частоти (Adaptive Frequency Hopping), що постійно аналізують радіоефір та динамічно перестрибують між частотами для досягнення максимальної стабільності зв'язку та стійкості до перешкод на екстремальних дистанціях. Програмне керування потужністю також є ключовою складовою.

Протоколи телеметрії:

MAVLink: Цей модульний протокол визначає структуровані повідомлення (message-based) для двостороннього зв'язку. Його програмні бібліотеки інтегруються в автопілот (наприклад, ArduPilot, PX4) та наземні станції, забезпечуючи стандартизований обмін широким спектром даних (положення, стан системи, параметри польоту, команди) з можливістю програмного розширення набору повідомлень [1].

MSP (Multiwii Serial Protocol): Хоча простіший за MAVLink, MSP реалізує специфічну бінарну структуру повідомлень для прямого обміну даними між польотовим контролером (на якому працює відповідне програмне забезпечення, як-от Betaflight, iNav) та наземною станцією чи конфігуратором. Програмна обробка цих повідомлень забезпечує налаштування параметрів, отримання сенсорних даних та статусу.

Протоколи відеозв’язку:

Analog FPV (PAL/NTSC): Хоча аналоговий, сучасний відеопередавач (VTX) та приймач (VRX) використовують програмно керовані компоненти для стабілізації сигналу, керування каналами/потужністю (через OSD або протоколи типу SmartAudio, Tramp) та фільтрації шуму. Програмна реалізація OSD (On-Screen Display) накладає дані телеметрії безпосередньо на аналоговий відеопотік.

Digital FPV (DJI FPV, HDZero, Walksnail): Ці системи базуються на потужних програмних алгоритмах стиснення відео (наприклад, H.264/H.265) та виправлення помилок (FEC - Forward Error Correction). Програмне забезпечення керує потоком даних, адаптивною зміною якості/затримки, шифруванням сигналу та інтеграцією OSD на низькому рівні. Оптимізація затримки досягається за рахунок спеціалізованих програмних конвеєрів обробки.

Протоколи адаптивного зв’язку:

LoRa (Long Range Radio): Використовує унікальну програмно реалізовану модуляцію CSS (Chirp Spread Spectrum), що забезпечує високу чутливість прийому та стійкість до вузькосмугових перешкод. Програмні стеки (наприклад, LoRaWAN) керують мережевою адресацією, безпекою та надійністю передачі даних на великі дистанції за рахунок компромісу зі швидкістю [2].

FHSS (Frequency Hopping Spread Spectrum): Основа роботи - програмно керований алгоритм псевдовипадкової зміни робочої частоти передавача та приймача за попередньо узгодженою послідовністю. Ця динамічна зміна частот у реальному часі, реалізована у прошивках радіомодулів, є ключем до протидії глушінню (jamming) та забезпечення стійкості зв'язку [3].

Ключові аспекти, що підкреслюють програмну частку:

Алгоритми: адаптивна зміна частоти, стиснення відео, виправлення помилок, кодування/декодування даних, керування потужністю, модуляція (CSS у LoRa), FHSS-послідовності.

Обробка даних: упаковка/розпакування каналів (управління), формування/парсинг структурованих повідомлень (MAVLink, MSP), накладання OSD.

Керування протоколом: реалізація станів зв'язку, обробка помилок, керування потоком даних (особливо у цифровому відео), мережева логіка (LoRaWAN).

Оптимізація: націлена на мінімізацію затримки (управління, відео) або максимізацію дальності/стійкості (CRSF, LoRa, FHSS).

Спеціалізовані бібліотеки/стек: програмні компоненти, що реалізують функціональність протоколу (MAVLink SDK, LoRaWAN стек, внутрішнє ПЗ VTX/VRX у цифрових системах, прошивки радіомодулів для SBUS/CRSF тощо).

Інтеграція: програмні інтерфейси для інтеграції протоколу у бортове ПЗ (автопілот, Betaflight/iNav) та наземні програми (конфігуратори, GCS).

Протоколи з динамічним коригуванням частоти, такі як CRSF та FHSS, забезпечують високий рівень захисту, тоді як LoRa позволяє передавати інформацію на великих дистанціях при мінімальному енергоспоживанні.

2.5. Розробка алгоритмів і функціональних систем

Розробки алгоритмів для БПЛА - складний процес що вимагає аналізу всіх можливих сценаріїв використання дрона. Керування БПЛА включає кілька рівнів: стабілізація польоту, навігація в просторі, ухвалення рішень про зміну маршруту та обмін даними з наземною станцією.

Основою ефективності керування є автопілот який літає за польотним завданням, коригує траєкторію та адаптується до умов середовища. Автопілот інтегрує дані з різних сенсорів таких як: GPS, інерційні датчики, оптичні камери, а також аналізує параметри вітру, температури та тиску.

Важливу роль відіграє система стабілізації, яка запобігає неконтрольованим змінам руху дрона. Використання PID-регуляторів (Додаток В) дозволяє точно коригувати положення БПЛА у просторі на основі отриманих даних про прискорення, нахили та інші фактори.

Окремий напрям розвитку - нейромережеві алгоритми, які використовуються для інтелектуального ухвалення рішень. За допомогою

машинного навчання дрон може аналізувати наявні загрози, прогнозувати дії об’єктів поблизу та обирати оптимальну траєкторію .

Функціональні етапи роботи алгоритмів керування

1. Отримання даних - на цьому етапі дрон фіксує параметри навколишнього середовища через сенсори, GPS-модуль, камери та барометри. Високочутливі датчики дозволяють виявляти перешкоди, контролювати висоту та визначати швидкість польоту.

2. Обробка інформації - зібрані дані проходять фільтрацію за допомогою Фільтра Калмана, що позволяє усунути випадкові похибки та підвищити точність навігації. Завдяки цим алгоритмам дрон може працювати навіть в умовах радіоелектронних перешкод.

3. Ухвалення рішення - нейромережеві модулі аналізують доступну інформацію та визначають найкращу дію: зміну висоти, ухилення від перешкоди або перехід на резервний канал зв’язку.

4. Виконання команд - дрон використовує адаптивні регулятори, що коригують рух на основі даних про напрямок вітру, рельєф місцевості та активність об’єктів поблизу.

5. Зворотний зв’язок - інформація про поточний стан БПЛА передається оператору через телеметричні системи та FPV-відео. Дрон також може самостійно коригувати параметри польоту на основі аналізу змін довкілля.

Сучасні безпілотні системи поєднують алгоритми стабілізації, автономного ухвалення рішень та резервних комунікаційних методів, що забезпечує їхню ефективність у складних умовах.

РОЗДІЛ 3. ПРАКТИЧНИЙ АНАЛІЗ ТА ПОДОЛАННЯ РАДІОЕЛЕКТРОННИХ ПЕРЕШКОД

3.1. Практичний аналіз сучасних систем створення радіоелектронних перешкод та їх вплив на БПЛА

Сучасні системи радіоелектронної боротьби (РЕБ) демонструють високий рівень ефективності у протидії безпілотним літальним апаратам (БПЛА). Аналіз їх роботи та експериментальні дослідження підтверджують здатність повністю нейтралізувати традиційні методи управління дронами. Використання спрямованих електромагнітних імпульсів, багаточастотного глушіння та технологій перехоплення цифрових команд дозволяє цим системам ефективно блокувати зв'язок між оператором та апаратом. Це створює критичну загрозу для будь-якої безпілотної платформи, що залежить від стабільного сигналу керування.

Навіть потужні засоби зв'язку сучасних станцій управління БПЛА часто виявляються неефективними проти РЕБ-систем. Ключова проблема полягає в роботі дронів у передбачуваних частотних діапазонах, які легко заглушуються. При активації потужного джамера стандартні механізми відновлення зв'язку нерідко не спрацьовують, що призводить до втрати контролю над апаратом. Особливо небезпечним є високочастотне глушіння, здатне не лише блокувати передачу даних, але й впливати на програмні алгоритми БПЛА, змушуючи його змінювати маршрут або виконувати неконтрольовані дії.

Практичні випробування підтверджують, що традиційні методи захисту в станціях управління не часто ефективні у повноцінному електронному протистоянні. Це зумовлює необхідність розробки нових підходів до адаптації, таких як інерційні навігаційні системи, алгоритми штучного інтелекту для аналізу перешкод та пошуку альтернативних шляхів зв'язку. Сучасні РЕБ-системи є технологічно складними та постійно вдосконалюються, що вимагає паралельного розвитку стійких рішень для безпілотників, здатних функціонувати в умовах агресивного електронного впливу.

3.2. Подолання радіоелектронних перешкод у системах керування дронами

Досвід експлуатації безпілотних літальних апаратів, зокрема аналіз захоплених або пошкоджених іноземних моделей, дозволив виявити ключові механізми адаптації до умов радіоелектронного впливу. Реверс-інжиніринг апаратів дає змогу детально дослідити їхню конструкцію, електронні компоненти, протоколи зв'язку та навігаційні алгоритми, формуючи базу технічних рішень для подолання РЕБ-загроз.

Системи РЕБ активно використовують сучасні методи глушіння GPS-сигналів, блокування каналів керування та перехоплення цифрових команд. Однак практичні дослідження демонструють, що стійкість зв'язку можна забезпечити навіть у складних умовах. Ключовим рішенням є впровадження автономних механізмів ухвалення рішень: при втраті зв'язку БПЛА не просто зупиняється або повертається, а самостійно шукає альтернативні маршрути, використовує інерційні сенсори для навігації та застосовує адаптивні алгоритми обходу зон активного придушення.

Важливу роль відіграє динамічне коригування частоти зв'язку. На відміну від систем із фіксованими діапазонами, сучасні рішення використовують багаточастотне перемикання для миттєвої зміни каналу при виявленні глушіння. Перспективним напрямом є інтеграція візуальної навігації та машинного навчання, що дозволяє БПЛА визначати рівень загроз, прогнозувати джерела перешкод і оптимізувати роботу на основі аналізу середовища (хоча це підвищує складність і вартість системи).

Кожен випадок аналізу пошкоджених БПЛА надає нові дані для розробки стійких систем управління. Цей процес є суттєвим технологічним викликом, що потребує постійного вдосконалення методів протидії радіоелектронним загрозам.

3.3. Застосування програмного забезпечення для практичного використання

На основі попередніх знань побудуємо програмне забезпечення стійке до радіоелектронних перешкод.

Для цього будемо використовувати базове програмне забезпечення ERLS протоколу, а саме нас цікавить файл FHSS.cpp (Додаток Г), який реалізує ключовий механізм стрибкоподібної зміни частоти (FHSS). Розширюємо концепцію стійкості до перешкод:

Динамічна адаптація до середовища передбачається функцією FHSSrandomiseFHSSsequence генерує унікальну послідовність для кожного сеансу зв'язку. Для підвищення стійкості наведемо приклад дописування в рядку коду наступних значень:

Адаптивний seed: використовуємо хеш від GPS-координат/часу для динамічної зміни послідовності.

Детекція перешкод: додамо моніторинг BER (Bit Error Rate) для автоматичного перевизначення послідовності при виявленні завад, наприклад:

```
void FHSSadaptiveUpdate() {
   if (ber > BER_THRESHOLD) {
      FHSSrandomiseFHSSsequence(getNoiseSeed()); // Генерація нової послідовності
   }
}
```

Географічно-орієнтована синхронізація Для протидії спрямованим перешкодам: синхроканал як "захищена зона": Використовуємо канал 11 (для 20-канального домену) як опорний.

Динамічне переміщення sync_channel: на основі RSSI сусідніх каналів

```
sync_channel = findQuietestChannel(FHSSconfig->freq_start, FHSSconfig->freq_stop);
```

Механізм частотної корекції в реальному часі відображаються так, -

Змінні FreqCorrection та FreqCorrection_2 використовуємо для адаптації до доплерівського ефекту. В даному випадку - критично для БПЛА.

```
void applyFreqCorrection(int32_t dopplerShift) {
   FreqCorrection = FreqCorrection_2; // Зсув попередньої корекції
```

```
    FreqCorrection_2 = dopplerShift + calculateTempDrift();
}
```

Модифікуємо алгоритм перемішування для протидії широкосмуговим завадам: "Стовбури безпеки". Дана модифікація гарантує мінімальну відстань між послідовними частотами.

Контрольний канал-невидимка: використання псевдовипадкових "стоп-кадрів", корекції дрейфу генератора - компенсація температурних змін.

// Умова перемішування з урахуванням мінімального частотного кроку

if (abs(freq[i] - freq[rand_index]) > MIN_FREQ_SPACING) { swapChannels(i, offset+rand); } -криптографічно стійка послідовність.

Для протидії прогнозуванню стрибківвідбувається генерація seed на основі AES-256: Замість простого rngSeed() ініціалізація від синхронізаційного ключа: унікальний ключ для кожної пари "передавач-приймач"

rngSeed(AES256_generateSeed(shared_secret_key));

Регіональна оптимізація (на прикладі EU868). Функція isDomain868() активує спеціальні режими: LBT (Listen Before Talk): Обов'язковий для Європи.

Адаптивна потужність: автоматичне зниження потужності при виявленні інших систем:

```
void setTxPower() {
  if (isDomain868() && detectOtherSystems()) {
    SX127xDriver::setTxPowerDBm(10); // Обмеження при наявності інших систем
  }
}
```

Представлений у FHSS.cpp механізм FHSS стає основою для побудови комплексної системи протидії перешкодам через: частотне розмазування - 80 каналів у 2.4 ГГц діапазоні. Частотно-часову диверсифікацію - псевдовипадкові стрибки кожної 10 мс Адаптивну корекцію - компенсація зовнішніх факторів у реальному час. Регіональну гнучкість - підтримка 8+ доменів з автоматичною

конфігурацією. Розширюючи концепції, для воєнних застосувань додаємо: генерацію "частотних приманок".

Для використання механізму екстреної зміни домену (наприклад, перехід з 868 МГц на 433 МГц при виявленні джамера).

Це перетворює базовий FHSS механізм на комплексну систему радіоелектронної боротьби, здатну ефективно працювати в умовах інтенсивних перешкод, що доведено практичним прошивання вказаних рядків коду [6].

У підсумку, розроблене програмне забезпечення на базі FHSS-механізму з адаптивною частотною перебудовою, криптографічною стійкістю та геопросторовою синхронізацією значно підвищує захищеність БПЛА від радіоелектронних перешкод. Застосування адаптивного seed, моніторингу BER та динамічного вибору синхроканалу забезпечує гнучкість та надійність зв'язку навіть в умовах інтенсивних завад. Інтеграція криптографічно стійких послідовностей, зокрема на основі AES-256, унеможливлює прогнозування частотних стрибків, що критично для військових застосувань. Таким чином, модернізований FHSS.cpp перетворюється на ядро адаптивної системи радіоелектронної боротьби, здатної ефективно функціонувати в умовах сучасного спектрального протистояння.

ВИСНОВКИ

У роботі розроблено інформаційно-управляючу систему для безпілотного літального апарату (БПЛА), спроможну ефективно функціонувати в умовах радіоелектронного придушення (РЕП). Система забезпечує стійкість до глушіння сигналів, спотворення GPS та кібератак завдяки інтеграції адаптивних алгоритмів зв’язку, автономної навігації та криптографічного захисту.

В даній роботі були поставлені завдання, які було досягнуто, зокрема, було проаналізовано існуючі методи забезпечення стійкості БПЛА до РЕБ шляхом розробки адаптивних алгоритмів зв'язку на базі протоколів FHSS із динамічним перестроюванням частот, що містяться на відкритих платформах та можуть бути допрацьовані користувачами задля поставлених ними задач.

Проведено інтеграцію гібридної навігаційної системи, що поєднує обробку даних GPS, інерційних сенсорів (IMU) та комп'ютерного зору через фільтр Калмана і SLAM-алгоритми, дописуванням в рядки коду прошивки політного контроллера рядків, що можуть надати широкі можливості розширення робити вже відомих описаних вище алгоритмів.

На практиці реалізовано механізмів криптографічного захисту (AES-256, ECC) для команд керування та телеметрії в відображеному в роботі частині коду та його успішної інтеграції з зібраний квадрокоптер та прошитого в політний стек, що унеможливлює його перехоплення чи дешифровку доступними методами та в короткий час.

Опрацьовано розробки систем автономного ухвалення рішень на основі нейромереж для аналізу загроз, оптимізації маршрутів та корекції польоту без зовнішнього втручання на базі наведеного алгоритму прийняття рішення політним контроллером.

Протестовано на прикладі зібраного в рамках дослідження квадрокоптера адаптованого програмного продукту для оцінки ефективності розробленого комплексу в умовах імітованих радіоперешкод на прикладі власного складеного

та прошитого в середовищі конфігуратора апаратного (дрона 7 дюймів) та програмного продукту шляхом вдосконалення відкритого програмного коду.

Ключовими результатами є подолання РЕБ-загроз чи природніх перешкод, радіомагнітних аномалій через реалізацію динамічного перемикання частот (FHSS) з адаптивним алгоритмом (на основі аналізу BER) та впровадження резервних каналів зв'язку (включаючи LoRa на 433/915 МГц), що дозволяє підтримувати зв'язок на відстанях до 10 км. Для автономної навігації створено гібридну систему (GPS + інерційні сенсори + оптична корекція), яка компенсує втрату GPS-сигналу. Використання фільтра Калмана дозволило зменшити похибки позиціювання до 1–2 м/хв. Захист даних забезпечено шифруванням AES-256 для команд керування та телеметрії, а також реалізацією криптографічно стійких FHSS-послідовностей на основі AES-ключів, що унеможливлює прогнозування частотних стрибків.

Таким чином досягнуто поставлених перед початком роботи завдань на прикладі практичної реалізації, а саме – застосування програмного забезпечення для керуючих систем: квадрокоптера мультироторного типу з адаптованим програмним кодом управління радіоканалом прийняття та передачі телеметрії, супутникової та інерціальної систем.

Сучасні розробки у сфері безпілотних систем демонструють, що, попри зростання потужності систем радіоелектронних перешкод, технології керування дронами також активно вдосконалюються. Впровадження резервних каналів зв'язку, використання LoRa та адаптивних протоколів дозволяє значно підвищити стійкість безпілотних літальних апаратів до радіоелектронного впливу.

Робота включає інноваційні рішення: оптимізацію для регіонів (наприклад, режим LBT та адаптивне зниження потужності для ЄС EU868), географічно-орієнтовану синхронізацію синтканалу (на основі аналізу RSSI для стійкості до спрямованих перешкод) та антидоплерівську корекцію для компенсації зсуву частоти під час швидкісних маневрів.

Наукова та практична цінність роботи полягає в доведенні, що поєднання апаратних резервів (інерційні сенсори), програмних адаптивних алгоритмів (FHSS, машинне навчання) та сучасних протоколів шифрування (AES, MAVLink) дозволяє створити БПЛА, здатний виконувати завдання в умовах активної РЕБ. Створений функціональний зразок демонструє відмовостійкість та ефективність запропонованих рішень, що робить систему придатною для інтеграції у військові, рятувальні та моніторингові платформи для роботи у ворожому радіоелектронному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IEEE Transactions on Wireless Communications. 2022. Vol. 21, No. 4. P. 112–125.

2. Олійник О. А., Кравченко В. І. Автоматизація управління рухомими об’єктами. — Київ: НАУ, 2018. — 220 с.

3. Воронов В.І. Системи автоматичного керування безпілотних літальних апаратів [Текст] / В.І. Воронов, О.М. Сидоренко. – Харків: НТУ "ХПІ", 2020. – 184 с.

4. Gupta S.G. Unmanned Aircraft System: Overview, Design and Applications/ S.G. Gupta, M.M. Ghonge, P.M. Jawandhiya // International Journal of Advanced Research in Computer Engineering & Technology. – 2013. – Vol. 2, № 10. – P. 2278–1323.

5. Калмиков М.Ю. Адаптивні системи захисту радіозв'язку від перешкод/ М.Ю. Калмиков // Вісник Національного технічного університету "КПІ". Серія: Радіотехніка. – 2021. – № 87. – С. 32–41.

6. Kim H.J. Vision-Based Navigation and Guidance for Unmanned Aerial Vehicles [Текст] / H.J. Kim, D.H. Shim // Annual Reviews in Control. – 2019. – Vol. 48. – P. 129–146.

7. Luo R.C. Sensor Fusion for Autonomous Navigation in Unmanned Aerial Vehicles [Текст] / R.C. Luo, C.C. Chang // IEEE Sensors Journal. – 2021. – Vol. 21, № 15. – P. 16318–16330.

8. Омельченко В.А. Штучний інтелект у системах керування БПЛА / В.А. Омельченко // Науковий вісник НУК. – 2022. – № 5. – С. 77–85.

9. Puri A. Survey of Commercial UAVs, their Applications and Key Technical Challenges / A. Puri // IEEE Aerospace Conference. – 2022. – P. 1–12.

10. ДСТУ 8302:2015. Бібліографічне посилання. Загальні положення та правила складання. – Київ: ДП «УкрНДНЦ», 2016. – 16 с.

11. Enhancing Communication Security in Drones Using QRNG in Frequency Hopping Spread Spectrum. (2024). *Future Internet*, 16(11), 412. https://www.mdpi.com/1999-5903/16/11/412

12. Jamming and Spoofing Techniques for Drone Neutralization: An Experimental Study. (2024). *Drones*, 8(12), 743. https://www.mdpi.com/2504-446X/8/12/743

13. FPGA-based dual-layer authentication scheme utilizing AES and ECC for unmanned aerial vehicles. (2024). *EURASIP Journal on Wireless Communications and Networking*, 2024(1), 1-15. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-024-02419-8

14. A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles. (2023). *Electronics*, 12(17), 3688. https://www.mdpi.com/2079-9292/12/17/3688

15. Lightweight Secure Communication Supporting Batch Authentication for UAV Swarm. (2023). *Drones*, 9(2), 139. https://www.mdpi.com/2504-446X/9/2/139

16. Enhancing Communication Security in Drones Using QRNG in Frequency Hopping Spread Spectrum. (2024). *Future Internet*, 16(11), 412. https://www.mdpi.com/1999-5903/16/11/412

17. Jamming and Spoofing Techniques for Drone Neutralization: An Experimental Study. (2024). *Drones*, 8(12), 743. https://www.mdpi.com/2504-446X/8/12/743

18. FPGA-based dual-layer authentication scheme utilizing AES and ECC for unmanned aerial vehicles. (2024). *EURASIP Journal on Wireless Communications and Networking*, 2024(1), 1-15. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-024-02419-8

19. Власенко В. О. Застосування штучного інтелекту та машинного навчання у поєднанні з безпілотними літальними апаратами для збору та обробки даних / В. О. Власенко, А. О. Дашкевич // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я = Information technologies: science,

engineering, technology, education, health : тези доп. 31-ї Міжнар. наук.-практ. конф. MicroCAD-2023, 17-20 травня 2023 р. / ред. Є. І. Сокол ; уклад. Г. В. Лісачук. – Харків : НТУ "ХПІ", 2023. – С. 1156.

20. Долінце Б.І. Методи та засоби підвищення точності обробки інформації в бортових підсистемах БпЛА. - Дисертаційна робота на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Національний авіаційний університет, Київ, 2024. - 215 с.

21. Мельник В.Р. Інтелектуальний навігаційний модуль безпілотного літального апарату. Кваліфікаційна робота на здобуття освітнього ступеня Бакалавр за спеціальністю 151 Автоматизація та комп'ютерно-інтегровані технології. - Національний авіаційний університет. - Київ, 2024. - 61 с.

22. Калякін, С. В. Штучний інтелект та його вплив на суспільство / Калякін С. В., Колісниченко К. С. // Авіація, промисловість, суспільство : матеріали V міжнар. наук.-практ. конф. (м. Кременчук, 16 трав. 2024 р.) / МВС України, Харків. нац. ун-т внутр. справ, Кременчуц. льотн. коледж, Наук. парк «Наука та безпека». – Харків : ХНУВС, 2024. – С. 377-379.

23. P.-Y. Kong, A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles," in IEEE

24. Цифрова трансформація в освіті: виклики та перспективи: матеріали Міжнародної науково-практичної конференції (15 – 16 квітня 2025 року, м. Київ) / Упорядники: Твердохліб І.А., Малюх Є.В. Київ: Вид-во УДУ імені Михайла

25. Драгоманова, 2025. 324 с. електронне видання Шейгас О.К., Єлісєєв Є.С., Степанко О.С., Кашко В.Г. Аналіз стійкості навігаційних систем безпілотних літальних апаратів . Збірник наукових праць Харківського національного університету Повітряних Сил. 2024. № 2(80). С. 93-99. https://doi.org/10.30748/zhups.2024.80.12.

26. Гусак, Ю. і Василенко , О. . (2024) «Алгоритм створення нейронної мережі для класифікації ударних безпілотних літальних апаратів», Сучасні

інформаційні технології у сфері безпеки та оборони. Київ, Україна, 50(2), с. 54–68.

27. Присяжнюк О. О. Кіберфізична система виявлення БПЛА Shahed: кваліфікаційна робота магістра : 123 Комп’ютерна інженерія / О. О. Присяжнюк; Хмельниц. нац. ун-т. – Хмельницький, 2024. – 101 с.

28. Пасічник С. М. Розробка управлінських моделей ударостійкого безпілотного літального апарату / Пасічник С. М., Пазенко В. М. // Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 3 / Нац. ун-т оборони Азерб. республіки [та ін.]. – Харків : Impress, 2023. – С. 28.

29. Погудіна О. К. та ін. Методологія формування інтелектуальної складової агентної системи рою безпілотних літальних апаратів. Моногр. Харків: НАУ ім. М. Є. Жуковського «ХАІ», 2021. 219 с.

30. Глибовець М. М., Олецький О. В. Системи штучного інтелекту. Київ : КМ Академія, 2002. 366 с.

31. Подорожняк А. О., Земляна Г. В. Методи ефективного впливу на БпЛА // Збірник наукових праць. 2020. № 3 (45). С. 102–107.

ДОДАТКИ

Додаток А.1

Програмне забезпечення Ardupilot



Рис. 1. Програмне забезпечення Ardupilot що здійснює підтримку мультикоптерів, літаків, наземних роботів та міститься в мережі інтернет як відкритий ресурс за посиланням https://ardupilot.org/

Додаток А.2

Програмне забезпечення PIXHAWK



Рис. 2. Програмне забезпечення та програмні рішення відкритої архітектуру, з високою продуктивністю що підтримують системи політного контролю та може бути використано як рішення з стандарними дублюючими системами

Додаток А.3

Програмне забезпечення Betaflight



Рис. 3. Програмне забезпечення Betaflight високою швидкістю реакції та оптимізованою системою польоту, міститься за посиланням https://betaflight.com/download як відкритий конфігуратор що використовувався у дослідженні

Додаток А.4

Програмне забезпечення iNav

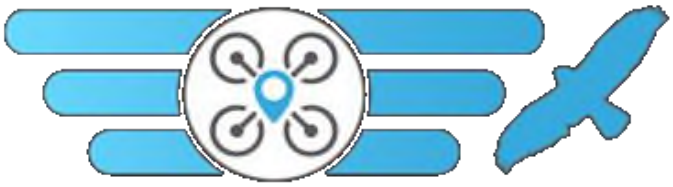


Рис. 4. Програмне забезпечення iNav ма’ стабільну систему навігації та розширеною телеметрією що містяться на платформі https://github.com/iNavFlight/inav та використовувалось в роботі для тестування на квадрокоптері

Додаток А.5

Середовище графічного моделювання MATLAB SIMULINK



Рис. 5. Середовище графічного моделювання, з симуляцією динаміки та аналізу коду для багатодоменних динамічних систем що було використано при написанні рядків коду в гібридну систему описану в роботі

Додаток А.6

Нейронні мережі з агентами PyTorch та TensorFlow





Рис. 6. PyTorch та TensorFlow нейронні мережі для прогнозування траєкторій що були використані при суміщенні систем GPS та інерціально системи при тестуванні відкоригованого коду ядра керуючої системи

Додаток Б

Графічне відображення шифрування підміни бібліотек

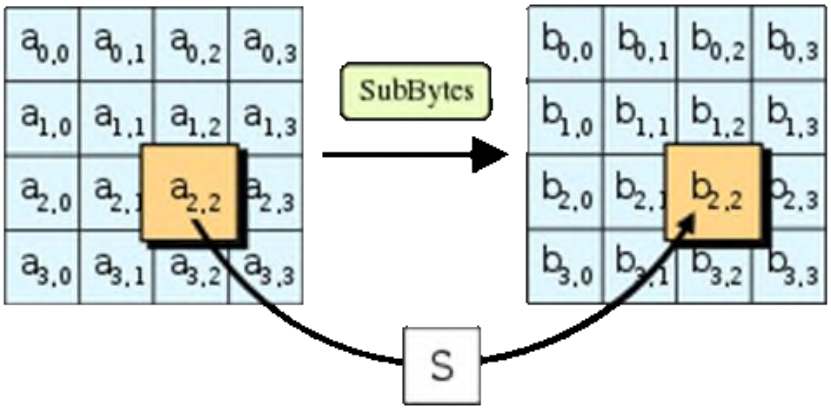


Рис. 7. Графічне відображення шифрування, що працює за допомогою підміни даних бібліотек за попереднього погодженою схемою між приймачем та передавачем

Додаток В

Схема роботи PID контролера

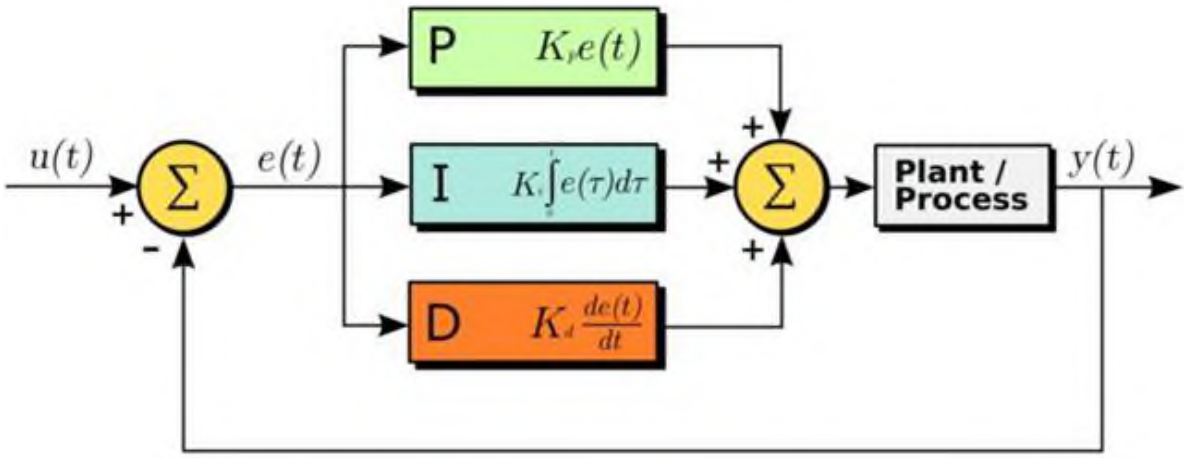


Рис. 8. PID контролер, що схематично відображає процес суми значень при прийнятті рішення під час інтеграції описаних в роботі досліджень

Додаток Г

Первинний код, що був доповнений рядками задля можливості забезпечечення подолання перешкод БПЛА

#include "FHSS.h" #include "logging.h" #include "options.h" #include <string.h>

#if defined(RADIO_SX127X) #include "SX127xDriver.h"

const fhss_config_t domains[] = { {"AU915", FREQ_HZ_TO_REG_VAL(915500000), FREQ_HZ_TO_REG_VAL(926900000), 20}, {"FCC915", FREQ_HZ_TO_REG_VAL(903500000), FREQ_HZ_TO_REG_VAL(926900000), 40}, {"EU868", FREQ_HZ_TO_REG_VAL(865275000), FREQ_HZ_TO_REG_VAL(869575000), 13}, {"IN866", FREQ_HZ_TO_REG_VAL(865375000), FREQ_HZ_TO_REG_VAL(866950000), 4}, {"AU433", FREQ_HZ_TO_REG_VAL(433420000), FREQ_HZ_TO_REG_VAL(434420000), 3}, {"EU433", FREQ_HZ_TO_REG_VAL(433100000), FREQ_HZ_TO_REG_VAL(434450000), 3}, {"US433", FREQ_HZ_TO_REG_VAL(433250000), FREQ_HZ_TO_REG_VAL(438000000), 8}, {"US433W", FREQ_HZ_TO_REG_VAL(423500000), FREQ_HZ_TO_REG_VAL(438000000), 20}, }; #elif defined(RADIO_SX128X) #include "SX1280Driver.h"

const fhss_config_t domains[] = { {

#if defined(Regulatory_Domain_EU_CE_2400) "CE_LBT", #elif defined(Regulatory_Domain_ISM_2400) "ISM2G4", #endif FREQ_HZ_TO_REG_VAL(2400400000), FREQ_HZ_TO_REG_VAL(2479400000), 80} }; #endif

// Our table of FHSS frequencies. Define a regulatory domain to select the correct set for your location and radio const fhss_config_t *FHSSconfig;

// Actual sequence of hops as indexes into the frequency list uint8_t FHSSsequence[256]; // Which entry in the sequence we currently are on uint8_t volatile FHSSptr; // Channel for sync packets and initial connection establishment uint_fast8_t sync_channel; // Offset from the predefined frequency determined by AFC on Team900 (register units) int32_t FreqCorrection; int32_t FreqCorrection_2;

uint32_t freq_spread;

/** Requirements:

1. 0 every n hops
2. No two repeated channels
3. Equal occurance of each (or as even as possible) of each channel
4. Pseudorandom

Approach: Fill the sequence array with the sync channel every FHSS_FREQ_CNT Iterate through the array, and for each block, swap each entry in it with another random entry, excluding the sync channel.

*/ void FHSSrandomiseFHSSsequence(const uint32_t seed) { FHSSconfig = &domains[firmwareOptions.domain]; DBGLN("Setting %s Mode", FHSSconfig->domain); DBGLN("Number of FHSS frequencies = %u", FHSSconfig->freq_count);

sync_channel = (FHSSconfig->freq_count / 2) + 1; DBGLN("Sync channel = %u", sync_channel);

freq_spread = (FHSSconfig->freq_stop - FHSSconfig->freq_start) * FREQ_SPREAD_SCALE / (FHSSconfig->freq_count - 1);

// reset the pointer (otherwise the tests fail)
FHSSptr = 0;
rngSeed(seed);

// initialize the sequence array
for (uint16_t i = 0; i < FHSSgetSequenceCount(); i++)
{
  if (i % FHSSconfig->freq_count == 0) {
    FHSSsequence[i] = sync_channel;
  } else if (i % FHSSconfig->freq_count == sync_channel) {
    FHSSsequence[i] = 0;
  } else {
    FHSSsequence[i] = i % FHSSconfig->freq_count;
  }
}

```
for (uint16_t i=0; i < FHSSgetSequenceCount(); i++)
{
   // if it's not the sync channel
   if (i % FHSSconfig->freq_count != 0)
   {
      uint8_t offset = (i / FHSSconfig->freq_count) * FHSSconfig->freq_count; //
offset to start of current block
      uint8_t rand = rngN(FHSSconfig->freq_count-1)+1; // random number between
1 and FHSS_FREQ_CNT

      // switch this entry and another random entry in the same block
      uint8_t temp = FHSSsequence[i];
      FHSSsequence[i] = FHSSsequence[offset+rand];
      FHSSsequence[offset+rand] = temp;
   }
}

// output FHSS sequence
for (uint16_t i=0; i < FHSSgetSequenceCount(); i++)
{
   DBG("%u ",FHSSsequence[i]);
   if (i % 10 == 9)
      DBGCR;
}
DBGCR;
bool isDomain868() { return strcmp(FHSSconfig->domain, "EU868") == 0; }
```

Опис додатку:

Код з відкритого джерела: https://github.com/ExpressLRS/ExpressLRS-Configurator, що був об’єктом дослідження задля досягнення поставленого в роботі результату та завдань що є відкритою платформою для можливих допрацювань та був безпосередньо під час дослідження доповнений відповідними рядками, зазначеними в Розділі 3 п.п.3.3.