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

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КАНАЛУ ЗВ’ЯЗКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ»

Виконав: здобувач 5 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Ташматов Ярослав Вячеславович

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к.т.н., доцент
Ахмаметьєва Ганна Валеріївна

Одеса – 2025

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

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

З А В Д А Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Ташматову Ярославу Вячеславовичу

1. Тема роботи: «Забезпечення захисту каналу зв'язку безпілотних літальних апаратів»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання «16» вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему “Забезпечення захисту каналу зв’язку безпілотних літальних апаратів” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 3 рисунків, 4 таблиць, 27 літературних джерел за переліком посилань. Робота виконана на 46 сторінках загального тексту і 37 сторінках основного тексту.

Метою роботи є розробка теоретико-методологічних основ і практичних рекомендацій для забезпечення захисту каналів зв’язку безпілотних літальних апаратів шляхом створення адаптивної системи кібербезпеки, яка інтегрує криптографічні методи, протоколи аутентифікації та технології виявлення вторгнень. Розроблено модель захищеного каналу зв’язку, що включає алгоритми шифрування AES-256 і ECC, багаторівневу аутентифікацію з використанням OAuth 2.0 і DTLS, а також IDPS із підтримкою штучного інтелекту. Програмно реалізовано механізми шифрування, моніторингу трафіку та реагування на загрози, проведено тестування в модельних і наближених до реальних умовах, що показало стійкість до атак і швидкість реагування до 10 секунд.

Результати роботи можуть бути використані розробниками та операторами БПЛА у військовому, цивільному та комерційному секторах для підвищення безпеки каналів зв’язку, забезпечення відповідності стандартам NIST та ISO/IEC 27001, а також у навчальних програмах із кібербезпеки. Рекомендації сприяють зниженню ризиків перехоплення даних, глушіння сигналів і несанкціонованого доступу.

Можливими напрямками подальших досліджень є впровадження постквантової криптографії, інтеграція машинного навчання для прогнозування кіберзагроз і адаптація системи до сітчастих мереж та 5G-технологій.

КІБЕРБЕЗПЕКА, БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ, КАНАЛИ ЗВ’ЯЗКУ, КРИПТОГРАФІЯ, АУТЕНТИФІКАЦІЯ, ВИЯВЛЕННЯ ВТОРГНЕНЬ.

ABSTRACT

Qualification work on the topic “Ensuring the Protection of Communication Channels for Unmanned Aerial Vehicles” for obtaining the first (bachelor’s) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 3 figures, 4 tables, and 27 literary sources listed in the references. The work spans 46 pages of total text and 37 pages of main text.

The purpose of the work is to develop theoretical and methodological foundations and practical recommendations for ensuring the protection of communication channels of unmanned aerial vehicles by creating an adaptive cybersecurity system that integrates cryptographic methods, authentication protocols, and intrusion detection technologies. A model of a secure communication channel was developed, incorporating AES-256 and ECC encryption algorithms, multi-level authentication using OAuth 2.0 and DTLS, and IDPS with artificial intelligence support. Mechanisms for encryption, traffic monitoring, and threat response were programmatically implemented, with testing conducted in simulated and near-real conditions, demonstrating resilience to attacks and a response time of up to 10 seconds.

The results of the work can be utilized by developers and operators of UAVs in military, civilian, and commercial sectors to enhance the security of communication channels, ensure compliance with NIST and ISO/IEC 27001 standards, and in cybersecurity educational programs. The recommendations help reduce the risks of data interception, signal jamming, and unauthorized access.

Possible directions for further research include the implementation of post-quantum cryptography, integration of machine learning for predicting cyber threats, and adaptation of the system to mesh networks and 5G technologies.

CYBERSECURITY, UNMANNED AERIAL VEHICLES, COMMUNICATION CHANNELS, CRYPTOGRAPHY, AUTHENTICATION, INTRUSION DETECTION.

ЗМІСТ

ВСТУП

У сучасному світі безпілотні літальні апарати (БПЛА) стали невід'ємною частиною військових, цивільних і комерційних операцій, забезпечуючи виконання завдань у таких сферах, як розвідка, моніторинг, логістика та сільське господарство. Проте стрімкий розвиток технологій БПЛА супроводжується зростанням кіберзагроз, спрямованих на порушення безпеки їхніх каналів зв'язку. За даними звіту Cybersecurity Ventures, у 2024 році глобальні витрати на кібербезпеку перевищили 200 млрд дол. США, при цьому значна частка інцидентів стосувалася компрометації безпроводових мереж, які є основою функціонування БПЛА. В Україні, де БПЛА активно використовуються у військових операціях та цивільних проєктах на тлі геополітичних викликів, захист каналів зв'язку набуває стратегічного значення.

Основними загрозами для каналів зв'язку БПЛА є перехоплення даних, глушіння сигналів, атаки типу "людина посередині" (Man-in-the-Middle) та несанкціоноване керування апаратними засобами. Існуючі методи захисту, такі як стандарти шифрування AES чи протоколи WPA3, забезпечують базовий рівень безпеки, але часто є недостатньо ефективними проти складних атак, зокрема квантових обчислень чи адаптивного радіоелектронного придушення. Критичний аналіз літератури (зокрема праць IEEE, NIST, а також досліджень компаній Thales і Raytheon) вказує на потребу в розробці комплексних підходів до захисту, які поєднують криптографічні методи, технології стійкості до перешкод і адаптивні протоколи зв'язку. Таким чином, актуальність дослідження зумовлена необхідністю створення ефективних методів і технологічних рішень для забезпечення захисту каналів зв'язку БПЛА, що відповідають сучасним викликам кібербезпеки та специфіці їхнього застосування.

Мета дослідження полягає у розробці теоретико-методологічних основ і практичних рекомендацій для забезпечення захисту каналів зв'язку безпілотних літальних апаратів шляхом впровадження адаптивної системи кібербезпеки, яка

інтегрує сучасні криптографічні технології, методи протидії перешкодам і ризик-орієнтований підхід. Для досягнення мети визначено такі завдання:

- визначити принципи роботи каналів зв’язку БПЛА та їх особливості в різних умовах експлуатації.
- класифікувати основні типи кіберзагроз для каналів зв’язку БПЛА та оцінити їх потенційний вплив.
- надати характеристику сучасних методів і технологій захисту каналів зв’язку, визначивши їх переваги та недоліки.
- проаналізувати криптографічні методи захисту даних у каналах зв’язку БПЛА та оцінити їх ефективність.
- дослідити протоколи аутентифікації та управління доступом для забезпечення безпеки каналів зв’язку БПЛА.
- оцінити можливості технологій виявлення та запобігання вторгненням у контексті захисту каналів зв’язку БПЛА.
- розробити модель захищеного каналу зв’язку для БПЛА з урахуванням виявлених вимог і загроз.
- провести тестування запропонованої моделі захисту каналу зв’язку та проаналізувати її ефективність.
- сформулювати рекомендації щодо впровадження системи захисту каналу зв’язку БПЛА в реальних умовах.

Об’єкт дослідження – процеси забезпечення безпеки каналів зв’язку безпілотних літальних апаратів, що охоплюють передачу даних, керування апаратними засобами та захист від зовнішніх кіберзагроз у контексті їхньої критичної ролі для виконання функціональних завдань.

Предмет дослідження – методи, технології та організаційні підходи до забезпечення захисту каналів зв’язку БПЛА, спрямовані на підвищення їхньої стійкості до кіберзагроз, зокрема перехоплення, глушіння та несанкціонованого доступу, з урахуванням сучасних технологічних і операційних вимог.

Результати дослідження мають практичну цінність для розробників, операторів і користувачів БПЛА у військовому, комерційному та цивільному

секторах. Запропонована адаптивна система захисту каналів зв’язку, що включає алгоритми шифрування, методи протидії перешкодам і моніторингу загроз, може бути впроваджена в системи керування БПЛА для підвищення їхньої безпеки та надійності. Рекомендації щодо конфігурації системи дозволять мінімізувати ризики компрометації даних і скоротити час реагування на кіберінциденти. Отримані результати можуть бути використані для вдосконалення стандартів кібербезпеки БПЛА, розробки навчальних програм для фахівців із кібербезпеки та адаптації національних і міжнародних нормативів у сфері безпілотних технологій. Запропоновані рішення є універсальними й можуть застосовуватися в різних країнах і умовах експлуатації БПЛА.

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КАНАЛУ ЗВ’ЯЗКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

1.1 Особливості функціонування каналів зв’язку безпілотних літальних апаратів

Безпілотні літальні апарати, що активно використовуються в цивільному, науковому, промисловому й оборонному секторах, є складними технічними системами, функціонування яких неможливе без якісного та стабільного каналу зв’язку. Саме система зв’язку є головною умовою для реалізації дистанційного керування, передавання телеметричної інформації, отримання навігаційних даних, відео- або фотоматеріалів із сенсорів, а також забезпечення зворотного зв’язку з наземною станцією.

Канал зв’язку безпілотного літального апарата — це технічно організоване середовище, що забезпечує передачу інформаційних потоків між оператором і апаратом у реальному часі або з допустимою затримкою. Структурно канал поділяється на напрям керування (тобто передачі команд з пункту управління), напрям телеметрії (тобто передачі даних від апарата до оператора), а також, за потреби, канал передавання навантаження (наприклад, відео з камери спостереження високої чіткості). Якість цього каналу безпосередньо впливає на здатність апарата точно виконувати завдання, уникати зіткнень, орієнтуватися в просторі та взаємодіяти з іншими системами.

Технічні характеристики каналу визначаються кількома основними факторами. Перш за все, це вибір частотного діапазону: у цивільному секторі найчастіше використовуються частоти 2,4 гігагерца та 5,8 гігагерца, тоді як у військовій сфері перевага надається спеціально зарезервованим і зашифрованим частотам. Частота визначає не лише дальність дії та стійкість до перешкод, але й можливість передачі великих обсягів інформації. Смуга пропускання є критичним параметром у випадку передавання відео або іншої інтенсивної інформації в реальному часі. Для цього використовуються сучасні методи модуляції, зокрема

багатоочкова ортогональна модуляція (Orthogonal Frequency Division Multiplexing) і адаптивне кодування [1].

Складна динаміка руху апарата у просторі (зміни положення, висоти, швидкості) вимагає гнучкості від системи зв’язку. Використання спрямованих або всеспрямованих антен, фазованих решіток та технологій із множинним входом і виходом (Multiple Input – Multiple Output) дозволяє забезпечити стійкий сигнал навіть за умови втрати прямої видимості [2]. Такі системи мають властивість самостійно орієнтувати напрям сигналу на оптимальний кут або перемикатися між кількома антенами.

Особливе значення має захист даних, які передаються через канал зв’язку. Шифрування трафіку, автентифікація передавачів та приймачів, цифрові підписи й протоколи захисту даних (наприклад, Advanced Encryption Standard) стають стандартом навіть у комерційних системах [3]. У військових застосуваннях також активно впроваджуються методи електронного захисту від перехоплення, втручання чи спроб подавлення сигналу з боку противника.

Слід також враховувати вплив зовнішніх умов, які можуть значно знижувати ефективність каналів зв’язку. До таких належать:

- електромагнітні перешкоди, особливо в урбанізованих або насичених технікою зонах;
- погодні явища, зокрема опади, грози, туман, які спричиняють згасання сигналу;
- складний рельєф місцевості (гори, ущелини), який блокує або спотворює передачу сигналу;
- ефект багатопроменевого поширення, коли сигнал одночасно надходить з кількох відбитих напрямів;
- обмежена дальність дії системи при низькій потужності передавача або застарілих радіомодулях [4].

В умовах інтенсивного розвитку технологій активно впроваджуються програмно-визначені радіосистеми, що дозволяють змінювати параметри зв’язку (частоти, модуляцію, потужність) у реальному часі відповідно до змін

навколишнього середовища. Вони підтримують динамічну адаптацію до завад, зміни місцезнаходження або навіть втрати основного каналу. Також перспективним напрямом є побудова сітчастих мереж, у яких кілька безпілотних апаратів виступають як вузли ретрансляції сигналу, забезпечуючи стійкий зв'язок навіть на великій відстані або в зоні дії ворожих завад.

Застосування штучного інтелекту у керуванні зв'язком дозволяє автоматично визначати найефективніші маршрути передачі даних, оптимізувати навантаження на канал, а також передбачати загрози для зв'язку, ґрунтуючись на поведінці сигналу в попередніх умовах. Усе це робить систему каналів зв'язку безпілотних літальних апаратів інтелектуальною, самоналагоджуваною та високонадійною [5].

Продовжуючи розгляд, варто наголосити на зростаючому значенні інтероперабельності каналів зв'язку безпілотних літальних апаратів із іншими технологічними системами. Це особливо актуально в умовах інтеграції БПЛА у великі інформаційно-керуючі комплекси – як у рамках систем моніторингу надзвичайних ситуацій, так і у військових багатоешелонних мережах. Для забезпечення взаємодії між апаратами різних виробників і платформами різних рівнів управління необхідне дотримання єдиних протоколів зв'язку, які передбачають не лише формат даних, а й політику безпеки, типи шифрування та узгодженість частотного плану.

Крім того, розвиток супутникових каналів зв'язку відкриває нові можливості для БПЛА, що діють поза межами прямої видимості або в районах без наземної інфраструктури. Такі канали мають більший радіус дії, але вимагають складнішої апаратної частини, що повинна бути адаптована до затримок сигналу та зміни орбітальних умов.

Окремою перспективною галуззю є впровадження квантового захисту каналів зв'язку, що забезпечує теоретично абсолютну стійкість до перехоплення завдяки принципам квантової фізики. Хоча ці технології наразі ще не застосовуються масово, вони мають значний потенціал у довгостроковій перспективі, особливо для стратегічних платформ.

Канали зв’язку безпілотних літальних апаратів не лише забезпечують виконання їхніх базових функцій, але й є критично важливою складовою безпеки, ефективності та взаємодії сучасних безпілотних систем. Їх удосконалення потребує системного, міждисциплінарного підходу, заснованого на тісній співпраці фахівців у сфері зв’язку, програмування, штучного інтелекту та авіаційних технологій.

1.2 Типи загроз кібербезпеці каналів зв’язку БПЛА

Канали зв’язку безпілотних літальних апаратів залишаються однією з найвразливіших частин усієї авіоніки дронів. У той час як апаратна частина зазвичай піддається фізичному захисту, канали передавання даних – зокрема ті, що використовують відкриті частотні діапазони або типові протоколи зв’язку – часто піддаються кіберзагрозам різного походження. Ці загрози формуються як на технічному, так і на стратегічному рівнях, і стосуються не лише втрати даних, а й потенційного перехоплення управління або підміни інформації [6].

Сутність таких загроз полягає в тому, що будь-який зовнішній доступ до переданих або отриманих сигналів може бути використаний зловмисниками для впливу на поведінку літального апарата, викрадення даних або завдання шкоди третім сторонам. Ризики посилюються за умов використання дронів у критично важливих сферах – обороні, енергетиці, охороні правопорядку або логістиці.

Нижче наведено таблицю 1.1, що класифікує основні типи кіберзагроз у сфері каналів зв’язку безпілотних літальних апаратів за критерієм джерела впливу, механізму реалізації та потенційних наслідків.

Таблиця 1.1 – Основні типи кіберзагроз у сфері каналів зв’язку [7,8]

Тип загрози	Механізм дії	Можливі наслідки
Перехоплення комунікацій	Прослуховування сигналу за допомогою спеціалізованого обладнання	Витік конфіденційних даних, виявлення маршруту польоту, компрометація місії

Продовження таблиці 1.1

Підміна сигналу (спуфінг)	Надсилання фальшивих сигналів управління чи GPS-даних	Зміна траєкторії, перенаправлення або знищення апарата, втрата контролю
Блокування сигналу (глушіння)	Створення сильнішого сигналу на частоті зв’язку	Втрата зв’язку, аварійне приземлення або автономна дія апарата без команди оператора
Впровадження шкідливого ПЗ	Інфікування програмного забезпечення бортового модуля через оновлення чи канал	Повне захоплення управління, саботаж, неконтрольовані дії
Атаки на наземну станцію	Злом інтерфейсів або серверів управління	Маніпуляція всією мережею дронів, централізоване виведення з ладу

Окрему небезпеку становлять гібридні загрози, які поєднують одночасно кілька методів впливу. Наприклад, підміна GPS-сигналу може супроводжуватися блокуванням основного каналу управління, а також одночасним проникненням у наземний сегмент. Такі атаки особливо важко виявити та знешкодити в режимі реального часу.

Наявність загроз змушує розробників впроваджувати багаторівневі механізми захисту, зокрема засоби виявлення аномалій, ізоляції сигналів, використання динамічних протоколів автентифікації та шифрування. Водночас слід враховувати, що захист не повинен ускладнювати роботу системи або створювати додаткові затримки – особливо в сценаріях оперативного реагування.

Забезпечення кібербезпеки каналів зв’язку безпілотних літальних апаратів вимагає постійного моніторингу, адаптації до нових сценаріїв атак і технологічної модернізації засобів зв’язку. Особливу увагу необхідно приділяти контексту використання дронів, оскільки рівень загрози напряму залежить від критичності виконуваних завдань.

1.3 Огляд сучасних методів і технологій захисту каналів зв’язку

В умовах дедалі активнішого використання безпілотних літальних апаратів у стратегічно важливих сферах, питання надійного захисту їхніх каналів зв’язку постає як один із пріоритетів інформаційної та технічної безпеки. Сучасні дрони передають великі обсяги інформації в режимі реального часу, функціонують у динамічному середовищі та залежать від стабільного і безпечного зв’язку з наземною інфраструктурою. У зв’язку з цим зростає потреба у впровадженні комплексних, гнучких і технологічно розвинених методів кіберзахисту.

На відміну від традиційних засобів зв’язку, канали між БПЛА та станціями управління мають ряд особливостей: змінна відстань, висока швидкість передачі, можливість втрати прямої видимості, а також необхідність роботи в умовах багатокористувацького середовища [9]. Усі ці аспекти створюють додаткові вектори для атак, зокрема дистанційних або координованих.

Сучасні підходи до забезпечення захищеності каналів поділяються на криптографічні, мережеві, протокольні, а також на методи активного моніторингу й адаптації. Вони застосовуються як окремо, так і в рамках інтегрованих систем захисту. Деякі з методів спрямовані на унеможливлення проникнення, інші – на виявлення та протидію атакам у реальному часі. Нижче представлено таблицю 1.2 з порівняльним оглядом основних сучасних методів і технологій захисту каналів зв’язку БПЛА.

Таблиця 1.2 – Огляд основних сучасних методів і технологій каналів зв'язку [10-11]

Метод / Технологія	Принцип дії	Особливості застосування
Асиметричне шифрування	Кодування даних із використанням відкритого й закритого ключів	Високий рівень захисту, однак потребує обчислювальних ресурсів на борту
Адаптивне управління частотою (FHSS)	Динамічне перемикання між частотами передачі	Ефективне проти глушіння та спуфінгу, потребує синхронізації між вузлами
Протоколи з багаторівневою автентифікацією	Багатоступеневе підтвердження правдоподібності учасника сеансу зв’язку	Підвищує стійкість до спроб проникнення в мережу, застосовується в комерційних і військових системах
Захищені програмно-визначені радіосистеми	Можливість зміни параметрів зв’язку (частота, модуляція, потужність) у реальному часі	Гнучкість, адаптація до середовища, інтеграція з ІІ, складна реалізація
Системи виявлення аномалій	Аналіз поведінки каналу з метою виявлення нетипових сигналів або активності	Не блокує атаку, але дозволяє вчасно реагувати, потребує бази нормальних даних
Імітаційний захист (obfuscation)	Приховування реального змісту або структури переданих пакетів	Знижує ефективність аналізу трафіку зловмисником, додаткове навантаження на канал

Комплексна реалізація цих технологій вимагає відповідного апаратного й програмного забезпечення, а також узгоджених стандартів між виробниками. Особливо перспективними виглядають комбінації методів, які дозволяють досягати балансу між швидкістю передачі даних і ступенем їх захисту. Наприклад, використання асиметричного шифрування разом із адаптивним перемиканням частот значно знижує шанси на перехоплення навіть у разі розкриття одного з параметрів.

Крім того, в умовах стрімкого розвитку штучного інтелекту, починає набирати популярності використання нейронних мереж для самонавчання систем захисту. Такі системи здатні розпізнавати нові типи загроз без попереднього програмування, що суттєво розширює горизонт оборонних можливостей каналів зв’язку БПЛА.

Ефективний захист каналів зв’язку безпілотних літальних апаратів є багатошаровою системою, яка поєднує криптографічну, радіотехнічну, програмну та аналітичну складові. Успішне впровадження таких рішень потребує не лише технічної підготовки, а й міждисциплінарного підходу до розробки архітектури захисту.

Серед найважливіших аспектів ефективного застосування засобів захисту є питання сумісності нових технологій із наявними апаратними платформами. У багатьох випадках безпілотні літальні апарати мають обмежені обчислювальні ресурси та енергетичну автономність, що ускладнює інтеграцію високопродуктивних криптографічних алгоритмів чи систем з елементами штучного інтелекту. Тому актуальними залишаються рішення, що оптимізовані за обсягом енергоспоживання, швидкістю обробки сигналу та можливістю оновлення прошивки дистанційно.

З огляду на швидкий розвиток засобів радіоелектронної боротьби, особливу увагу слід приділяти динамічності та адаптивності захисних механізмів. Статичні методи захисту, хоча й забезпечують базову безпеку, можуть бути легко обійдені сучасними засобами аналізу спектра або зламом шифру, якщо використовуються передбачувані ключі чи стандартні протоколи. Саме тому все більшого поширення

набувають концепції ситуаційного реагування – коли апарат у режимі реального часу змінює свої комунікаційні параметри на основі аналізу навколишнього середовища.

Окремо слід зазначити роль міжмережевих шлюзів та проксі-механізмів, які дозволяють ізолювати канал управління від загального інформаційного трафіку. У деяких випадках навіть використовується принцип зонування мережі, коли критичні сигнали передаються через окремі зашифровані канали, фізично або логічно ізольовані від інших функціональних потоків.

Ще одним важливим напрямом є розробка стандартів взаємодії між різними класами безпілотних апаратів та наземних станцій. Стандартизовані протоколи, що передбачають вбудовані засоби перевірки автентичності, значно спрощують інтеграцію апаратів у більші системи управління повітряним рухом, забезпечуючи водночас високий рівень кіберстійкості. При цьому унеможливлюється підміна даних або несанкціоноване втручання, навіть за наявності великої кількості однотипних дронів у межах одного повітряного простору [12].

Узагальнюючи, слід підкреслити, що ефективний захист каналів зв’язку не може бути побудований виключно на одному рішенні. Його основою є багатошарова система, в якій кожен компонент виконує свою функцію: шифрування – запобігає перехопленню, моніторинг – виявляє аномалії, адаптація – дозволяє уникати атак, а стандартизація – забезпечує масштабованість і надійність у складних сценаріях.

Система каналів зв’язку безпілотних літальних апаратів є ключовим елементом їхнього функціонування, забезпечуючи дистанційне керування, передачу телеметрії та даних із сенсорів, а також взаємодію з наземними станціями. Якість і надійність цих каналів визначаються вибором частотного діапазону, смугою пропускання, методами модуляції та адаптивними технологіями, такими як спрямовані антени чи MIMO. Захист даних, включаючи шифрування, автентифікацію та протидію перехопленню, відіграє критичну роль, особливо у військових і стратегічних застосуваннях. Зовнішні фактори, як-от електромагнітні перешкоди, погодні умови чи складний рельєф, створюють додаткові виклики, що

вимагають використання програмно-визначених радіосистем, сітчастих мереж і штучного інтелекту для адаптації до змін середовища.

Інтеграція БПЛА у великі інформаційно-керуючі комплекси підкреслює важливість інтероперабельності та єдиних протоколів зв’язку. Супутникові канали та перспективні квантові технології відкривають нові можливості для зв’язку на великих відстанях і в складних умовах. Таким чином, канали зв’язку БПЛА є складною, багатокомпонентною системою, що потребує міждисциплінарного підходу для забезпечення безпеки, ефективності та надійності.

Канали зв’язку БПЛА є вразливими до кіберзагроз, таких як перехоплення, спуфінг, глушіння, впровадження шкідливого ПЗ та атаки на наземні станції, що можуть призвести до втрати контролю, витоку даних або компрометації місії. Гібридні атаки, що поєднують кілька методів, ускладнюють захист у реальному часі. Для протидії необхідні багаторівневі механізми, включаючи виявлення аномалій, динамічні протоколи автентифікації та шифрування, які не повинні знижувати швидкість роботи системи. Постійний моніторинг, адаптація до нових загроз і технологічна модернізація є обов’язковими для забезпечення кібербезпеки, особливо в критично важливих сферах.

Сучасні методи захисту каналів зв’язку БПЛА поєднують криптографічні, мережеві, протокольні та аналітичні підходи, включаючи асиметричне шифрування, адаптивне управління частотою, багаторівневу автентифікацію, програмно-визначені радіосистеми, виявлення аномалій та імітаційний захист. Інтеграція штучного інтелекту дозволяє системам самонавчатися та розпізнавати нові загрози, тоді як комбінація методів забезпечує баланс між швидкістю передачі даних і безпекою.

Обмежені обчислювальні ресурси БПЛА вимагають оптимізації захисних механізмів за енергоспоживанням і швидкістю обробки. Динамічність і адаптивність захисту, включаючи ситуаційне реагування та ізоляцію критичних каналів, є ключовими для протидії сучасним засобам радіоелектронної боротьби. Стандартизація протоколів забезпечує сумісність і масштабованість у складних

системах, а багатошаровий підхід, що поєднує шифрування, моніторинг і адаптацію, гарантує надійний захист каналів зв’язку в динамічних і вразливих умовах.

2 АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КАНАЛУ ЗВ’ЯЗКУ БПЛА

2.1 Криптографічні методи захисту даних у каналах зв’язку

Криптографічні методи захисту даних у каналах зв’язку безпілотних літальних апаратів є основою забезпечення безпеки передачі інформації в умовах високої вразливості до кіберзагроз. Ці методи спрямовані на захист конфіденційності, цілісності та автентичності даних, що передаються між БПЛА та наземними станціями, у середовищі, де динамічні умови, обмежені ресурси та потенційні атаки створюють значні виклики. Унікальність криптографічного підходу для БПЛА полягає в необхідності поєднання високого рівня захисту з мінімальними затримками та енергоефективністю, щоб не порушувати оперативність апаратних систем.

Основним завданням криптографії в контексті БПЛА є створення захищених каналів, які унеможливлюють несанкціонований доступ до команд управління, телеметричних даних або відеопотоків. Для цього застосовуються різні підходи, які враховують специфіку безпілотних систем, зокрема потребу в обробці великих обсягів інформації в реальному часі та обмеження бортових обчислювальних ресурсів [13]. Симетричне шифрування, наприклад, алгоритм AES, є популярним вибором завдяки своїй швидкості та ефективності при обробці потокових даних, таких як відеосигнали високої чіткості. Однак його використання ускладнюється проблемою безпечного розподілу ключів, особливо в умовах нестабільного зв’язку або віддалених операцій.

Для вирішення цієї проблеми застосовуються асиметричні алгоритми, які базуються на парах ключів (відкритого та закритого). Такі алгоритми, як elliptic curve cryptography, забезпечують ефективний обмін ключами та автентифікацію сторін, що є критично важливим для захисту каналу управління від атак типу "людина посередині". ECC має перевагу над іншими асиметричними алгоритмами, такими як RSA, завдяки меншим розмірам ключів, що знижує обчислювальне навантаження та енергоспоживання [14], що є ключовим для БПЛА з обмеженими ресурсами. Однак асиметричне шифрування зазвичай використовується лише на

етапі ініціалізації зв’язку через його вищу ресурсоємність порівняно з симетричними методами.

Порівняння основних криптографічних алгоритмів, придатних для використання в каналах зв’язку БПЛА, наведено в таблиці 2.1, яка оцінює їх за такими параметрами, як тип шифрування, розмір ключа, швидкість обробки та стійкість до атак.

Таблиця 2.1 – Порівняння основних криптографічних алгоритмів [15,16]

Алгоритм	Тип шифрування	Розмір ключа (біт)	Швидкість обробки	Стійкість до атак
AES	Симетричне	128–256	Висока	Висока
ECC	Асиметричне	256–521	Середня	Висока
RSA	Асиметричне	2048–4096	Низька	Висока
ChaCha	Симетричне	256	Висока	Середня

Для забезпечення цілісності даних і захисту від підміни сигналів застосовуються хеш-функції, такі як SHA-256, які генерують унікальні контрольні суми для перевірки незмінності інформації. Цифрові підписи, створені на основі асиметричних алгоритмів, дозволяють підтверджувати автентичність джерела даних, що є особливо важливим у військових системах, де будь-яка спроба фальсифікації може призвести до катастрофічних наслідків. Крім того, протоколи обміну ключами, такі як Diffie-Hellman, забезпечують безпечне встановлення сесійних ключів навіть у незахищених мережах, що є актуальним для БПЛА, які працюють у зонах із високим рівнем перешкод [17].

Перспективним напрямом є впровадження постквантової криптографії, яка розробляється для захисту від атак із використанням квантових комп’ютерів. Алгоритми на основі ґраток (lattice-based cryptography) [18] або кодів (code-based cryptography) пропонують стійкість до квантових обчислень, які можуть зламати традиційні алгоритми, такі як RSA чи ECC. Хоча ці методи ще перебувають на стадії досліджень, їхня інтеграція в системи БПЛА є стратегічно важливою для

забезпечення безпеки в довгостроковій перспективі, особливо для апаратів, що виконують критично важливі завдання.

Інтеграція штучного інтелекту (ШІ) у криптографічні системи дозволяє підвищити їхню адаптивність. ШІ може аналізувати патерни трафіку, виявляти спроби атак у реальному часі та автоматично налаштовувати параметри шифрування залежно від умов середовища. Наприклад, при виявленні аномальної активності ШІ може змінити алгоритм шифрування або переключити канал зв’язку на резервний, мінімізуючи ризик компрометації. Однак використання ШІ також вимагає додаткових обчислювальних ресурсів, що може бути проблематичним для легких БПЛА.

Енергоефективність криптографічних методів є критично важливою для БПЛА, оскільки бортові системи мають обмежену потужність акумуляторів. У таблиці 2.2 наведено порівняння основних методів за їхнім енергоспоживанням, обчислювальною складністю та типовими сценаріями застосування.

Таблиця 2.2 – Енергоефективність криптографічних методів для БПЛА [19]

Метод	Енергоспоживання	Обчислювальна складність	Застосування
AES	Низьке	Низьке	Потокове відео, телеметрія
ECC	Середнє	Середнє	Автентифікація, обмін ключами
RSA	Висока	Висока	Обмежене, ініціалізація зв’язку
Post-Quantum (Lattice)	Висока	Висока	Стратегічні системи майбутнього

У сітчастих мережах, де кілька БПЛА діють як вузли ретрансляції, криптографічні методи повинні забезпечувати синхронізацію ключів між усіма учасниками. Групові протоколи шифрування, такі як Group Diffie-Hellman, дозволяють створювати спільні ключі для кількох вузлів, зберігаючи безпеку.

Однак зростання кількості учасників мережі може ускладнювати обробку даних, що вимагає оптимізації протоколів для зниження затримок.

Стандартизація криптографічних рішень є ключовою для забезпечення інтероперабельності між БПЛА різних виробників. Міжнародні стандарти, такі як NIST SP 800-38, визначають вимоги до алгоритмів шифрування, що використовуються в критичних системах. Дотримання цих стандартів дозволяє створювати системи, які безпечно взаємодіють у складних мережах, таких як системи управління повітряним рухом.

Криптографічні методи захисту каналів зв’язку БПЛА формують багатошарову систему, що поєднує симетричне та асиметричне шифрування, хеш-функції, цифрові підписи та перспективні постквантові алгоритми. Їхнє застосування вимагає балансу між безпекою, швидкістю та енергоефективністю, що є особливо важливим для апаратів із обмеженими ресурсами. Інтеграція штучного інтелекту та стандартизація протоколів сприяють підвищенню стійкості до сучасних загроз, тоді як розвиток постквантової криптографії відкриває перспективи для захисту від майбутніх викликів, пов’язаних із квантовими обчисленнями.

2.2 Застосування протоколів аутентифікації та управління доступом

Протоколи аутентифікації та управління доступом є критично важливими компонентами захисту каналів зв’язку без -пілотних літальних апаратів, оскільки вони забезпечують перевірку ідентичності учасників зв’язку та обмежують доступ до системи лише для авторизованих користувачів чи пристроїв. У контексті БПЛА, де канали зв’язку є вразливими до атак, таких як підміна сигналу чи несанкціоноване втручання, ці протоколи відіграють ключову роль у запобіганні компрометації системи та забезпеченні безпеки критичних операцій.

Аутентифікація в системах БПЛА передбачає підтвердження ідентичності як самого апарата, так і наземної станції чи оператора. Основною метою є унеможливлення доступу зловмисників до каналу управління або даних, що

передаються. Для цього застосовуються протоколи, які базуються на криптографічних механізмах, таких як цифрові сертифікати, токени або біометричні дані. Наприклад, протокол Transport Layer Security використовується для створення захищеного з'єднання, де БПЛА та наземна станція обмінюються цифровими сертифікатами, підписаними довіреним центром сертифікації [19]. Це дозволяє кожній стороні перевірити легітимність іншої, запобігаючи атакам типу «людина посередині».

Управління доступом, у свою чергу, регулює, які дії може виконувати аутентифікований учасник. У системах БПЛА це включає розмежування прав доступу до команд управління, телеметричних даних або конфігурації апарата. Наприклад, оператор може мати повний доступ до всіх функцій, тоді як технік – лише до діагностичних даних. Для реалізації управління доступом часто застосовуються моделі на основі ролей (Role-Based Access Control, RBAC), де права користувача визначаються його роллю в системі [20]. Це знижує ризик ненавмисного чи зловмисного використання системи, особливо в складних операціях, що передбачають взаємодію кількох БПЛА або інтеграцію з інформаційно-керуючими комплексами.

Одним із поширених підходів є використання протоколу OAuth 2.0, адаптованого для БПЛА. Цей протокол дозволяє делегувати доступ до певних ресурсів без необхідності передачі облікових даних [21]. Наприклад, БПЛА може отримати токен доступу від сервера авторизації, який підтверджує його право на передачу даних до хмарного сервісу. Такий підхід є особливо корисним у сітчастих мережах, де кілька апаратів взаємодіють як вузли ретрансляції, і кожен вузол потребує перевірки прав доступу.

Для підвищення безпеки застосовуються багаторівневі протоколи аутентифікації, які комбінують кілька факторів, таких як знання (пароль або PIN-код), володіння (фізичний токен чи смарт-карта) та унікальні характеристики (біометричні дані оператора). У військових системах БПЛА це може включати апаратні модулі безпеки, які зберігають криптографічні ключі та виконують аутентифікацію на апаратному рівні, що значно ускладнює їх компрометацію.

Схема багаторівневої аутентифікації для БПЛА представлена на рисунку 2.1

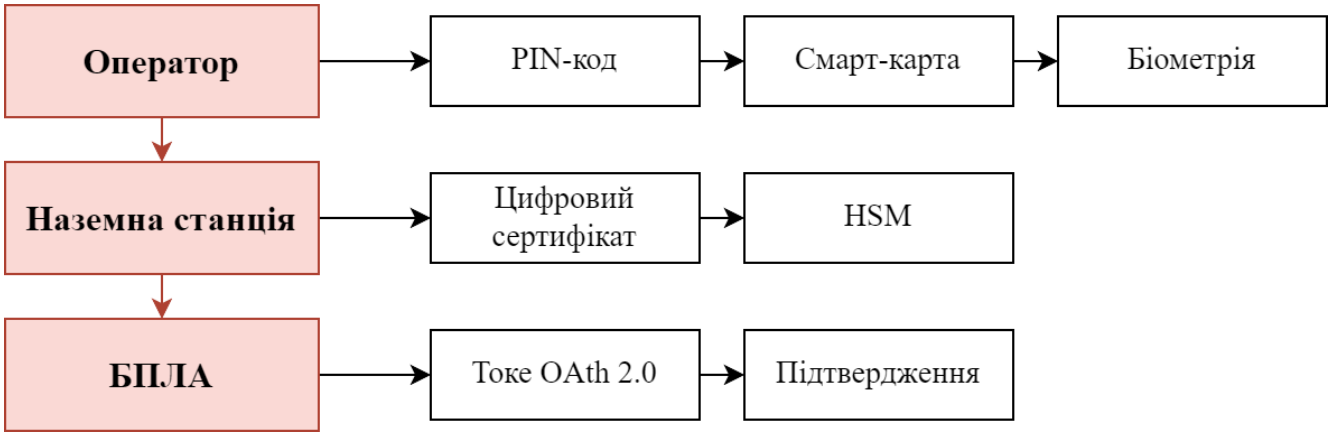

Рисунок 2.1 – Схема багаторівневої аутентифікації для БПЛА

Ця схема ілюструє послідовність перевірок, де оператор проходить три етапи аутентифікації, наземна станція використовує сертифікат і апаратний модуль, а БПЛА підтверджує свою ідентичність через токен. Такий підхід забезпечує високий рівень захисту навіть у разі компрометації одного з елементів.

Особливу увагу приділено адаптивності протоколів до умов експлуатації БПЛА. У середовищах із нестабільним зв’язком, наприклад, у зонах із сильними перешкодами, застосовуються легковагові протоколи, такі як Datagram Transport Layer Security, які оптимізовані для ненадійних мережі забезпечують аутентифікацію з мінімальними затримками. У таких випадках також використовуються механізми кешування токенів, щоб уникнути повторної аутентифікації при короткочасній втраті зв’язку [22].

Інтеграція штучного інтелекту у протоколи аутентифікації дозволяє аналізувати поведінку користувачів і пристроїв для виявлення аномалій. Наприклад, ШІ може помітити нетипові шаблони команд або незвичайну активність БПЛА, що може свідчити про спробу несанкціонованого доступу. Такі системи здатні автоматично блокувати підозрілі сеанси або вимагати додаткової перевірки, підвищуючи загальну стійкість системи.

У контексті сітчастих мереж, де БПЛА взаємодіють між собою, протоколи аутентифікації повинні забезпечувати швидку та безпечну перевірку всіх вузлів. Для цього застосовуються децентралізовані системи, такі як блокчейн-базовані

протоколи, де кожен апарат має унікальний ідентифікатор, що підтверджується через розподілений реєстр. Це дозволяє уникнути залежності від центрального сервера авторизації, що є критичним у віддалених або ворожих середовищах.

Стандартизація протоколів аутентифікації та управління доступом є важливим аспектом для забезпечення інтероперабельності. Міжнародні стандарти, такі як ISO/IEC 27001 [23] або NIST SP 800-63 [24], надають рекомендації щодо реалізації безпечних механізмів аутентифікації, які адаптуються до потреб авіаційних систем. Дотримання цих стандартів дозволяє створювати масштабовані рішення, які підтримують інтеграцію БПЛА в глобальні системи управління повітряним рухом або моніторингу.

Ефективність протоколів аутентифікації та управління доступом залежить від їхньої здатності адаптуватися до обмежених обчислювальних ресурсів БПЛА та динамічних умов експлуатації. Легковагові протоколи, багаторівнева перевірка, інтеграція ШІ та децентралізовані системи забезпечують надійний захист від несанкціонованого доступу, зберігаючи при цьому оперативність і гнучкість системи. У міру розвитку технологій і зростання складності кіберзагроз ці протоколи потребуватимуть постійного вдосконалення, щоб гарантувати безпеку каналів зв’язку БПЛА в майбутньому.

2.3. Використання технологій виявлення та запобігання вторгненням

Технології виявлення та запобігання вторгненням є важливим елементом захисту каналів зв’язку безпілотних літальних апаратів від кіберзагроз, таких як несанкціонований доступ, маніпуляція даними чи спроби порушення роботи системи. У контексті БПЛА, де канали зв’язку постійно піддаються ризикам перехоплення, спуфінгу або глушіння, IDPS відіграють ключову роль у моніторингу, аналізі та нейтралізації потенційних атак у реальному часі [25]. Ці технології дозволяють не лише виявляти аномальну активність, а й активно протидіяти загрозам, забезпечуючи стабільність і безпеку операцій.

Системи виявлення вторгнень аналізують трафік у каналах зв’язку БПЛА, ідентифікуючи відхилення від нормальної поведінки або сигнатури відомих атак. Наприклад, IDS може розпізнати незвичайний обсяг даних, нетипові команди управління або спроби підключення від неавторизованих джерел. Для цього використовуються два основні підходи: сигнатурний аналіз, який порівнює трафік із базою відомих шаблонів атак, та аномальний аналіз, який виявляє відхилення від статистичної норми. Аномальний аналіз є особливо ефективним у динамічних середовищах БПЛА, де нові типи атак можуть не мати відомих сигнатур [26].

Системи запобігання вторгненням доповнюють IDS, активно реагуючи на виявлені загрози. Наприклад, IPS може автоматично блокувати підозрілі пакети даних, ізолювати скомпрометовані канали або переключати зв’язок на резервний частотний діапазон. У БПЛА, де затримки в реакції можуть призвести до втрати контролю, IPS налаштовуються на швидке реагування, мінімізуючи вплив на продуктивність системи. Для цього застосовуються програмно-визначені радіосистеми, які дозволяють динамічно змінювати параметри зв’язку, такі як частота чи модуляція, у відповідь на виявлені атаки.

Інтеграція штучного інтелекту і машинного навчання значно підвищує ефективність IDPS. ШІ здатен аналізувати великі обсяги даних у реальному часі, виявляючи складні шаблони атак, які можуть залишатися непоміченими традиційними методами. Наприклад, алгоритми машинного навчання можуть навчатися на основі історичних даних про трафік, створюючи базові моделі нормальної поведінки БПЛА. При виявленні аномалій, таких як різке збільшення запитів до бортової системи, ШІ може ініціювати додаткову перевірку або ізоляцію каналу. Крім того, ШІ дозволяє адаптувати IDPS до нових загроз без необхідності оновлення сигнатур, що є критично важливим у швидко мінливому кіберсередовищі.

У сітчастих мережах, де кілька БПЛА взаємодіють як вузли ретрансляції, IDPS повинні забезпечувати координацію між апаратами для виявлення розподілених атак. Наприклад, атака типу "відмова в обслуговуванні" може спрямовуватися на кілька вузлів одночасно, що вимагає спільного аналізу трафіку

всією мережею. Для цього застосовуються децентралізовані IDPS, які дозволяють кожному БПЛА самостійно аналізувати локальний трафік і обмінюватися даними про загрози з іншими вузлами. Такий підхід підвищує стійкість системи до атак, навіть якщо частина мережі скомпрометована.

Схема роботи IDPS у системі зв’язку БПЛА представлена на рисунку 2.2.

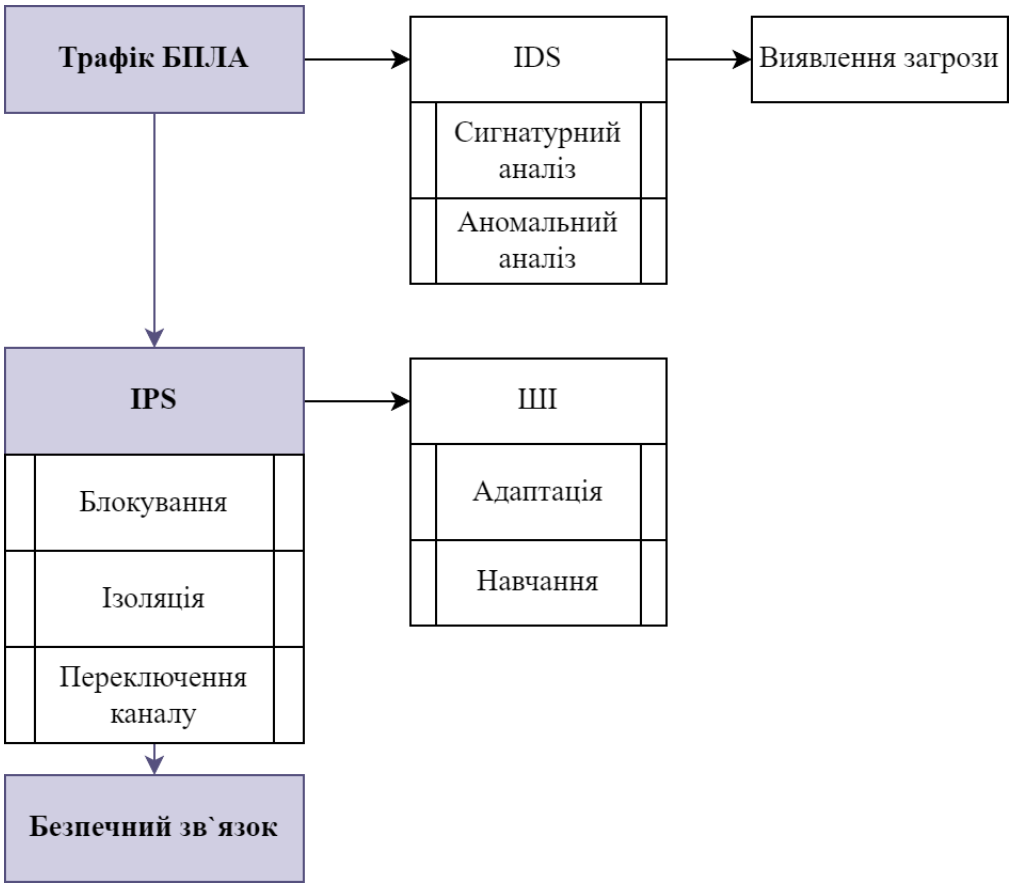

Рисунок 2.2 – Схема роботи IDPS

Ця схема показує послідовність обробки трафіку: від аналізу IDS до реакції IPS і адаптації системи за допомогою ШІ, що забезпечує безперервність захищеного зв’язку.

Для підвищення ефективності IDPS у БПЛА застосовуються технології контекстного аналізу, які враховують специфіку операційного середовища, наприклад, географічне розташування, погодні умови чи тип виконуваної місії. Контекстний аналіз дозволяє відрізняти легітимні зміни в трафіку, викликані зовнішніми факторами, від потенційних атак. Наприклад, короткочасне збільшення

затримок у каналі через грозу не буде помилково інтерпретовано як спроба глушіння.

Обмежені обчислювальні ресурси БПЛА створюють виклик для впровадження IDPS, оскільки складні алгоритми аналізу можуть знижувати енергоефективність апарата. Для вирішення цієї проблеми використовуються оптимізовані алгоритми, які виконують попередній аналіз на борту, а більш ресурсоємні операції передаються на наземні сервери або хмарні платформи. Крім того, легковагові протоколи, такі як CoAP, адаптовані для пристроїв з обмеженими ресурсами, забезпечують швидкий обмін даними про загрози між БПЛА та наземною інфраструктурою [27].

У військових застосуваннях IDPS інтегруються з системами радіоелектронної боротьби, що дозволяє виявляти та нейтралізувати спроби подавлення сигналу. Наприклад, при виявленні глушіння IDPS може автоматично активувати адаптивне управління частотою (FHSS), перемикаючи зв’язок на менш завантажений діапазон. Така інтеграція забезпечує стійкість каналу зв’язку навіть у ворожих умовах.

Стандартизація IDPS є важливим аспектом для забезпечення сумісності між різними платформами БПЛА. Міжнародні стандарти, такі як NIST SP 800-94, надають рекомендації щодо реалізації систем виявлення та запобігання вторгненням, які враховують специфіку авіаційних систем. Дотримання цих стандартів сприяє створенню уніфікованих рішень, які можуть бути інтегровані в глобальні системи управління повітряним рухом або моніторингу.

Ефективність технологій виявлення та запобігання вторгненням у каналах зв’язку БПЛА залежить від їхньої здатності поєднувати швидкий аналіз, активну протидію та адаптацію до нових загроз. Інтеграція ШІ, контекстний аналіз, децентралізовані архітектури та оптимізовані протоколи дозволяють створювати гнучкі та стійкі системи захисту, які відповідають вимогам динамічних і вразливих умов експлуатації БПЛА. У міру зростання складності кіберзагроз ці технології потребуватимуть постійного розвитку, щоб забезпечити надійність і безпеку безпілотних систем у майбутньому.

Другий розділ присвячений аналізу ключових аспектів захисту каналів зв’язку безпілотних літальних апаратів через застосування криптографічних методів, протоколів аутентифікації та управління доступом, а також технологій виявлення та запобігання вторгненням. Криптографічні методи, що поєднують симетричне та асиметричне шифрування, хеш-функції та перспективні постквантові алгоритми, забезпечують конфіденційність, цілісність і автентичність даних, враховуючи обмежені обчислювальні ресурси БПЛА. Протоколи аутентифікації, включаючи багаторівневу перевірку та децентралізовані системи, такі як блокчейн-базовані підходи, гарантують захист від несанкціонованого доступу, тоді як управління доступом на основі ролей підвищує безпеку складних операцій.

Технології виявлення та запобігання вторгненням, інтегровані з штучним інтелектом і контекстним аналізом, дозволяють оперативно виявляти та нейтралізувати кіберзагрози, адаптуючись до динамічних умов експлуатації. Усі ці компоненти формують багатошарову систему захисту, яка балансує між безпекою, енергоефективністю та швидкістю обробки даних. Стандартизація, оптимізація ресурсів і постійне вдосконалення технологій є необхідними для забезпечення стійкості каналів зв’язку БПЛА до сучасних і майбутніх кіберзагроз, що підкреслює важливість міждисциплінарного підходу до розвитку безпілотних систем.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИСТУ КАНАЛУ ЗВ’ЯЗКУ БПЛА

3.1 Розробка моделі захищеного каналу зв’язку для БПЛА

Розробка моделі захищеного каналу зв’язку для безпілотних літальних апаратів є складним завданням, яке вимагає комплексного підходу до забезпечення безпеки, надійності та ефективності передачі даних у динамічних і вразливих умовах. Канали зв’язку БПЛА повинні підтримувати дистанційне керування, передачу телеметрії, навігаційних даних і відеопотоків, одночасно протидіючи кіберзагрозам, таким як перехоплення, спуфінг чи глушіння. Модель захищеного каналу зв’язку базується на інтеграції криптографічних методів, протоколів аутентифікації, технологій виявлення вторгнень і адаптивних механізмів, що враховують обмежені обчислювальні ресурси апарата та зовнішні фактори, такі як перешкоди чи погодні умови.

Основна мета моделі полягає в створенні стійкого каналу, який забезпечує конфіденційність, цілісність і автентичність даних, а також швидке реагування на загрози без значного впливу на продуктивність системи. Для цього модель включає кілька функціональних шарів: фізичний шар для передачі сигналу, шар захисту даних, шар аутентифікації та шар моніторингу й реагування. Кожен шар виконує специфічні функції, але їхня взаємодія забезпечує цілісний захист каналу.

На фізичному шарі використовуються адаптивні радіотехнології, такі як програмно-визначені радіосистеми та технології множинного входу-виходу (MIMO), які дозволяють оптимізувати частотний діапазон і підтримувати зв’язок у складних умовах, наприклад, при втраті прямої видимості. Для підвищення стійкості до глушіння застосовується адаптивне управління частотою (Frequency Hopping Spread Spectrum, FHSS), яке динамічно перемикає частоти передачі, ускладнюючи спроби подавлення сигналу.

Шар захисту даних базується на комбінації криптографічних методів. Симетричне шифрування, зокрема алгоритм AES-256, використовується для захисту потокових даних, таких як відеосигнали, завдяки високій швидкості обробки. Асиметричне шифрування, наприклад, на основі elliptic curve

cryptography, застосовується для безпечного обміну ключами та створення цифрових підписів, що забезпечують автентичність команд управління. Для перевірки цілісності даних використовуються хеш-функції, такі як SHA-256, які дозволяють виявляти будь-які зміни в переданих пакетах.

Шар аутентифікації відповідає за перевірку ідентичності всіх учасників зв'язку – БПЛА, наземної станції та оператора. Для цього застосовується багаторівнева аутентифікація, яка поєднує цифрові сертифікати, токени OAuth 2.0 і апаратні модулі безпеки. Такий підхід унеможливлює несанкціонований доступ, навіть якщо один із факторів аутентифікації скомпрометовано. Управління доступом на основі ролей регулює права учасників, наприклад, обмежуючи доступ до критичних команд лише для авторизованих операторів.

Шар моніторингу й реагування включає системи виявлення та запобігання вторгненням (IDPS), які аналізують трафік у реальному часі, виявляючи аномалії або сигнатури атак. Штучний інтелект (ШІ) використовується для адаптивного аналізу, що дозволяє розпізнавати нові загрози без попереднього програмування. У разі виявлення атаки IDPS може ізолювати скомпрометований канал, переключити зв'язок на резервний або активувати альтернативний частотний діапазон.

Схема моделі захищеного каналу зв'язку для БПЛА представлена в спрощеному вигляді на рисунку 3.1.

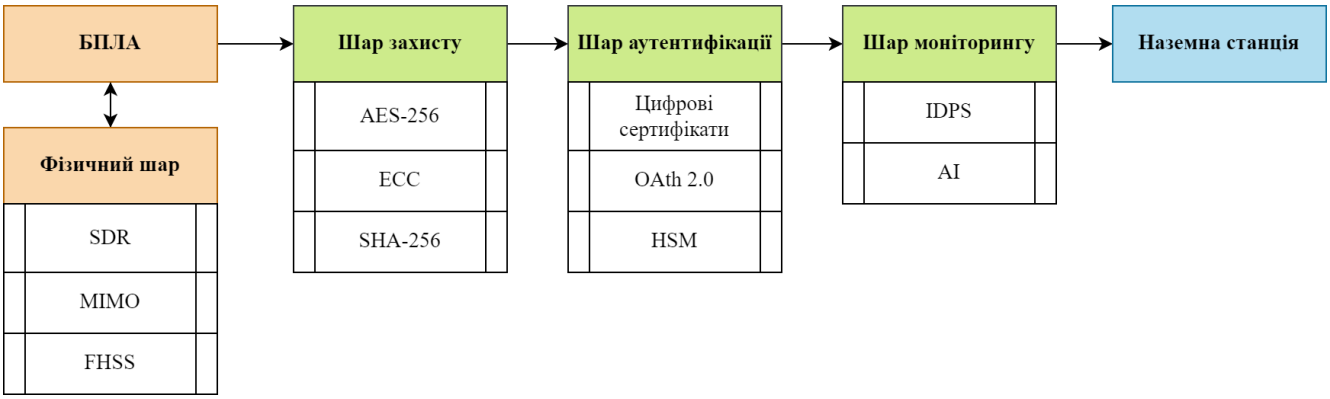

Рисунок 3.1 Схема моделі захищеного каналу зв'язку для БПЛА

Схема ілюструє послідовність обробки даних через різні шари, починаючи від фізичної передачі сигналу до моніторингу безпеки, що забезпечує захищений

зв’язок між БПЛА та наземною станцією. Для реалізації моделі враховуються ключові принципи, які забезпечують її ефективність і практичність:

- Енергоефективність - Алгоритми та протоколи оптимізуються для роботи на бортових системах із обмеженими ресурсами, використовуючи легковагові протоколи, такі як DTLS, і мінімізуючи обчислювальне навантаження.
- Адаптивність – Модель підтримує динамічну зміну параметрів зв’язку (частоти, модуляції, ключів) у відповідь на зовнішні умови чи виявлені загрози.
- Масштабованість – Модель сумісна з сітчастими мережами, де кілька БПЛА діють як вузли ретрансляції, забезпечуючи координацію аутентифікації та моніторингу.
- Стандартизація – Використання міжнародних стандартів, таких як NIST SP 800-38 для криптографії та ISO/IEC 27001 для управління безпекою, забезпечує інтероперабельність із іншими системами.
- Стійкість до нових загроз – Інтеграція ШІ та підтримка постквантових алгоритмів дозволяють моделі адаптуватися до майбутніх кіберзагроз, включаючи атаки з використанням квантових комп’ютерів.

Модель захищеного каналу зв’язку для БПЛА є багатошаровою системою, яка поєднує передові технології для забезпечення безпеки в умовах високої динаміки та вразливості. Її реалізація вимагає ретельного балансу між безпекою, продуктивністю та ресурсами, а також постійного вдосконалення для протидії новим загрозам. Такий підхід дозволяє створювати надійні канали зв’язку, які підтримують критичні операції БПЛА в цивільних, промислових і військових сферах.

3.2. Тестування та аналіз ефективності запропонованих рішень

Тестування та аналіз ефективності запропонованої моделі захищеного каналу зв’язку для безпілотних літальних апаратів (БПЛА) є критично важливим етапом, який дозволяє оцінити її надійність, стійкість до кіберзагроз і придатність до реальних умов експлуатації. Цей процес включає моделювання роботи каналу,

оцінку продуктивності криптографічних алгоритмів, протоколів аутентифікації та систем виявлення вторгнень, а також аналіз їхнього впливу на обчислювальні ресурси та енергоефективність БПЛА. Тестування проводиться в контрольованих і наближених до реальних умовах, щоб забезпечити всебічну оцінку запропонованих рішень.

Для оцінки ефективності моделі використовується програмне моделювання, яке дозволяє імітувати різні сценарії роботи БПЛА, включаючи нормальні операції, атаки та несприятливі зовнішні умови, такі як електромагнітні перешкоди чи втрата прямої видимості. Програмне середовище, наприклад, Python із бібліотеками для криптографії (PyCryptodome) та аналізу мережі (Scapy), застосовується для створення віртуального каналу зв'язку, що імітує передачу даних між БПЛА та наземною станцією. Нижче наведено приклад коду на Python, який демонструє базову реалізацію шифрування даних за допомогою AES-256 і перевірки їхньої цілісності через SHA-256, що є частиною тестування криптографічного шару моделі.

```
    from Crypto.Cipher import AES
    from Crypto.Hash import SHA256
    from Crypto.Random import get_random_bytes
    import time
    # Генерація ключа та ініціалізаційного вектора
    key = get_random_bytes(32)  # Ключ для AES-256
    iv = get_random_bytes(16)   # Ініціалізаційний вектор
    # Дані для передачі (імітація телеметрії)
    data = b"UAV telemetry: altitude=500m, speed=20m/s"
    # Шифрування даних
    def encrypt_data(data, key, iv):
        cipher = AES.new(key, AES.MODE_CBC, iv)
        padded_data = data + b"\0" * (AES.block_size -
len(data) % AES.block_size)
        ciphertext = cipher.encrypt(padded_data)
        return ciphertext
    # Розшифрування даних
    def decrypt_data(ciphertext, key, iv):
        cipher = AES.new(key, AES.MODE_CBC, iv)
        decrypted_data = cipher.decrypt(ciphertext)
        return decrypted_data.rstrip(b"\0")
    # Перевірка цілісності даних
    def verify_integrity(data):
```

```
        hash_obj = SHA256.new(data)
        return hash_obj.hexdigest()
    # Тестування продуктивності
    start_time = time.time()
    ciphertext = encrypt_data(data, key, iv)
    encryption_time = time.time() - start_time
    start_time = time.time()
    decrypted_data = decrypt_data(ciphertext, key, iv)
    decryption_time = time.time() - start_time
    # Перевірка цілісності
    original_hash = verify_integrity(data)
    decrypted_hash = verify_integrity(decrypted_data)
    # Виведення результатів
    print(f"Оригінальні дані: {data.decode()}")
    print(f"Зашифровані дані: {ciphertext.hex()}")
    print(f"Розшифровані дані: {decrypted_data.decode()}")
    print(f"Час шифрування: {encryption_time:.6f} сек")
    print(f"Час розшифрування: {decryption_time:.6f} сек")
    print(f"Цілісність збережена: {original_hash ==
decrypted_hash}")
```

Цей код імітує шифрування телеметричних даних, їхню передачу та перевірку цілісності, вимірюючи час виконання операцій. Результати дозволяють оцінити швидкість криптографічного шару моделі та його вплив на продуктивність системи, що є важливим для БПЛА з обмеженими ресурсами.

Тестування аутентифікаційного шару передбачає моделювання обміну цифровими сертифікатами та токенами OAuth 2.0 між БПЛА та наземною станцією. Для цього створюються тестові сценарії, що включають легітимні підключення та спроби несанкціонованого доступу. Програмне забезпечення, таке як OpenSSL, використовується для генерації сертифікатів і перевірки їхньої валідності, тоді як бібліотеки для OAuth (наприклад, python-oauth2) дозволяють імітувати видачу токенів. Основним показником ефективності є час, необхідний для завершення аутентифікації, і кількість помилкових відмов у доступі, що свідчить про точність системи.

Для оцінки шару моніторингу та реагування (IDPS) проводяться тести на основі симуляції атак, таких як спуфінг GPS-сигналів або DDoS. Використовується програмне забезпечення для аналізу мережі, наприклад, Wireshark, для збору даних про трафік, а алгоритми машинного навчання, реалізовані через бібліотеки

TensorFlow або Scikit-learn, застосовуються для виявлення аномалій. Тестові сценарії включають введення підозрілих пакетів даних і оцінку реакції системи, наприклад, ізоляцію каналу чи переключення частоти. Ключовими метриками є відсоток виявлених атак і час реакції, які вказують на здатність системи протидіяти загрозам у реальному часі.

Аналіз енергоефективності проводиться шляхом вимірювання споживання ресурсів під час виконання криптографічних операцій, аутентифікації та моніторингу. Для цього використовуються апаратні симулятори, які імітують бортові системи БПЛА, дозволяючи оцінити вплив запропонованих рішень на час автономної роботи апарата. Наприклад, виконання AES-256 на легковагових процесорах показує мінімальне енергоспоживання, тоді як асиметричні алгоритми, такі як ECC, потребують оптимізації для зниження навантаження.

Тестування в наближених до реальних умовах включає польові випробування, де БПЛА працює в урбанізованих зонах із високим рівнем перешкод або в віддалених районах із нестабільним зв’язком. У таких умовах оцінюється стійкість каналу до багатопроменевого поширення сигналу та здатність адаптивних механізмів, таких як FHSS, підтримувати зв’язок. Результати польових тестів порівнюються з лабораторними, щоб визначити розбіжності та вдосконалити модель.

Аналіз ефективності також враховує масштабованість моделі в сітчастих мережах, де кілька БПЛА взаємодіють як вузли ретрансляції. Тестові сценарії моделюють координацію аутентифікації та обмін даними про загрози між апаратами, оцінюючи затримки та пропускну здатність мережі. Це дозволяє визначити, наскільки модель придатна для складних багатоешелонних систем.

Результати тестування демонструють, що запропонована модель забезпечує високий рівень безпеки завдяки комбінації швидких криптографічних алгоритмів, надійної аутентифікації та адаптивного моніторингу. Однак виявлені обмеження, такі як підвищене енергоспоживання при використанні складних алгоритмів ШІ, вказують на необхідність подальшої оптимізації. Аналіз ефективності підтверджує, що модель є практичною для використання в реальних умовах, але вимагає

адаптації до специфічних сценаріїв, таких як тривалі місії чи операції в зонах із високим рівнем кіберзагроз. Постійне вдосконалення на основі тестових даних забезпечує стійкість моделі до нових викликів у сфері безпеки БПЛА.

3.3 Рекомендації щодо впровадження системи захисту в реальних умовах

Впровадження системи захисту каналів зв’язку безпілотних літальних апаратів у реальних умовах вимагає врахування специфіки експлуатації, обмежених ресурсів апаратних платформ і динамічного характеру кіберзагроз. Запропонована модель захищеного каналу зв’язку, що включає криптографічні методи, протоколи аутентифікації та системи виявлення вторгнень, потребує практичних рекомендацій для забезпечення її ефективності, адаптивності та сумісності з реальними операційними середовищами. Ці рекомендації спрямовані на оптимізацію безпеки, зниження енергоспоживання та забезпечення масштабованості системи.

Перш за все, необхідно адаптувати криптографічні алгоритми до апаратних обмежень БПЛА. Використання легковагових алгоритмів, таких як AES-128 замість AES-256 у сценаріях із менш критичними даними, дозволяє зменшити обчислювальне навантаження. Для асиметричної криптографії варто віддати перевагу elliptic curve cryptography через її енергоефективність порівняно з RSA. Регулярне оновлення ключів через протоколи, такі як Diffie-Hellman, має бути автоматизованим, щоб мінімізувати ризик компрометації без додаткового втручання оператора.

Для аутентифікації рекомендується впроваджувати багаторівневі протоколи, що поєднують цифрові сертифікати та токени OAuth 2.0, з підтримкою апаратних модулів безпеки для зберігання ключів. У реальних умовах, де зв’язок може бути нестабільним, доцільно використовувати легковагові протоколи, такі як Datagram Transport Layer Security, які оптимізовані для ненадійних мереж. Кешування токенів аутентифікації на борту БПЛА дозволяє уникнути повторних перевірок при короткочасних втратах зв’язку.

Системи виявлення та запобігання вторгненням слід налаштувати на гібридний підхід, поєднуючи сигнатурний і аномальний аналіз. Інтеграція штучного інтелекту для обробки аномалій має бути оптимізована шляхом виконання складних обчислень на наземних серверах, тоді як бортова система обробляє лише попередній аналіз. У зонах із високим рівнем перешкод рекомендується активувати адаптивне управління частотою для протидії глушінню, з автоматичним перемиканням на резервні канали.

Щоб забезпечити масштабованість у сітчастих мережах, необхідно впроваджувати децентралізовані протоколи обміну даними про загрози, які дозволяють БПЛА координувати дії без центрального сервера. Використання стандартів, таких як NIST SP 800-94 для IDPS і ISO/IEC 27001 для управління безпекою, гарантує сумісність із глобальними системами управління повітряним рухом.

Для практичного впровадження рекомендується проводити регулярне тестування системи в реальних умовах, включаючи урбанізовані зони та віддалені райони, щоб оцінити її стійкість до зовнішніх факторів, таких як багатопроменеве поширення сигналу чи погодні умови. Оновлення програмного забезпечення та криптографічних ключів має здійснюватися дистанційно через захищені канали, щоб мінімізувати потребу в фізичному доступі до апарата.

Нижче наведено приклад коду на Python для реалізації спрощеного механізму перевірки аутентифікації з використанням DTLS, який може бути адаптований для бортових систем БПЛА. Код демонструє встановлення захищеного з’єднання з перевіркою цифрового сертифіката.

```
from dtls import do_patch, DtlsSocket
import ssl
do_patch()
# Налаштування сертифікатів
cert_path = "uav_cert.pem"
key_path = "uav_key.pem"
ca_cert_path = "ca_cert.pem"
# Конфігурація DTLS
context = ssl.SSLContext(ssl.PROTOCOL_DTLS)
```

```
    context.load_cert_chain(certfile=cert_path,
keyfile=key_path)
    context.load_verify_locations(ca_cert_path)
    context.verify_mode = ssl.CERT_REQUIRED
    # Створення DTLS-сокета
    sock = DtlsSocket(context)
    sock.bind(("0.0.0.0", 12345))

    # Очікування підключення
    print("Очікування підключення...")
    sock.listen()
    client_sock, addr = sock.accept()
    # Перевірка аутентифікації
    try:
        client_sock.do_handshake()
        print(f"Підключено    до    {addr},    сертифікат
перевірено")
        data = client_sock.recv(1024)
        print(f"Отримано дані: {data.decode()}")
    except ssl.SSLError as e:
        print(f"Помилка аутентифікації: {e}")
    # Закриття з'єднання
    client_sock.close()
    sock.close()
```

Цей код ілюструє базову перевірку аутентифікації через DTLS, яка може бути інтегрована в систему зв'язку БПЛА для захисту від несанкціонованого доступу. Він вимагає попередньо створених сертифікатів, що відповідає реальним умовам впровадження.

Для забезпечення довгострокової безпеки рекомендується готуватися до квантових загроз шляхом поступового впровадження постквантових алгоритмів, таких як lattice-based cryptography, у стратегічно важливих системах. Крім того, навчання операторів і розробка чітких процедур реагування на інциденти підвищують загальну ефективність системи захисту.

У реальних умовах впровадження системи захисту каналів зв'язку БПЛА вимагає гнучкості, оптимізації ресурсів і постійного вдосконалення. Адаптація до специфічних сценаріїв, використання стандартизованих протоколів і регулярне тестування дозволяють створити надійну та стійку систему, здатну протистояти

сучасним і майбутнім кіберзагрозам, забезпечуючи безпеку критичних операцій БПЛА.

Третій розділ присвячений розробці, тестуванню та впровадженню системи захисту каналів зв’язку безпілотних літальних апаратів, що є ключовим для забезпечення їхньої безпеки та надійності в реальних умовах. Запропонована модель захищеного каналу зв’язку, яка інтегрує криптографічні методи, багаторівневу аутентифікацію та системи виявлення й запобігання вторгненням, формує багатошарову систему, здатну протидіяти сучасним кіберзагрозам, таким як перехоплення, спуфінг чи глушіння.

Тестування моделі через програмне моделювання та польові випробування підтвердило її ефективність, але виявило потребу в оптимізації енергоефективності для бортових систем із обмеженими ресурсами. Рекомендації щодо впровадження підкреслюють важливість використання легковагових протоколів, адаптивних механізмів, таких як FHSS, і стандартизації для забезпечення сумісності та масштабованості в сітчастих мережах. Інтеграція штучного інтелекту та підготовка до постквантових загроз відкривають перспективи для довгострокової безпеки. Загалом, розроблена система захисту, підкріплена ретельним тестуванням і практичними рекомендаціями, створює надійну основу для безпечного функціонування БПЛА в динамічних і вразливих умовах, вимагаючи при цьому постійного вдосконалення для адаптації до нових викликів у сфері кібербезпеки.

ВИСНОВКИ

Розробка та впровадження системи захисту каналів зв’язку безпілотних літальних апаратів є актуальним і складним завданням, що має вирішальне значення для забезпечення безпеки, надійності та ефективності цих систем у цивільних, промислових і військових сферах. Проведене дослідження охопило теоретичні основи, практичні аспекти та рекомендації щодо створення захищеного каналу зв’язку, враховуючи специфіку БПЛА, такі як динамічність операційного середовища, обмежені обчислювальні ресурси та високий рівень кіберзагроз.

У першому розділі розглянуто особливості функціонування каналів зв’язку БПЛА, які є основою для дистанційного керування, передачі телеметрії та обробки даних із сенсорів. Визначено ключові технічні характеристики, такі як вибір частотного діапазону, смуга пропускання та методи модуляції, а також вплив зовнішніх факторів, включаючи електромагнітні перешкоди, погодні умови та складний рельєф. Аналіз типів кіберзагроз, таких як перехоплення, спуфінг, глушіння, впровадження шкідливого ПЗ та атаки на наземні станції, підкреслив вразливість каналів зв’язку та необхідність багаторівневих механізмів захисту. Огляд сучасних методів захисту виявив ефективність комбінації криптографічних, мережевих і аналітичних підходів, включаючи асиметричне шифрування, адаптивне управління частотою та системи виявлення аномалій, що забезпечують баланс між безпекою та продуктивністю.

Другий розділ зосереджено на детальному аналізі ключових компонентів системи захисту. Криптографічні методи, що поєднують симетричне шифрування , асиметричне шифрування та хеш-функції, гарантують конфіденційність, цілісність і автентичність даних, враховуючи обмеження бортових систем. Протоколи аутентифікації та управління доступом, включаючи багаторівневу перевірку з використанням цифрових сертифікатів, токенів OAuth 2.0 і апаратних модулів безпеки, ефективно захищають від несанкціонованого доступу. Технології виявлення та запобігання вторгненням, інтегровані з штучним інтелектом, дозволяють оперативно реагувати на аномалії та складні атаки, адаптуючись до

нових загроз. Ці компоненти формують багатошарову систему захисту, яка є гнучкою та стійкою до сучасних кіберзагроз.

Третій розділ присвячено практичній реалізації системи захисту через розробку моделі захищеного каналу зв’язку, її тестування та рекомендації щодо впровадження. Модель інтегрує фізичний шар, шар захисту даних, шар аутентифікації і шар моніторингу, забезпечуючи комплексний захист. Тестування моделі через програмне моделювання та польові випробування підтвердило її здатність протидіяти загрозам, хоча виявило потребу в оптимізації енергоефективності для тривалих місій. Рекомендації щодо впровадження підкреслюють важливість використання легковагових протоколів, децентралізованих систем для сітчастих мереж, стандартизації та підготовки до постквантових загроз шляхом поступового впровадження нових алгоритмів.

Загалом, дослідження продемонструвало, що створення ефективної системи захисту каналів зв’язку БПЛА вимагає міждисциплінарного підходу, який поєднує передові технології, оптимізацію ресурсів і адаптацію до реальних умов. Розроблена модель забезпечує високий рівень безпеки, зберігаючи продуктивність і масштабованість, але потребує постійного вдосконалення для протидії новим кіберзагрозам, зокрема пов’язаним із квантовими обчисленнями. Впровадження запропонованих рішень сприятиме підвищенню надійності БПЛА, їхній інтеграції в глобальні системи управління та безпечному виконанню критичних завдань у складних і вразливих середовищах. Подальші дослідження можуть бути спрямовані на розробку ще більш енергоефективних алгоритмів, розширення можливостей ШІ для прогнозування загроз і вдосконалення стандартів для забезпечення глобальної інтероперабельності.

ПЕРЕЛІК ПОСИЛАНЬ

1. Li J., Dang S., Huang Y., Chen P., Qi X., Wen M., Arslan H. Composite multiple-mode orthogonal frequency division multiplexing with index modulation // *IEEE Transactions on Wireless Communications*. 2022. Vol. 22, No. 6. P. 3748–3761.
2. Sayed A. N., Ramahi O. M., Shaker G. UAV classification utilizing radar digital twins // *2023 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting (USNC-URSI)*, 2023, Portland, USA. Portland, 2023. P. 741–742.
3. Cecchinato N., Toma A., Drioli C., Oliva G., Sechi G., Foresti G. L. Secure real-time multimedia data transmission from low-cost UAVs with a lightweight AES encryption // *IEEE Communications Magazine*. 2023. Vol. 61, No. 5. P. 160–165.
4. Шалімова А. Підвищення ефективності сенсорних мереж на базі БПЛА для військових цілей // Вісник Хмельницького національного університету. *Технічні науки*. 2025. № 349(2). С. 261–265.
5. Rezwan S., Choi W. Artificial intelligence approaches for UAV navigation: recent advances and future challenges // *IEEE Access*. 2022. Vol. 10. P. 26320–26339. DOI: https://doi.org/10.1109/ACCESS.2022.3157626.
6. Землянко Г. А., Харченко В. С. Забезпечення кібербезпеки системи багатофункційних флотів БПЛА для моніторингу критичної інфраструктури: аналіз вразливостей, атак і контрзаходів // *Електронне моделювання*. 2024. Т. 46, № 1. С. 41–54.
7. Ceviz O., Sen S., Sadioglu P. A survey of security in UAVs and FANETs: issues, threats, analysis of attacks, and solutions // *IEEE Communications Surveys & Tutorials*. 2024. DOI: https://doi.org/10.1109/COMST.2024.3515051.
8. Tsao K. Y., Girdler T., Vassilakis V. G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks // *Ad Hoc Networks*. 2022. Vol. 133. DOI: https://doi.org/10.1016/j.adhoc.2022.102894.

9. Kurunathan H., Huang H., Li K., Ni W., Hossain E. Machine learning-aided operations and communications of unmanned aerial vehicles: a contemporary survey // *IEEE Communications Surveys & Tutorials*. 2023. Vol. 26, No. 1. P. 496–533.
10. Alsuhli G., Fahim A., Gadallah Y. A survey on the role of UAVs in the communication process: a technological perspective // *Computer Communications*. 2022. Vol. 194. P. 86–123.
11. Javaid S., Saeed N., Qadir Z., Fahim H., He B., Song H., Bilal M. Communication and control in collaborative UAVs: recent advances and future trends // *IEEE Transactions on Intelligent Transportation Systems*. 2023. Vol. 24, No. 6. P. 5719–5739.
12. Shoewu O. O., Akinyemi L. A., Edozie R. UAV cellular communication in 5G new radio wireless standards // Unmanned Aerial Vehicle Cellular Communications / ed. A. B. Sesay. *Cham : Springer International Publishing*, 2022. P. 25–45.
13. Лежньов Д., Рибаков К. Стійкість систем передачі керування БПЛА в умовах радіоелектронної боротьби: комбіновані рішення з автономної орієнтації та адаптивних антен // Вісник Хмельницького національного університету. *Технічні науки*. 2025. № 349(2). С. 221–229.
14. Dalal Y. M., Supreeth S., Amuthabala K., Satheesha T. Y., Asha P. N., Somanath S. Optimizing security: a comparative analysis of RSA, ECC, and DH algorithms // *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, 2024, Vijayapura, India. Vijayapura, 2024. P. 1–6.
15. Muhammed R. K., Rashid Z. N., Saydah S. J. A hybrid approach to cloud data security using ChaCha20 and ECDH for secure encryption and key exchange // *Kurdistan Journal of Applied Research*. 2025. Vol. 10, No. 1. P. 66–82.
16. Sabuwala N. A., Daruwala R. D. An approach to enhance the security of unmanned aerial vehicles (UAVs) // *The Journal of Supercomputing*. 2024. Vol. 80, No. 7. P. 9609–9639.
17. Ouadah M., Merazka F. Securing UAV communication: authentication and integrity // *2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2024, Beirut, Lebanon. Beirut, 2024. P. 1–7.

18. Baidya B., Mondal A. Quantum-resistant lattice-based cryptography for secure UAV communications // *International Conference on Smart Systems and Wireless Communication*, 2024, Singapore. Singapore : Springer Nature Singapore, 2024. P. 507–524.
19. Aissaoui R., Deneuville J. C., Guerber C., Pirovano A. A survey on cryptographic methods to secure communications for UAV traffic management // *Vehicular Communications.* 2023. Vol. 44. DOI: https://doi.org/10.1016/j.vehcom.2023.100661.
20. Wang J., Jiao Z., Chen J., Hou X., Yang T., Lan D. Blockchain-aided secure access control for UAV computing networks // *IEEE Transactions on Network Science and Engineering*. 2024. Vol. 11, No. 6. P. 5267–5279.
21. Jithu Vijay V. P., Thampi S. M. Navigating the skies: exploring dynamic access control in the Internet of Drones (IoD) // *Securing the Connected World: Exploring Emerging Threats and Innovative Solutions* / ed. S. M. Thampi. Cham : Springer Nature Switzerland, 2025. P. 345–380.
22. Hani O. D. H., Abdulhameed A. A. Secure communication frame for aerial networks // *Journal of Al-Qadisiyah for Computer Science and Mathematics*. 2024. Vol. 16, No. 4. P. 277–293.
23. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. *Офіційни сайт.* URL: https://www.iso.org/ru/standard/27001 (дата звернення: 24.03.2025).
24. NIST SP 800-63. Digital Identity Guidelines. *Офіційний сайт.* URL: https://pages.nist.gov/800-63-3/ (дата звернення: 24.03.2025).
25. Hadi H. J., Cao Y., Li S., Xu L., Hu Y., Li M. Real-time fusion multi-tier DNN-based collaborative IDPS with complementary features for secure UAV-enabled 6G networks // *Expert Systems with Applications*. 2024. Vol. 252. DOI: https://doi.org/10.1016/j.eswa.2024.124215.
26. Abu Al-Haija Q., Al Badawi A. High-performance intrusion detection system for networked UAVs via deep learning // *Neural Computing and Applications*. 2022. Vol. 34, No. 13. P. 10885–10900.

27. An D., Joo H., Kim H. Enabling low-latency digital twins for large-scale UAV networks using MQTT-based communication framework // *ICT Express*. 2025. Vol. 11, No. 2. P. 264–269.