COMPUTER SYSTEMS AND NETWORKS

Vol. 7, No. 1, 2025

DOI: https://doi.org/10.23939/csn2025.01.091

УДК 003.26:629.7.05

АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ТА ПРОТОКОЛІВ ДЛЯ ЗАХИСТУ БПЛА

А. Я. Горпенюк, Н. М. Лужецька, О. А. Горпенюк

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: andrii.y.horpeniuk@lpnu.ua, nataliia.m.luzhetska@lpnu.ua, oleksandr.horpeniuk.kb.2024@lpnu.ua

Досліджено особливості побудови і застосування криптографічних протоколів захисту безпілотних літальних апаратів (БПЛА) від кібератак.

Сьогодні ми є свідками унікального швидкого розвитку БПЛА військового призначення. Очевидно, такий розвиток БПЛА військового призначення зумовлений визначальним впливом характеристик бойових БПЛА і результатів їх (БПЛА) застосування (проаналізованих, задокументованих і усвідомлених) на результати реальних бойових дій.

Розглянуто основні типи спеціалізованих кібератак. Також проаналізовано вплив таких кібератак на ефективність роботи БПЛА, а також криптографічні методи, які можуть бути застосовані для забезпечення безпеки передавання даних, автентифікації, конфіденційності та цілісності інформації. Окремо розглянуто порівняння різних криптографічних протоколів, таких як TLS, IPsec, DTLS та інші, у контексті їх застосування для захисту каналів зв'язку БПЛА. У результаті виконаного аналізу розроблено базову і вдосконалену архітектуру системи захисту БПЛА на основі вибраних протоколів. Надано також рекомендації щодо впровадження цієї системи в реальних умовах. Проаналізовано перспективні шляхи удосконалення систем захисту БПЛА.

Ключові слова: БПЛА, криптографія, автентичність повідомлення, функція хешування.

Вступ

Розглянуто актуальне сьогодні питання застосування спеціалізованих криптографічних протоколів для підвищення стійкості БПЛА до кібератак. Безпілотні літальні апарати (БПЛА) посідають важливе місце у сучасних технологіях і використовуються в найрізноманітніших сферах: від військових операцій і гуманітарних місій до комерційного застосування у доставці товарів і виконанні дослідницьких завдань. БПЛА стали незамінними помічниками в багатьох галузях завдяки своїй мобільності, автономії та здатності працювати в умовах, де традиційні методи неможливі або неприйнятно дорогі. Проте зростаюча популярність цих апаратів спричиняє значне збільшення ризиків, пов'язаних із безпекою. БПЛА є потенційними цілями для різноманітних кібератак, що може мати серйозні наслідки як для самих апаратів, так і для тих, хто їх використовує. Тому важливим завданням є аналіз загроз, з якими стикаються ці технології, а також визначення найбільш ефективних способів їх захисту. Праця спрямована на аналіз основних вразливостей

БПЛА, а також на розгляд різних типів кібератак, які можуть бути спрямовані на ці системи. Враховуючи значну різноманітність сценаріїв використання БПЛА, необхідно ретельно дослідити вплив атак на роботу та безпеку цих апаратів, а також визначити основні інструменти та методики, які дають змогу забезпечити захист БПЛА.

Огляд літературних джерел

Безпілотні літальні апарати (БПЛА) класифікують за різними критеріями.

За призначенням [1, 2]:

· Військові БПЛА. Такі апарати використовуються для розвідки, збору інформації, спостереження за ворогом або навіть виконання бойових операцій, таких як нанесення ударів по цілях. Військові БПЛА повинні мати високий рівень захисту, зокрема системи радіоелектронної боротьби та механізми захисту від атак на сигнал.

· Цивільні БПЛА. Ці апарати зазвичай використовуються для мирних цілей, таких як зйомка відео, картографія, агрономія та інші. Вони можуть не мати таких високих вимог до захисту, однак їх використання в умовах, де існують можливі загрози (наприклад, в районах із значними радіоелектронними завадами), потребує специфічних заходів захисту.

· Комерційні БПЛА. Вони є найпоширенішими серед масових користувачів і використовуються для доставки товарів, моніторингу інфраструктури, інспекції будівель і навіть у сфері розваг. Такі дрони можуть бути оснащеними технологіями штучного інтелекту для автономних операцій, але також підлягають впливу зовнішніх загроз.

За розмірами та масою:

· Мікро-БПЛА. Мають масу до 250 грамів і використовуються для зйомки на близьких відстанях, моніторингу, а також для виконання коротких завдань. Їх конструкція компактна, а технічні характеристики дозволяють їм працювати навіть в обмежених просторах, наприклад між будівлями.

· Міні-БПЛА. Вага від 250 грамів до 2 кг. Ці дрони застосовуються для більш тривалих місій, таких як зйомка відео з висоти, моніторинг природи, інспекція будівель та інші. Вони можуть нести складне обладнання, наприклад тепловізори.

· Середні та великі БПЛА. Вага понад 2 кг. Середні та великі дрони використовують для довготривалих місій, таких як доставка товарів на великі відстані, перевезення важких вантажів, а також для розвідки, виконання аерофотозйомки або картографії.

За типом конструкції [1, 2]:

· Квадрокоптери. Найпоширеніший тип БПЛА, основою конструкції яких є чотири пропелери. Вони мають високу маневреність і стабільність у повітрі, що робить їх ідеальними для використання в містах та обмежених просторах.

· Гексакоптери та октокоптери. Мають шість або вісім пропелерів, що дає їм більшу потужність і стабільність. Вони зазвичай використовуються для виконання складних завдань, таких як транспортування важких вантажів або виконання розвідки на великих територіях.

· Крилькові БПЛА. Вони нагадують звичайні літаки і здатні долати великі відстані. Ці дрони зазвичай застосовуються для виконання тривалих місій, таких як моніторинг лісів, збір даних про стан навколишнього середовища або військова розвідка [1].

Основні компоненти БПЛА [1].

Безпілотні літальні апарати складаються з компонентів, які працюють в комплексі, забезпечуючи стабільність, ефективність і безпеку їх операцій:

· Механічні компоненти (пропелери та двигуни) є основними елементами, що відповідають за підйом і маневрування БПЛА. Вибір типу двигунів і пропелерів залежить від розміру та призначення дрона. Двигуни можуть бути електричними. Проте для важких апаратів використовуються двигуни внутрішнього згоряння.

· Рама та корпус. Рама утримує всі компоненти дрона. Вона має бути міцною і легкою, що дає змогу збільшити тривалість польоту.

· Електроніка і навігація (контролер польоту). Це “мозок” БПЛА, що відповідає за стабільність та контроль польоту. Він аналізує дані від сенсорів і виправляє будь-які відхилення в параметрах польоту.

· Система навігації. Містить GPS та інші датчики, які визначають місце розташування дрона в повітрі, допомагають йому орієнтуватися у просторі, а також виконувати автопілотні функції.

· Корисне навантаження (сенсори і камери). Дрони можуть бути оснащені камерами високої роздільної здатності, тепловізорами, сенсорами для вимірювання температури, вологості, рівня забруднення та іншими пристроями для збору даних в реальному часі. Це дозволяє БПЛА виконувати задачі, що потребують збору інформації з високою точністю.

· Система зв’язку. БПЛА використовують різноманітні способи зв’язку для обміну даними з пілотом або наземними станціями. Це можуть бути радіочастоти, стільникові мережі або супутникові канали для передачі даних на великі відстані.

Типи кібератак на БПЛА (табл. 1).

Існує низка кібератак на БПЛА, які можуть вплинути на їхню працездатність і безпеку [3].

· Перехоплення керування (Takeover Attack). Цей тип атаки полягає у віддаленому захопленні управління безпілотним літальним апаратом. Це дає змогу супернику перенаправити дрон в інше місце або змінити його параметри.

· Перехоплення даних (Data Interception). Цей вид атаки полягає в перехопленні даних, що передаються між БПЛА та його контролером або наземною станцією. Зловмисник може отримати доступ до важливої інформації, такої як відео- та знімки, координати, топографічні дані або інші чутливі відомості.

· Глушіння сигналу (Signal Jamming). Тут зловмисник знищує або знижує якість сигналу, що використовується для управління БПЛА або його навігаційної системи (наприклад, GPS). Глушіння може призвести до втрати контролю або збою у роботі системи.

· Спуфінг GPS (GPS Spoofing). Цей тип атаки полягає в підробці GPS сигналів, щоб змусити БПЛА вважати, що він знаходиться в іншому місці. Це може бути використано для того, щоб змінити траєкторію польоту або вивести апарат з визначеної зони.

· Атаки на програмне забезпечення (Software Vulnerabilities). Можуть передбачати експлуатацію вразливостей у прошивці або операційній системі БПЛА. Зловмисники можуть використовувати ці вразливості для модифікації або виведення апарата з ладу.

· Атаки на систему живлення (Power System Attack). Полягають у впливі на систему живлення БПЛА, наприклад, через її під’єднання до джерела енергії або зарядний пристрій. Зловмисники можуть скористатися цією вразливістю для витоку енергії, виключення БПЛА або порушення його роботи.

Таблиця 1

Типи кібератак на БПЛА

Тип атаки	Методи здійснення атаки	Наслідки	Рівень загрози
1	2	3	4
Перехоплення керування	Захоплення каналу зв’язку, вразливості в ПО	Втрата контролю, небажане переміщення	Високий
Перехоплення даних	Прослуховування каналів зв’язку, MITM атаки	Витік даних, порушення конфіденційності	Високий

Продовження табл. 1

1	2	3	4
Глушіння сигналу	Радіоелектронне глушіння, перешкода сигналів GPS	Втрата зв'язку, порушення маршруту	Середній
Спуфінг GPS	Підробка GPS-сигналів, маніпуляція координатами	Зміна траєкторії, втрата орієнтації	Високий
Атаки на програмне забезпечення	Використання вразливостей у програмному забезпеченні	Збої, модифікація програмного коду	Високий
Атаки на систему живлення	Пошкодження батарей або зарядних пристроїв	Втрата живлення, зупинка роботи	Середній

Вплив конструктивних особливостей БПЛА на можливості їх системи захисту.

Однією з головних проблем під час побудови системи захисту БПЛА є технічні обмеження самих апаратів. Зазвичай такі апарати мають обмежені ресурси (обчислювальні, пам'ять, енергозабезпечення тощо). Ці обмеження значно ускладнюють впровадження складних механізмів захисту, таких як високоякісне шифрування [5], багаторівнева автентифікація або системи виявлення аномалій у реальному часі. Як наслідок, на практиці доводиться вибирати між ефективністю системи захисту і ресурсозбереженням [3].

Вплив розвитку технологій радіоелектронної боротьби (РЕБ) на можливості системи захисту.

РЕБ містить різноманітні методи і засоби, що використовуються для перехоплення сигналів, глушіння зв'язку, а також для втручання в системи навігації, зокрема GPS. Спеціалізовані засоби глушіння сигналів можуть значно обмежити ефективність безпілотного апарата. В умовах наявності таких технологій навіть найсучасніші протоколи зв'язку часто не забезпечують повної безпеки [14].

Проблеми інтеграції з існуючими системами безпеки.

Інтеграція БПЛА в існуючі системи безпеки (як військові, так і цивільні) також викликає певні труднощі. Багато сучасних систем захисту базуються на усталених принципах, а технології безпілотних апаратів потребують специфічних і адаптованих рішень. Наприклад, інтеграція системи автентифікації та шифрування з різними платформами може потребувати оновлення або модифікації існуючих інфраструктур.

Відсутність стандартів і узгоджених підходів.

Ще однією відчутною проблемою є відсутність єдиних міжнародних стандартів безпеки БПЛА. Власники, розробники та оператори БПЛА стикаються з проблемами, пов'язаними з відсутністю чітких стандартів щодо того, як саме потрібно захищати ці апарати. Немає єдиних вимог до шифрування, автентифікації, протоколів безпеки, що ускладнює створення уніфікованих рішень, здатних працювати в різних країнах та на різних платформах. Водночас технології на ринку безпілотників розвиваються дуже швидко, і нові загрози виникають постійно. Тому стандартні рішення не завжди можуть бути ефективними, а існуючі нормативи часто не встигають врахувати нові види атак.

Використання штучного інтелекту (ШІ) для виявлення аномалій.

Зі зростанням кількості атак і дедалі більшими вимогами до безпеки починають використовуватися нові підходи до захисту БПЛА, зокрема за допомогою штучного інтелекту (ШІ). ШІ може бути використаний для виявлення аномалій у поведінці БПЛА в реальному часі, таких як незвичайні маневри, несанкціоновані зміни траєкторії чи спроби відключення систем зв'язку. Однак використання ШІ також створює додаткові труднощі, оскільки такі системи потребують значних обчислювальних ресурсів, що в умовах обмеженого обладнання БПЛА може стати серйозним бар'єром. Крім того, навчені моделі ШІ можуть бути вразливими до атак на саму систему навчання (наприклад, через маніпуляції з навчальними даними або вплив на архітектуру моделі).

Проаналізовані проблеми і виклики свідчать про те, що якісний захист БПЛА є складним завданням, що потребує поєднання багатьох різних технологій і підходів. Технічні обмеження, відсутність єдиних стандартів, а також швидкий розвиток нових методів атак ставлять під загрозу ефективність існуючих систем захисту. Однак із розвитком нових технологій, таких як штучний інтелект, а також із подальшим вдосконаленням шифрування та автентифікації, можна сподіватися на досягнення значних результатів у підвищенні рівня захисту БПЛА в майбутньому.

Постановка задачі

Завданнями роботи є дослідження основних криптографічних інструментів – криптографічних алгоритмів та протоколів – та особливостей їх застосування для захисту БПЛА. Розроблення базового та вдосконалених підходів до побудови системи захисту БПЛА на основі аналізу особливостей побудови та застосування криптографічних інструментів, а також спираючись на аналіз моделі загроз БПЛА. Розроблення рекомендацій з модифікації і впровадження систем захисту БПЛА та аналіз перспектив розвитку систем захисту БПЛА.

Порівняльний аналіз криптографічних протоколів, придатних для захисту БПЛА

Застосування сучасних криптографічних протоколів забезпечує високий рівень безпеки передачі даних, автентифікації користувачів і збереження конфіденційності інформації [4]. Для убезпечення безпілотних літальних апаратів використання таких протоколів є особливо важливим, оскільки забезпечує надійний захист каналів зв’язку, запобігає втручанню зловмисників і зберігає цілісність даних. Досліджено п’ять ключових криптографічних протоколів, які доцільно застосовувати для захисту БПЛА: TLS, DTLS, IPsec, VPN та QUIC.

TLS - це криптографічний протокол, який забезпечує захищений обмін даними через мережу [6, 7]. Він використовується для шифрування переданих даних, автентифікації сторін та запобігання перехопленню або модифікації інформації. Основні функції TLS:

· шифрування даних - гарантує, що навіть у разі перехоплення передана інформація залишатиметься недоступною для зловмисників;

· автентифікація сторін - використовує сертифікати для підтвердження автентичності сторін, які обмінюються інформацією;

· цілісність даних - за допомогою хеш-функцій (HMAC) перевіряється, чи були змінені дані під час передачі.

Особливості застосування протоколу TLS для захисту БПЛА:

Захист каналів зв’язку між оператором і БПЛА, які застосовуються для передачі команд управління, телеметрії та іншої важливої інформації. Використання TLS гарантує, що зв’язок є конфіденційним і захищеним від атак типу “людина посередині”. У такий спосіб забезпечується захист зв’язку між оператором і БПЛА у випадках, коли з’єднання здійснюється через стандартні TCP-протоколи (Wi-Fi, LTE, 5G).

Цей протокол може застосовуватися для тактичних, комерційних (невеликі апарати, які передають телеметрію або відеопотоки) та військових БПЛА. Загалом протокол TLS може використовуватися як проміжний рівень захисту в разі підключення до наземної станції [6].

DTLS - це модифікована версія TLS, адаптована для роботи з протоколом UDP (User Datagram Protocol). UDP використовується там, де важлива швидкість передачі, наприклад для потокового відео або телеметрії, що очевидно притаманне БПЛА.

Відмінності між протоколами TLS і DTLS.

Протоколи передачі даних. TLS працює з TCP, що забезпечує надійність, але з високою затримкою. Натомість DTLS працює з UDP, що дає змогу істотно знизити затримки.

Робота з втратами пакетів. На відміну від TLS, DTLS має спеціальні механізми для роботи з втратою пакетів. А це є дуже важливим у нестабільних мережах, якими, зокрема, є мережі зв'язку з БПЛА.

Роль DTLS у захисті БПЛА. Протокол DTLS застосовується для гарантування безпеки потокових даних, таких як відеопотоки з камер БПЛА, та захищає телеметричні дані в реальному часі. Також протокол, як і TLS, гарантує конфіденційність і автентичність інформації.

Отже, протокол DTLS доцільно застосовувати у розвідувальних (передача відеопотоків і оперативної інформації) та гібридних або ройових (де кожен апарат передає дані до центрального вузла у реальному часі) систем БПЛА [6].

IPsec (Internet Protocol Security) - це протокол захисту мережевого рівня, який використовується для шифрування та автентифікації IP-з'єднань [8, 9]. Цей протокол є важливим компонентом безпеки для мережевої інфраструктури, такої як передача даних від БПЛА.

Основні функції IPsec.

Шифрування даних – забезпечує конфіденційність переданої інформації.

Автентифікація – підтверджує, що обидві сторони з'єднання є тими, за кого себе видають, запобігаючи атакам типу "людина посередині".

Цілісність даних – тут використовується хеш-функція для перевірки того, чи не були дані змінені під час передачі.

Широкий рівень захисту – протокол діє на мережевому рівні (рівень IP), забезпечуючи універсальний захист усіх видів трафіку без необхідності зміни додатків або вищих рівнів протоколів.

Підтримка різних режимів роботи – транспортний режим захищає тільки дані в межах IP-пакета (наприклад, TCP чи UDP). Тунельний режим захищає весь IP-пакет, що дає змогу створювати VPN-з'єднання.

Застосування протоколу IPsec в БПЛА забезпечує захист комунікацій на мережевому рівні, що є дуже важливим для захисту від атак перехоплення та маніпуляції даними. Може використовуватися для захисту з'єднань між БПЛА, наземними станціями та хмарними сервісами. Підходить для військових БПЛА (захист критичних даних, таких як координати, маршрути або бойові завдання). Доцільне його застосування також у великомасштабних комерційних БПЛА. Наприклад, для доставки, де необхідна інтеграція з хмарними платформами.

VPN створює захищений канал для передачі даних через відкриті мережі. Це дає змогу віддалено керувати БПЛА в умовах потенційно небезпечних мереж.

Особливості VPN.

Забезпечує шифрування даних за допомогою протоколів IPsec або SSL/TLS.

Гарантує анонімність і захист від атак з боку третіх осіб.

Застосування VPN для БПЛА.

VPN використовується для захисту зв'язку між оператором і БПЛА під час віддаленого управління. При цьому умови нестабільного зв'язку компенсуються механізмами повторної передачі та шифрування. VPN доцільно застосовувати під час віддаленого керування через публічні мережі (наприклад, під час керування БПЛА з іншого регіону або країни) та забезпечення конфіденційності даних у ситуаціях, коли апарат під'єднується до загальнодоступної мережі. Підходить для комерційних БПЛА (наприклад, дрони для зйомки або моніторингу, які працюють через мобільні мережі).

QUIC (Quick UDP Internet Connections) - це новий транспортний протокол, розроблений як альтернатива TCP для поєднання низької затримки та високого рівня безпеки [10, 11].

Особливості QUIC.

Швидкодія. Протокол мінімізує затримку завдяки зменшенню кількості обмінів даними на етапі встановлення з'єднання.

Інтегроване шифрування. Шифрування є частиною базової специфікації QUIC, що підвищує загальну безпеку.

Стійкість до втрат пакетів. Протокол адаптований для роботи в умовах нестабільних мереж.

Використання QUIC у БПЛА.

QUIC підходить для передачі даних із низькою затримкою, таких як різноманітні команди або потокове відео. При цьому QUIC забезпечує високу швидкість та надійність навіть у мережах із високою затримкою або втратою пакетів, що є важливим саме для БПЛА.

Протокол забезпечує низьку затримку для швидкої передачі даних у реальному часі, роботу в середовищах із високим ризиком втрати пакетів (сільські райони, зони бойових дій, нестабільне покриття мережі) та додатковий захист у середовищах із низькою пропускною здатністю. Ідеально підходить для високошвидкісних розвідувальних або рятувальних БПЛА, де потрібна миттєва передача зображень і даних, а також для компактних або мікро-БПЛА з обмеженими ресурсами та необхідністю легкої інтеграції в мережі [10].

Розроблення на основі криптографічних алгоритмів та протоколів базових і вдосконалених підходів до побудови системи захисту БПЛА

Як було підсумовано вище, безпілотні літальні апарати (БПЛА) є яскравим прикладом сучасних прогресивних технологій. Сьогодні вони активно застосовуються у військових, комерційних і цивільних цілях. Але разом із розвитком сфер застосування та можливостей БПЛА зростає також і діапазон загроз, які можуть впливати на безпеку подібних пристроїв. Розробка ефективної системи захисту БПЛА потребує чіткого розуміння ризиків, з якими можуть зіткнутися БПЛА, і способів їх ліквідації або мінімізації. Отже, модель загроз виконує ключову роль у визначенні вразливих місць і формуванні основних вимог до систем захисту.

Виконаний аналіз загроз для БПЛА дав змогу класифікувати ці загрози за кількома основними категоріями (табл. 2). Ці категорій охоплюють як кібернетичні, так і фізичні аспекти атак. Визначені та сформульовані в табл. 2 загрози суттєво впливають на конфіденційність, цілісність і доступність даних, а також на безпечну експлуатацію БПЛА.

Таблиця 2

Модель загроз

Категорія загроз	Тип загрози	Опис	Можливий вплив
1	2	3	4
Атаки на конфіденційність	Перехоплення даних	Отримання зловмисником телеметрії, відео чи навігаційної інформації	Компрометація даних, витік конфіденційної інформації
	Витік команд управління	Використання зловмисником перехоплених команд для контролю БПЛА	Втрата конфіденційності управління, ризик несанкціонованих дій
Атаки на цілісність	Зміна команд або даних	Модифікація команд або передачі телеметрії	Некоректна робота БПЛА, виконання небажаних дій
	Ін’єкція шкідливих пакетів	Додавання підроблених даних до потоку, що передається між оператором і БПЛА	Збої в роботі системи управління
Атаки на доступність	Глушіння радіосигналу	Блокування зв’язку між оператором і БПЛА	Втрата управління, зупинка виконання місії
	DoS-атаки	Перевантаження каналів зв’язку або ресурсів БПЛА	Зниження продуктивності, недоступність системи

Продовження табл. 2

1	2	3	4
Атаки на автентичність	Фальшиві ідентифікатори	Використання зловмисником фальшивих даних для видачі себе за оператора	Неавторизований доступ до управління БПЛА
	Підробка аутентифікаційних даних	Перехоплення та використання автентифікаційної інформації	Компрометація системи захисту, несанкціонований контроль
Фізичні загрози	Використання пристроїв для перехоплення або ураження	Зовнішнє втручання за допомогою ЕМР або лазерних пристроїв	Знищення БПЛА або його апаратних компонентів
	Ураження фізичними об’єктами	Використання спеціалізованих технологій для зупинки чи пошкодження дрона	Повна або часткова втрата БПЛА

Подальше розроблення архітектури системи захисту для БПЛА на базі проаналізованої моделі загроз є визначальним кроком для забезпечення конфіденційності, автентичності, цілісності та доступності даних під час зв’язку між БПЛА та наземною станцією управління. Основою розроблення такої системи захисту є застосування різних криптографічних методів і протоколів, призначених для шифрування, автентифікації та захисту каналів зв’язку.

Загалом система захисту має реалізовувати:

· шифрування даних – для забезпечення конфіденційності переданих команд і отриманих даних;

· автентифікацію – для перевірки автентичності учасників зв’язку;

· захист каналу зв’язку – для запобігання перехопленню або модифікації переданих даних.

Для забезпечення перелічених властивостей застосовуються різні криптографічні методи і протоколи. Серед них виділимо як пріоритетні для побудови системи захисту БПЛА стандартний алгоритм шифрування AES, протоколи TLS/DTLS, а також алгоритм цифрового підпису RSA. Під час цього дослідження висвітлено практичні реалізації цих алгоритмів та протоколів, аналіз результатів яких визначили рекомендації до застосування та варіантів впровадження, сформульовані у цій статті.

Проаналізуємо тут призначення і основну мету застосування згаданих криптографічних алгоритмів та протоколів у системах захисту БПЛА.

AES (Advanced Encryption Standard) - це стандартний (США) алгоритм симетричного шифрування, який дає змогу забезпечити високу безпеку для захисту команд і даних, що передаються між БПЛА та наземною станцією.

Стандарт AES визначає низку режимів застосування цього алгоритму, серед яких особливо потрібно виділити режим CFB (Cipher Feedback Mode – Режим зворотного зв’язку за шифротекстом). У режимі CFB кожен блок зашифрованих даних впливає на наступний, забезпечуючи у такий спосіб більшу стійкість до атак. Він підходить для потокового шифрування, оскільки не потребує повних блоків.

Роль алгоритму AES у системі захисту БПЛА така: AES шифрує команди оператора і дані, отримані від сенсорів дрона, що забезпечує їх конфіденційність під час передачі через відкриті канали зв’язку.

Протокол захисту каналів зв'язку TLS (Transport Layer Security) широко застосовується для забезпечення безпечного зв'язку між клієнтами та серверами. Цей протокол дає змогу захистити канали зв'язку, гарантувати конфіденційність і цілісність переданих даних, а також забезпечити автентифікацію сторін.

Цифрові підписи, створені за допомогою асиметричного алгоритму RSA, використовуються для автентифікації учасників зв'язку, у нашому випадку - оператора та власне БПЛА. RSA забезпечує автентифікацію, дозволяючи перевіряти, що команда або дані надійшли від авторизованого оператора або авторизованого безпілотного апарата.

Отже, основою створення базової комплексної системи захисту БПЛА є застосування і поєднання розглянутих криптографічних алгоритмів та протоколів:

- алгоритм AES забезпечує шифрування команд і даних для забезпечення конфіденційності;
- протокол TLS використовується для захисту каналу зв'язку між БПЛА і наземною станцією, щоб запобігти перехопленню даних;
- алгоритм RSA в режимі цифрового підпису забезпечує автентифікацію. Це гарантує, що лише авторизовані користувачі можуть управляти БПЛА або отримувати дані.

Така базова архітектура забезпечує повний захист БПЛА від кіберзагроз, таких як несанкціонований доступ, маніпулювання даними та атаки на канали зв'язку.

Це основні принципи проєктування архітектури безпеки на основі обраних криптографічних протоколів. Інтегрувавши ці методи в систему захисту, забезпечимо надійний захист БПЛА, що дозволить їм ефективно діяти в умовах кіберзагроз.

Інтегральний аналіз проаналізованих основних принципів проєктування архітектури безпеки БПЛА, а також особливостей ресурсної обмеженості БПЛА дає змогу зробити такі висновки. У сучасних БПЛА основними проблемами є обмежені обчислювальні ресурси та високі вимоги до енергоефективності таких пристроїв. Враховуючи ці фактори, доцільно за можливості, з метою удосконалення системи захисту БПЛА, застосовувати (за умови допустимого зменшення надійності) полегшені (обчислювально простіші) криптографічні алгоритми і протоколи [16, 17], які дозволяють зменшити обчислювальне навантаження на БПЛА, а також споживання енергії при збереженні прийнятного рівня безпеки.

Отже, основна мета вдосконалення архітектури системи захисту сучасних БПЛА – інтеграція легковагових криптографічних алгоритмів та протоколів для підвищення ефективності (як з погляду швидкодії, так і з погляду споживаної енергії) без критичного зниження надійності системи захисту. Суть згаданого удосконалення передбачає такі ключові зміни на трьох основних етапах забезпечення надійності:

1. Шифрування: замість використання стандартних обчислювально складних алгоритмів шифрування (таких як AES), в архітектуру додаються легковагові шифри, для прикладу PRESENT чи LEA, які власне і призначені та оптимізовані для пристроїв з обмеженими обчислювальними ресурсами.

PRESENT - це ефективний алгоритм блокового симетричного шифрування, який дає змогу підтримувати безпеку з мінімальним споживанням ресурсів. Цей алгоритм використовує менше пам'яті та енергії порівняно з більш дорогими алгоритмами, такими як AES.

2. Протоколи аутентифікації: для забезпечення аутентифікації використовується легковагова версія протоколів аутентифікації, наприклад такі як ECDSA. Подібні протоколи істотно знижують обчислювальне навантаження на систему захисту без значного зниження рівня безпеки.

ECDSA (Elliptic Curve Digital Signature Algorithm) менш вимогливі до ресурсів, порівняно з RSA, проте зберігають високу надійність. Можливе також застосування алгоритму SECP256R1, який оптимізований для використання на пристроях з обмеженими ресурсами [15].

3. Передача даних: для передачі даних між БПЛА та базовою станцією використовуються оптимізовані версії протоколів, таких як TLS або DTLS, які сумісні та інтегруються із згаданими легковаговими шифрувальними алгоритмами.

Отже, удосконалення архітектури системи захисту БПЛА з урахуванням спрощених легковагових криптографічних алгоритмів і протоколів передбачає заміну стандартних компонентів системи на оптимізовані легковагові версії, які працюють з обмеженими ресурсами, забезпечуючи високу безпеку.

Аналізуючи переваги застосування легковагових криптографічних алгоритмів і протоколів, робимо такі висновки. Насамперед застосування легковагових криптографічних алгоритмів і протоколів дає змогу зменшити енергоспоживання. Легковагові алгоритми і протоколи споживають менше енергії, що важливо для продовження роботи БПЛА протягом тривалого часу. Крім того, оскільки легковагові шифри займають менше пам'яті та процесорного часу, БПЛА зможе обробляти більше даних за менший час. Нарешті, такі алгоритми і протоколи мають істотну перевагу з точки зору масштабованості. Легковагові алгоритми і протоколи дозволяють забезпечити безпеку на великій кількості пристроїв, що необхідно для масового застосування БПЛА у різних сферах.

Модифікація архітектури захисту з урахуванням легковагових протоколів передбачає заміну стандартних компонентів системи на оптимізовані версії, що працюють з обмеженими ресурсами, забезпечуючи високу безпеку.

Підсумуємо основні відмінності у застосуванні криптографічних алгоритмів та протоколів в класичних та вдосконалених архітектурах систем захисту БПЛА.

Класична архітектура системи захисту БПЛА:

- Шифрування даних: алгоритм AES;
- Протоколи аутентифікації: на базі алгоритму RSA;
- Передача даних: TLS/DTLS.

Удосконалена архітектура з легковаговими протоколами:

- Шифрування даних: PRESENT, LEA;
- Протоколи аутентифікації: алгоритм ECDSA;
- Передача даних: Легковаговий TLS/DTLS .

Дані, узагальнені в табл. 3 та 4 демонструють ключові відмінності між двома дослідженими архітектурами системи захисту БПЛА. У табл. 3 відображено відмінності між засобами забезпечення ключових компонентів систем захисту цих двох архітектур. У табл. 4 подано результати порівняльного аналізу основних характеристик систем захисту БПЛА, що належать до двох досліджених архітектур. Аналіз даних, наведених в табл. 4, показує, що використання легковагових криптографічних алгоритмів і протоколів дає змогу значно зменшити енергоспоживання та обчислювальне навантаження на систему захисту, що робить їх ідеальними для застосування в системах з обмеженими ресурсами, до яких належать, зокрема, і БПЛА.

Таблиця 3

Засоби побудови систем захисту двох базових архітектур БПЛА

Компонент системи захисту	Без легковагових протоколів	З легковаговими протоколами
Шифрування даних	AES (Advanced Encryption Standard)	PRESENT, LEA (легковагові шифри для обмежених ресурсів)
Протоколи аутентифікації	RSA, ECDSA (для забезпечення автентичності)	ECDSA (підвищена ефективність з малими ресурсами)
Передача даних	TLS (Transport Layer Security), DTLS (Datagram TLS)	Легковаговий TLS/DTLS (оптимізовані для меншої обчислювальної потужності)

Таблиця 4

Порівняльний аналіз основних характеристик систем захисту БПЛА

Характеристика системи захисту	Без легковагових протоколів	З легковаговими протоколами
Енергоспоживання	Високе через використання важких алгоритмів шифрування	Знижене енергоспоживання завдяки використанню легковагових шифрів
Обчислювальне навантаження	Високе через потребу в значних ресурсах для виконання складних алгоритмів	Знижене обчислювальне навантаження, оптимізовано для БПЛА з обмеженими ресурсами
Швидкість роботи	Повільніше через високі вимоги до ресурсів	Швидше завдяки оптимізації криптографічних операцій для обмежених пристроїв
Масштабованість	Залишається високим, але з обмеженням ресурсів на великій кількості пристроїв	Краще масштабування, оскільки легковагові протоколи спрощують інтеграцію в більшу кількість БПЛА

Розроблення рекомендацій з модифікації і впровадження систем захисту БПЛА та аналіз перспектив розвитку систем захисту БПЛА

Окрім аналізу сучасних криптографічних протоколів і їхніх можливостей для забезпечення безпеки безпілотних літальних апаратів (БПЛА), важливо також сформувати рекомендації щодо особливостей модифікації і впровадження цих систем у реальних умовах застосування. Існують різноманітні умови і сценарії застосування БПЛА. Тому під час розроблення ефективної системи захисту необхідно враховувати такі аспекти, як робоче середовище, вимоги до різного типу ресурсів, необхідних для впровадження, вимоги до адаптованості та масштабованості системи, а також необхідність регулярних оновлень для протидії новим загрозам.

Важливим етапом у розробці системи захисту є врахування специфіки середовища, в якому БПЛА будуть виконувати свої завдання. Це дає змогу точно налаштувати архітектуру захисту відповідно до вимог та умов експлуатації. У табл. 5 подано результати аналізу особливостей експлуатації БПЛА різного призначення, а також сформульовано основні вимоги до системи захисту таких БПЛА.

Таблиця 5

Аналіз вимог до системи захисту залежно від особливостей експлуатації БПЛА

Категорія БПЛА	Основні вимоги до системи захисту	Особливості експлуатації
Військові	- захист від складних атак на всіх етапах польоту; - висока автономність системи; - захист від фізичного втручання	Використовуються у складних умовах бойових дій, де потрібно забезпечити високу стійкість до кібернападів
Цивільні	- легкість інтеграції з іншими системами; - захист відеопотоків і передачі персональних даних; - сумісність із стандартами	Підходять для рятувальних місій, моніторингу та інших цивільних завдань, які потребують, зокрема, надійного захисту даних
Комерційні	- масштабованість для обробки даних від великої кількості дронів; - мінімізація витрат енергії; - можливість керування парком дронів через одну платформу	Орієнтовані на комерційні операції, наприклад доставку товарів, моніторинг територій, де передусім важлива ефективність

Для впровадження системи безпеки БПЛА необхідно також оцінити ресурси, які будуть необхідні для її впровадження. Ці ресурси, зокрема, містять апаратне забезпечення для виконання складних криптографічних операцій і програмне забезпечення для керування безпекою. У табл. 6 розглянуто приклади апаратних і програмних компонентів системи захисту БПЛА і їх роль у забезпеченні захисту.

Таблиця 6

Роль у захисті апаратних і програмних компонентів системи захисту БПЛА

Тип ресурсу	Приклади	Роль у захисті
Апаратні компоненти	- процесори з апаратним шифруванням (наприклад, ARM з підтримкою AES-NI); - захищені сховища ключів (HSM)	Прискорюють обчислення, забезпечують надійне зберігання ключів і даних для шифрування
Програмні компоненти	- Підтримка протоколів TLS/DTLS для шифрування передачі даних; - інтеграція VPN для захисту каналу зв'язку	Забезпечують захист переданих даних, автентифікацію учасників зв'язку, створюють безпечне середовище для обміну даними

Важливим аспектом впровадження системи захисту є здатність системи ефективно масштабуватися для роботи з великою кількістю БПЛА, що можуть бути частинами однієї операційної мережі. Зважаючи на це, важливо впроваджувати рішення, які дають змогу легко інтегрувати нові блоки дронів у загальну систему. При цьому базовими принципами для ефективного масштабування системи є:

· динамічне управління ключами. Система має підтримувати ефективний обмін ключами, використовуючи протоколи, такі як DTLS, для захисту передачі даних між БПЛА та наземними станціями управління;

· централізоване управління. Використання централізованих серверів або хмарних платформ для зберігання даних та моніторингу безпеки всіх підключених БПЛА;

· інтеграція IoT. Застосування IoT-рішень для забезпечення взаємодії між безпілотниками та іншими пристроями в екосистемі.

Захисні системи мають забезпечувати властивість адаптованості до нових кіберзагроз, що будуть з'являтися з часом. Отже, регулярне оновлення програмного забезпечення та криптографічних протоколів є необхідним для забезпечення високого рівня безпеки (табл. 7).

Таблиця 7

Аналіз впливу оновлень компонентів на ефективність захисту БПЛА

Частина системи захисту	Необхідні оновлення	Переваги від оновлення
Програмне забезпечення	- оновлення бібліотек шифрування (наприклад, OpenSSL); - Впровадження нових алгоритмів та протоколів захисту, наприклад постквантової криптографії	Підвищення стійкості до нових типів атак, зокрема MITM та DoS, квантове розкриття, тощо
Апаратні компоненти	- підвищення рівня безпеки на рівні чіпів (наприклад, HSM або TPM)	Забезпечення надійності шифрування та захисту від атак на фізичному рівні

Для підтримки високої стійкості БПЛА до нових загроз у майбутньому важливо інтегрувати захисні системи з новітніми технологіями, такими як штучний інтелект, квантові канали зв'язку, постквантова криптографія та IoT.

Штучний інтелект. Використання AI для виявлення аномалій у телеметрії та автоматичного реагування на загрози в режимі реального часу.

Квантові канали зв'язку. Забезпечать в майбутньому надійну і гарантовано убезпечену від зовнішнього втручання передачу ключів та іншої конфіденційної інформації.

Постквантова криптографія. Застосування постквантових криптоалгоритмів, які зараз активно розробляються і стандартизуються, дозволить уникнути загрози квантового розкриття існуючих криптоалгоритмів в умовах впровадження ефективних квантових обчислювальних систем.

IoT та 5G. Інтеграція дронів в екосистеми IoT для збирання даних з різних сенсорів та управління парками безпілотників за допомогою 5G для високошвидкісних і безпечних зв'язків.

Результати дослідження

За результатами виконаного дослідження визначено основні етапи та особливості проєктування та аналізу системи захисту для безпілотних літальних апаратів (БПЛА). Розроблено модель загроз для БПЛА, визначено основні етапи проєктування архітектури захисту БПЛА із застосуванням сучасних криптографічних протоколів. Досліджено способи модифікації архітектури захисту із застосуванням легковагових криптографічних протоколів.

Аналіз моделі загроз для БПЛА дав змогу виявити основні вразливості та потенційні загрози, які можуть виникнути під час роботи таких пристроїв. Модель загроз є важливим елементом для визначення необхідного переліку елементів захисту. Така модель допомагає визначити, які алгоритми, методи, протоколи та механізми потрібно використовувати для забезпечення необхідного рівня захисту.

У процесі проєктування архітектури захисту БПЛА досліджено інтеграцію протоколів TLS/DTLS та алгоритмів шифрування RSA та AES, які забезпечують надійний захист даних, автентифікацію та зв'язок між БПЛА та базовими станціями. Водночас, зважаючи на обмежені ресурси БПЛА, було запропоновано доповнити цю архітектуру полегшеними криптографічними протоколами, такими як PRESENT і LEA. Такий підхід дає змогу кратно зменшити вимоги до обчислювальних та енергетичних ресурсів БПЛА і так адаптувати захист до умов, коли важливо забезпечити високу ефективність та надійність за жорстких обмежень на доступні ресурси.

За результатами проведених досліджень визначено також рекомендації щодо можливих і доцільних модифікацій, а також щодо особливостей впровадження системи захисту БПЛА в реальних умовах. Ці рекомендації, зокрема, передбачають: врахування призначення, умов і особливостей практичного застосування БПЛА; врахування вимог до апаратних та програмних ресурсів; врахування можливостей масштабування системи захисту за великої кількості одночасно працюючих БПЛА, а також можливостей швидкого і ефективного адаптування до змінних умов застосування.

Крім того, визначено також важливість регулярного оновлення системи захисту для протидії новим типам кібератак, а також доцільність інтеграції новітніх технологій, таких як штучний інтелект, технології квантової передачі даних, постквантові криптоалгоритми, Інтернет речей, нові технології безпровідного зв'язку, для забезпечення гнучкості та швидкості реагування на нові загрози.

Висновки

Сьогодні ми є свідками бурхливого розвитку безпілотних літальних апаратів, що пов'язано з активним застосуванням цих апаратів у найрізноманітніших сферах. Сучасні БПЛА класифікують за призначенням та типом конструкції. Зазвичай, незалежно від призначення, більшість сучасних БПЛА потребують системи захисту певних даних від певних загроз. Водночас система захисту БПЛА різного призначення буде мати різну складність. Очевидно, що найскладнішими є вимоги до

систем захисту БПЛА військового призначення. Процес побудови системи захисту БПЛА спирається передусім на аналіз основних загроз та типів кібератак на БПЛА. Інакше кажучи, складають і аналізують модель загроз БПЛА. Проведений аналіз моделі загроз БПЛА показує, що основний вплив на можливості та ефективність системи безпеки БПЛА мають такі основні фактори. Конструктивні особливості БПЛА – зазвичай обмежують ресурси БПЛА (обчислювальні, енергетичні, ресурси пам'яті), обмежуючи так вибір розробника недорогими компонентами системи безпеки БПЛА. Активний розвиток технологій радіоелектронної боротьби (РЕБ) визначає необхідність врахування в реальному часі, адаптування системи безпеки і впровадження нових елементів протидії РЕБ. Проблеми інтеграції з існуючими системами безпеки: БПЛА є спеціалізованими комплексними апаратами з обмеженими ресурсами, які застосовуються часто в унікальних умовах за умови впливу найрізноманітніших, часто ворожих факторів. Тому системи безпеки таких апаратів часто є унікальними і їх складно інтегрувати в універсальні системи захисту інших об'єктів і систем. Відсутність стандартів та усталених підходів до побудови систем безпеки БПЛА – сучасні БПЛА загалом та їх системи безпеки зокрема настільки швидко прогресують, реагуючи на нові загрози та виклики, що об'єктивно не можуть відповідати неіснуючим стандартам, розробка і впровадження яких тільки планується.

На основі аналізу способів конструювання БПЛА, особливостей їх використання в різних сферах та вимог то систем захисту БПЛА різного призначення, аналізу моделі загроз БПЛА та основних видів кібератак та такі апарати, розроблено базову та вдосконалену архітектуру системи захисту БПЛА. Основою цих архітектур системи захисту БПЛА є застосування криптографічних алгоритмів та протоколів, особливості яких проаналізовано в цій статті. Водночас у вдосконалених архітектурах систем захисту БПЛА, орієнтованих на БПЛА з обмеженими ресурсами, рекомендовано застосовувати легковагові криптографічні інструменти для підтримання безпеки БПЛА.

На основі аналізу перспективних шляхів розвитку БПЛА, а також прогресуючих методів, засобів та інструментів деструктивного впливу на них, визначено перспективні шляхи розвитку систем захисту БПЛА, до яких передусім належить застосування штучного інтелекту для виявлення різних аномалій в поведінці БПЛА, а також застосування постквантових криптографічних алгоритмів та криптографічних протоколів на їх основі для уникнення загрози квантового розкриття.

Список літератури

1. *Основні властивості та моделі БПЛА: мультикоптери, FPV, крила. URL: https:// vseosvita.ua/ lesson/osnovni-vlastyvosti-ta-modeli-bpla-multykoptery-fpv-kryla-700086.html (дата звернення: 04.01.2025).*

2. *Іванченко О. В., Курдюк С. В., Хатунцев Ю. Ю., Рудніченко С. В. Аналіз можливостей застосування та класифікація безпілотних літальних апаратів для забезпечення бойових дій військово-морських сил збройних сил України. Збірник наукових праць ДНДІ ВС ОВТ. 2023. Вип. 4(18). С. 23- 34. DOI: https:// doi.org/10.37701/dndivsovt.18.2023.04.*

3. *A Step-by-Step Guide to Counter UAS (Unmanned Aerial Systems) Technologies. URL: https:// sentrycs.com/uk/the-counter-drone-blog/a-step-by-step-guide-to-counter-uas-unmanned-aerial-systems-technologies/ (дата звернення: 04.01.2025).*

4. *Аналіз безпеки криптографічних протоколів. URL: https://studfile.net/preview/6012701/page:45/ (дата звернення: 04.01.2025).*

5. *Gorpeniuk A. Fast algorithms and computing means of cryptological functions. International Scientific Journal of Computing. October 2005. Vol. 4. Issue 2. Pp. 69- 76. DOI: https://doi.org/10.47839/ijc.4.2.339.*

6. *TLS протокол: як він працює і від чого захищає. URL: https://cityhost.ua/uk/blog/scho-take-protokol-tls-yak-vin-pracyu-ta-vid-chogo-zahischa.html (дата звернення: 04.01.2025).*

7. *Бабенко Т., Толюпа С., Гречко В. Проблеми використання SSL/TLS. Захист інформації. жовтень-грудень 2017. Т. 19. № 4. С. 298- 302. DOI: https://doi.org/ 10.18372/2410-7840.19.12218.*

8. *Що таке протокол IPsec і навіщо він потрібен? URL: https://resit.com.ua/navisho-potriben-ipsec-protokol/ (дата звернення: 04.01.2025).*

9. *Паталашко П. Ю., Кушніренко Н. І. Автоматизація конфігурування безпечного під'єднання до корпоративних мереж. Інформатика та математичні методи в моделюванні. 2022. Т. 12. № 1- 2. С. 73- 83. DOI: https://doi.org/ 10.15276/imms.v12.no1-2.73.*

10. *QUIC Protocol. URL: https://www.pubnub.com/learn/glossary/quic-protocol/ (дата звернення: 04.01.2025).*

11. *Langley A., Riddoch A. et al. The QUIC Transport Protocol: Design and Internet-Scale Deployment. SIGCOMM '17. August 2017. 21- 25. Pp. 183- 196. DOI: https://doi.org/10.1145/3098822.3098842.*

12. *Horpenyuk A., Opirskyy I., Vorobets P. Analysis of problems and prospects of implementation of post-quantum cryptographic algorithms. CEUR Workshop Proceedings. 2023. Vol. 3504 : Workshop on classic, quantum, and post-quantum cryptography, CQPC'2023. Pp. 39–49.*

13. *Vorobets P., Vakhula O., Horpenuk A., Korshun N. Implementing post-quantum KEMs: practical challenges and solutions. CEUR Workshop Proceedings. 2024. Vol. 3826 : Proceedings of the workshop "Cybersecurity providing in information and telecommunication systems II". Kyiv, Ukraine, October 26, 2024 (online). Pp. 212–219.*

14. *Опірський Р., Бибик Р. Дослідження сучасних методів РЕБ та методів і засобів її протидії. Безпека інформації. 2023. Т. 29. № 2. С. 88- 97. DOI: 10.18372/2225-5036.29.17873.*

15. *Elliptic Curve Digital Signature Algorithm. URL: https://www.hypr.com/security-encyclopedia/elliptic-curve-digital-signature-algorithm (дата звернення: 04.01.2025).*

16. *Легковагова криптографія. URL: https://www.secure-ic.com/blog/lightweight-cryptography/ (дата звернення: 04.01.2025).*

17. *Щур Н., Покотило О., Байлюк Є. Огляд та порівняльний аналіз алгоритмів-фіналістів конкурсу NIST зі стандартизації легковагової криптографії. Вісник Хмельницького національного університету. 2023. Т. 1. № 5 (325). С. 269- 278. DOI: https://doi.org/ 10.31891/2307-5732-2023-325-5-269-278.*

ANALYSIS OF THE FEATURES OF USING CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS FOR UAV PROTECTION

A. Y. Horpenyuk, N. M. Luzhetska, O. A. Horpenyuk

Lviv Polytechnic National University,
Department of Information Protection

This paper investigates the features of constructing and applying cryptographic protocols to protect unmanned aerial vehicles (UAVs) from cyberattacks.

Today, we witness a uniquely rapid development of military-purpose UAVs. This unprecedented growth is driven by the decisive influence of combat UAV characteristics on the outcomes of real military operations. Additionally, this development is based on the analyzed, documented, and recognized results of UAV usage in combat conditions.

The paper examines the main types of specialized cyberattacks on UAVs and their impact on UAV performance. The study examines cryptographic algorithms and protocols designed to secure data transmission, ensure authentication, maintain confidentiality, and preserve information integrity. The application of various cryptographic protocols, such as TLS, IPsec, DTLS, and others, is studied in the context of their use for securing UAV communication channels. As a result of the analysis, a basic and enhanced architecture for a UAV protection system was developed based on the selected protocols. Recommendations for implementing this system in real conditions are also provided. Prospective ways to improve UAV protection systems are analyzed.

Keywords: UAV, cryptography, message authenticity, hashing function.