ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захищеного зв'язку для дронів на основі криптографії»

зі спеціальності *123 Комп'ютерна інженерія*
(код, найменування спеціальності)

освітньо-професійної програми *Комп'ютерні системи та мережі*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____
(підпис)

Виконав: здобувач вищої освіти групи КСДМ-61
Дмитро СКУДНИЙ
(прізвище, ім'я)

Керівник *к.т.н. доцент* Наталія ЛАЩЕВСЬКА
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Комп’ютерної інженерії
Ступінь вищої освіти Магістр
Спеціальність 123 Комп’ютерна інженерія
Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри КІ
_____ Лащевська Н.О.
“___” _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

_____
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Система захищеного зв’язку для дронів на основі криптографії»

керівник кваліфікаційної роботи Лащевська Н.О., к.т.н. доцент
(прізвище, ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.12.2024

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси сучасних систем зв’язку БПЛА.
криптографічні алгоритми AES, RSA, ECC та їх програмні реалізації.
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. дослідження проблеми захисту зв’язку БПЛА.
2. дослідити можливості застосування криптографії для захисту даних у системах зв’язку БПЛА.
3. розробити архітектуру захищеної системи зв’язку для БПЛА.

4. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту зв'язку БПЛА.	15.09.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	25.09.2024 р.	
3.	Проаналізувати загрози та вразливості каналів зв'язку БПЛА	02.10.2024 р.	
4.	Дослідити можливості застосування криптографії для захисту даних у системах зв'язку БПЛА;	15.10.2024 р.	
5.	Розробити архітектуру захищеної системи зв'язку для БПЛА.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	22.11.2024 р.	
7.	Підготовка доповіді до захисту.	26.11.2024 р.	

Здобувач вищої освіти _____ _____
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ _____
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу

здобувача Скудного Дмитра

на тему: «Система захищеного зв’язку для дронів на основі криптографії»

Актуальність: Забезпечення захищеного зв’язку для дронів набуває ключового значення в сучасному світі, оскільки ці безпілотні системи дедалі більше використовуються в різних сферах, таких як оборона, логістика, рятувальні операції та сільське господарство. Незахищений зв'язок може стати об'єктом кібератак, що може призвести до перехоплення управління, витоку даних або навіть повної компрометації місії дрона.

Використання криптографії в системах зв’язку для дронів забезпечує високий рівень конфіденційності, автентифікації та цілісності даних. Це дозволяє уникнути несанкціонованого доступу до управління дронами, забезпечуючи безперервність їх роботи навіть у разі спроби злому.

Зростання числа кібератак на безпілотні системи демонструє необхідність у запровадженні криптографічних рішень для захисту кінцевих точок зв’язку дронів. Порушення або компрометація цих систем може призвести до значних втрат, що впливає на безпеку, продуктивність і функціональність організацій, які використовують дрони.

Таким чином, розробка системи захищеного зв’язку для дронів на основі криптографії є актуальною та своєчасною, оскільки сприяє забезпеченню кібербезпеки в умовах сучасних загроз.

Позитивні сторони:

1. На основі проведеного аналізу у роботі визначено ключові аспекти проблеми забезпечення захищеного зв’язку для дронів.
2. Досліджено сучасні методи і технології криптографічного захисту, що можуть бути застосовані для забезпечення конфіденційності, автентифікації та цілісності даних у системах зв’язку для дронів.
3. Запропоновано варіант архітектури системи захищеного зв’язку для дронів, що базується на сучасних криптографічних алгоритмах, а також розроблено рекомендації щодо їх інтеграції у системи управління безпілотними апаратами.

Матеріали роботи викладено грамотно і послідовно. Результати досліджень узагальнені у чітких і змістовних висновках.

Недоліки:

1. У роботі варто було б провести більш детальний аналіз використання криптографічних систем захищеного зв’язку для дронів на прикладі конкретної організації або сценарію застосування, що дозволило б краще оцінити практичну ефективність запропонованих рішень.

У роботі варто було б провести більш детальний аналіз використання криптографічних систем захищеного зв’язку для дронів на прикладі конкретної організації або сценарію застосування, що дозволило б краще оцінити практичну ефективність запропонованих рішень.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“відмінно”**, а здобувач(ка) **Скудного Дмитра** – присвоєння кваліфікації магістр з комп’ютерної інженерії за спеціалізацією комп'ютерні системи та мережі.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач СКУДНОГО Дмитра до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 123 Комп'ютерна інженерія
освітньо-професійної програми Комп'ютерні системи та мережі
(шифр і назва спеціальності)
на тему: «Система захищеного зв'язку для дронів на основі криптографії».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Андрій БОНДАРЧУК
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***СКУДНИЙ Дмитро*** обрав тему роботи, метою якої було розробити систему захищеного зв'язку для безпілотних літальних апаратів із використанням криптографічних методів. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***СКУДНИЙ Дмитро*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***СКУДНОГО Дмитра*** на оцінку **"відмінно"** та присвоїти йому кваліфікацію магістр з комп'ютерної інженерії за спеціалізацією комп'ютерні системи та мережі.

Керівник кваліфікаційної роботи _____ Наталія ЛАЩЕВСЬКА
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **СКУДНИЙ Дмитро** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Комп'ютерної інженерії
(назва)

_____ Наталія ЛАЩЕВСЬКА
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 85 стор., 10 табл., 21 рис., 35 джерел.

Наукове завдання – полягає у дослідженні сучасних систем зв'язку безпілотних літальних апаратів, аналізі їхніх вразливостей, вивченні принципів криптографії, розробці та тестуванні архітектури захищеної системи зв'язку з використанням криптографічних методів.

Мета роботи – розробити систему захищеного зв'язку для безпілотних літальних апаратів із використанням криптографічних методів.

Об'єкт дослідження – системи зв'язку безпілотних літальних апаратів.

Предмет дослідження – методи та засоби криптографічного захисту даних у каналах зв'язку БПЛА.

Короткий зміст роботи: Проведено аналіз предметної області та розробку системи захищеного зв'язку для безпілотних літальних апаратів із використанням криптографічних методів.

Виконано аналіз сучасних систем зв'язку БПЛА, розглянуто їх класифікацію, специфіку функціонування та основні вразливості каналів зв'язку. Проаналізовано сучасні загрози, такі як перехоплення даних, несанкціонований доступ та атаки на канали зв'язку.

Розроблено архітектуру системи захищеного зв'язку для дронів, реалізовано криптографічний захист із використанням сучасних алгоритмів шифрування. Проведено тестування розробленої системи, оцінено її стійкість до загроз та ефективність.

Розроблено рекомендації для практичного впровадження системи та запропоновано напрями для її подальшого вдосконалення.

КЛЮЧОВІ СЛОВА: БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ (БПЛА), СИСТЕМА ЗАХИЩЕНОГО ЗВ'ЯЗКУ, КРИПТОГРАФІЧНИЙ ЗАХИСТ ДАНИХ, КАНАЛИ ЗВ'ЯЗКУ ДРОНІВ, АСИМЕТРИЧНЕ ШИФРУВАННЯ

ABSTRACT

Text part of the master's qualification work: 85 pages, 10 pictures, 21 table, 35 sources.

Scientific Task – involves studying modern communication systems of unmanned aerial vehicles (UAVs), analyzing their vulnerabilities, exploring cryptographic principles, and developing and testing the architecture of a secure communication system using cryptographic methods.

Purpose of the Work – to develop a secure communication system for unmanned aerial vehicles using cryptographic methods.

Object of Research – communication systems of unmanned aerial vehicles.

Subject of Research – methods and means of cryptographic data protection in UAV communication channels.

Summary of the Work: The subject area has been analyzed, and a secure communication system for unmanned aerial vehicles has been developed using cryptographic methods.

An analysis of modern UAV communication systems has been conducted, their classification, functioning specifics, and main vulnerabilities of communication channels have been reviewed. Modern threats, such as data interception, unauthorized access, and attacks on communication channels, have been examined.

The architecture of a secure communication system for drones has been developed, implementing cryptographic protection using modern encryption algorithms. The developed system has been tested, and its resilience to threats and effectiveness have been evaluated.

Recommendations for practical implementation of the system have been provided, and directions for its further improvement have been proposed.

KEYWORDS: UNMANNED AERIAL VEHICLES (UAVs), SECURE COMMUNICATION SYSTEM, CRYPTOGRAPHIC DATA PROTECTION, DRONE COMMUNICATION CHANNELS, ASYMMETRIC ENCRYPTION

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8
ВСТУП 9
1 АНАЛІЗ СУЧАСНИХ СИСТЕМ ЗВ'ЯЗКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ 11
1.1 Типи безпілотних літальних апаратів та їх класифікація 11
1.2 Особливості систем зв'язку у БПЛА 20
1.3 Сучасні загрози та вразливості у каналах зв'язку 24
Висновок до розділу 1 32
2 КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ДАНИХ 33
2.1 Основи криптографії: принципи та механізми симетричного та асиметричного шифрування 33
2.2 Застосування криптографії для захисту каналів зв'язку 46
2.3 Аналіз ефективності криптографічних алгоритмів у системах зв'язку 59
Висновок до розділу 2 67
3 РОЗРОБКА СИСТЕМИ ЗАХИЩЕНОГО ЗВ'ЯЗКУ ДЛЯ ДРОНІВ 68
3.1 Моделювання процесу створення захищеного каналу управління БПЛА та його вплив на механіку польоту 68
3.2 Реалізація криптографічного захисту у каналах передачі даних 74
3.3 Математична модель системи захищеного вз'язку 80
Висновок до розділу 3 83
ВИСНОВКИ 84
ПЕРЕЛІК ПОСИЛАНЬ 86
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 90

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БПЛА – Безпілотний літальний апарат.

AES – Advanced Encryption Standard (стандарт шифрування даних).

RSA – Rivest-Shamir-Adleman (алгоритм асиметричного шифрування).

SSL – Secure Sockets Layer (протокол захисту передачі даних).

TLS – Transport Layer Security (протокол безпечної передачі даних).

VPN – Virtual Private Network (віртуальна приватна мережа).

ECC – Elliptic Curve Cryptography (криптографія на основі еліптичних кривих).

SHA – Secure Hash Algorithm (алгоритм хешування).

PKI – Public Key Infrastructure (інфраструктура відкритих ключів).

OTP – One-Time Pad (одноразовий шифроблокнот).

IoT – Internet of Things (інтернет речей).

DoS – Denial of Service (відмова в обслуговуванні, тип атаки).

MITM – Man-in-the-Middle (атака типу "людина посередині").

HMAC – Hash-based Message Authentication Code (хешований код автентифікації повідомлення).

GPS – Global Positioning System (глобальна система позиціонування).

ВСТУП

Актуальність дослідження. Забезпечення безпеки систем зв’язку безпілотних літальних апаратів (БПЛА) набуває особливої важливості з огляду на стрімкий розвиток технологій дистанційного керування та передачі даних. По-перше, БПЛА активно використовуються у різних сферах, включаючи військову, цивільну та комерційну, що робить їх критично важливими для забезпечення безпеки даних і операцій. По-друге, канали зв’язку БПЛА є вразливими до кібератак, включаючи перехоплення, злам і внесення шкідливих даних, що може призвести до компрометації всієї системи управління. По-третє, зростання складності загроз та використання сучасних методів атаки, таких як глушіння сигналу або спуфінг, вимагає впровадження більш ефективних методів захисту.

Криптографічні методи захисту є важливим інструментом забезпечення безпеки передачі даних у каналах зв’язку БПЛА. Вони дозволяють запобігати несанкціонованому доступу до інформації, гарантують цілісність даних і забезпечують аутентифікацію учасників зв’язку. Використання сучасних криптографічних алгоритмів дозволяє не лише посилити безпеку, але й мінімізувати ризики перехоплення та маніпуляцій даними в умовах роботи в реальному часі.

Актуальність даної теми визначається необхідністю створення комплексних рішень для захисту каналів зв’язку БПЛА, які враховують сучасні загрози та забезпечують ефективність у різних сценаріях використання.

Мета роботи – розробити систему захищеного зв’язку для безпілотних літальних апаратів із використанням криптографічних методів.

Об’єкт дослідження – системи зв’язку безпілотних літальних апаратів.

Предмет дослідження – методи та засоби криптографічного захисту даних у каналах зв’язку БПЛА.

Наукові завдання:

1. дослідити особливості сучасних систем зв’язку БПЛА;
2. проаналізувати загрози та вразливості каналів зв’язку БПЛА;

3. вивчити принципи та механізми криптографії;

4. дослідити можливості застосування криптографії для захисту даних у системах зв’язку БПЛА;

5. розробити архітектуру захищеної системи зв’язку для БПЛА;

6. протестувати ефективність запропонованого рішення.

Методи дослідження – аналіз наукових джерел, вивчення стандартів і технічної документації, моделювання, тестування ефективності криптографічних алгоритмів.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування криптографічних методів для захисту каналів зв’язку БПЛА та реалізації цих рекомендацій на практиці.

1 АНАЛІЗ СУЧАСНИХ СИСТЕМ ЗВ'ЯЗКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Системи зв'язку безпілотних літальних апаратів (БПЛА) є одним із ключових елементів їхньої функціональності, що забезпечує взаємодію між дроном та оператором, передавання даних, а також виконання автоматичних і напівавтоматичних завдань. Розвиток технологій зв'язку та збільшення сфер застосування БПЛА призводять до зростання вимог до їхніх каналів зв'язку, включаючи швидкість передачі, надійність, масштабованість і безпеку. Здатність забезпечити ефективний зв'язок особливо важлива для виконання критичних завдань, таких як військові операції, моніторинг катастроф чи комерційна доставка вантажів [1].

1.1 Типи безпілотних літальних апаратів та їх класифікація

Мікродрон – це компактний безпілотний літальний апарат вагою до 2 кг. Вони зазвичай використовуються для виконання короткотривалих місій у межах обмежених територій або приміщень, де більші дрони не можуть діяти через їхні розміри. Мікродрони характеризуються невисокою вартістю, простотою використання та низьким рівнем шуму, що робить їх ідеальними для аерофотозйомки, огляду будівель або пошуково-рятувальних робіт у важкодоступних місцях. Приклад мікродрону представлений на рисунку 1.1.

– Приклади застосування: моніторинг приміщень, інспекція вузьких ділянок, навчання операторів.

– Популярні моделі: DJI Tello, Parrot Mambo.

– Обмеження: мала вантажопідйомність, короткий час автономної роботи (до 20–30 хвилин).

Рисунок 1.1 – Мікродрон DJI Tello

Міні-дрон – це безпілотник вагою від 2 до 25 кг, який використовується для завдань середньої складності, таких як моніторинг невеликих територій, аерофотозйомка та відеозйомка. Міні-дрони популярні у комерційних і цивільних додатках через їхню гнучкість, високу якість отримуваних даних і більший час автономної роботи в порівнянні з мікродронами [2]. Приклад міні-дрону представлений на рисунку 1.2.

– Приклади застосування: сільськогосподарський моніторинг, картографування, екологічний моніторинг.

– Популярні моделі: DJI Mavic 3, Autel EVO II.

– Переваги: підвищена автономність (до 40–60 хвилин), можливість виконувати місії на більших відстанях (до 5–10 км).

– Обмеження: обмежена дальність польоту, менша стійкість до сильного вітру порівняно з більшими моделями.

Рисунок 1.2 – Міні-дрон DJI Mavic 3

Середній дрон – це БПЛА вагою від 25 до 150 кг, який забезпечує можливість виконання складних місій у різних умовах. Такі дрони часто використовуються для спостереження за великими територіями, проведення довготривалих моніторингових завдань або рятувальних операцій. Приклад середнього дрону представлений на рисунку 1.3.

– Приклади застосування: моніторинг лісових пожеж, морських акваторій, пошуково-рятувальні місії.

– Популярні моделі: Insitu ScanEagle, Yamaha RMAX.

– Переваги: значна дальність польоту (до 50 км і більше), можливість тривалого перебування у повітрі.

– Обмеження: вимагають спеціального обладнання для злету та посадки, потребують більш складного управління [3].

Рисунок 1.3 – Середній дрон Insitu ScanEagle

Великі дрони – це безпілотники вагою понад 150 кг, призначені для виконання стратегічних завдань у військовій, комерційній або науковій сфері. Вони здатні перевозити великі вантажі, здійснювати розвідувальні місії на великі відстані та працювати у складних погодних умовах. Приклад середнього дрону представлений на рисунку 1.4.

– Приклади застосування: військова розвідка, доставка великогабаритних вантажів, стратегічний моніторинг територій.

– Популярні моделі: MQ-9 Reaper, Bayraktar TB2

Рисунок 1.4 – Середній дрон Bayraktar TB2

– Переваги: велика вантажопідйомність, тривалий час польоту (до 24 годин і більше).

– Обмеження: висока вартість, складність експлуатації, потреба у великій наземній інфраструктурі.

Дрони короткого радіусу дії забезпечують дальність польоту до 5 км і здебільшого використовуються для локальних завдань. Вони ідеальні для аерофотозйомки, локального моніторингу чи інспекції [4]. Приклад короткого радіусу дії дрону представлений на рисунку 1.5.

– Популярні моделі: DJI Phantom 4.

– Переваги: простота управління, низька вартість.

– Обмеження: обмежена дальність і автономність.

Рисунок 1.5 – Дрони короткого радіусу дії DJI Phantom 4

Дрони середнього радіусу дії мають дальність польоту до 50 км. Вони широко застосовуються у сільському господарстві, моніторингу інфраструктури та охороні територій. Приклад середнього радіусу дії дрону представлений на рисунку 1.6.

Популярні моделі: eBee X.

– Переваги: підвищена автономність, більший радіус дії.

– Обмеження: необхідність в удосконалених системах зв’язку для стабільного управління.

Рисунок 1.6 – Дрони середнього радіусу дії eBee X

Дрони великого радіусу дії можуть здійснювати польоти на відстань понад 50 км. Вони використовуються у стратегічних місіях, таких як військова розвідка, трансконтинентальна доставка або геологічна розвідка. Приклад середнього радіусу дії дрону представлений на рисунку 1.7.

– Популярні моделі: MQ-1 Predator.

– Переваги: можливість роботи у важкодоступних регіонах, велика автономність.

– Обмеження: потреба у складній інфраструктурі для забезпечення зв’язку та управління.

Рисунок 1.7 – Дрони середнього радіусу дії MQ-1 Predator

БПЛА поділяються на військові, комерційні та цивільні залежно від їхнього призначення та сфер використання. Кожна категорія має свої особливості, що визначають вимоги до систем зв’язку, які забезпечують їх ефективне функціонування.

Військові дрони є високотехнологічними апаратами, розробленими для виконання завдань у складних та небезпечних умовах. Основні функції військових БПЛА включають розвідку, спостереження, наведення, нанесення ударів, перевезення вантажів, забезпечення зв’язку та електронної боротьби.

Особливості використання:

– Необхідність забезпечення стійкого та зашифрованого зв’язку для управління та передачі даних.

– Використання супутникових каналів зв’язку для тривалих місій і на великих відстанях.

– Реалізація заходів для захисту від перехоплення даних і глушіння сигналів.

Приклади моделей:

– MQ-9 Reaper – ударний дрон із можливістю тривалого патрулювання.

– Bayraktar TB2 – розвідувально-ударний дрон, який широко застосовується в бойових операціях.

Вимоги до зв’язку:

– Застосування криптографічних протоколів (TLS, VPN).

– Використання захищених частот і систем резервування зв’язку для мінімізації впливу атак.

Комерційні дрони знаходять застосування у багатьох галузях, включаючи логістику, сільське господарство, будівництво та моніторинг інфраструктури. Їхні основні завдання – це доставка вантажів, картографування територій, обстеження інфраструктурних об'єктів, моніторинг стану сільськогосподарських угідь [5].

Особливості використання:

– Потребують систем зв’язку, які забезпечують високу якість передачі даних у реальному часі.

– Зазвичай працюють у межах середнього радіусу дії (до 50 км) із використанням мобільних мереж або Wi-Fi.

– Залежність від хмарних технологій для аналізу даних і зберігання інформації.

Приклади моделей:

– Amazon Prime Air – дрон для доставки невеликих вантажів.

– SenseFly eBee X – дрон для аерофотозйомки та сільськогосподарських завдань.

Вимоги до зв’язку:

– Стабільне підключення до мережі для управління через хмарні платформи.

– Використання захищених каналів для передачі комерційно важливих даних.

Цивільні дрони розроблені для аматорського використання, хобі, а також для некомерційних задач, таких як фотографування, відеозйомка, або моніторинг локальних територій. Такі дрони є найпоширенішими через їхню доступність та простоту у використанні.

Особливості використання:

– Працюють у межах обмеженого радіусу дії (до 5 км).

– Використовують стандартні канали зв’язку, такі як Wi-Fi або Bluetooth, які можуть бути вразливими до перехоплення сигналу.

– Мають низьку потребу у складних системах шифрування.

Приклади моделей:

– DJI Phantom 4 – популярний дрон для фотографії та відеозйомки.

– Parrot Anafi – компактний дрон для аматорського використання.

Вимоги до зв’язку:

– Стабільність сигналу для управління через смартфони чи пульти дистанційного керування.

– Можливість підключення до мобільних додатків для обробки та збереження даних.

Таблиця 1.1 – Особливості зв’язку кожного типу БПЛА

Тип БПЛА	Основні завдання	Особливості зв’язку	Приклади моделей
Військові	Розвідка, удари, електронна боротьба	Захищені супутникові канали, криптографія	MQ-9 Reaper, Bayraktar TB2
Комерційні	Логістика, моніторинг, агроаналіз	Мобільні мережі, Wi-Fi, хмарні платформи	Amazon Prime Air, eBee X
Цивільні	Фотографія, відео, хобі	Wi-Fi, Bluetooth, базові системи управління	DJI Phantom 4, Parrot Anafi

1.2 Особливості систем зв’язку у БПЛА

Системи зв’язку безпілотних літальних апаратів є ключовим компонентом, що забезпечує їхню ефективну роботу. Вони відповідають за передачу даних між дроном, наземною станцією та іншими елементами системи. Залежно від призначення і технічних характеристик, БПЛА можуть використовувати різні архітектури зв’язку, кожна з яких має свої особливості [6].

Архітектура систем зв’язку БПЛА

Прямий канал керування (Line-of-Sight, LOS) використовується для забезпечення зв’язку між оператором та дроном у межах прямої видимості. Цей метод є найпростішим і найпоширенішим для цивільних та аматорських БПЛА.

Особливості:

– Частоти передачі: 2.4 ГГц або 5.8 ГГц.

– Дальність дії: до 5 км для більшості аматорських дронів.

– Придатність для завдань, що не потребують великого радіусу дії.

Переваги:

– Простота реалізації.

– Низька вартість обладнання.

Недоліки:

– Залежність від перешкод (будівлі, дерева).

– Вразливість до глушіння сигналу.

Супутниковий зв’язок (Beyond-Line-of-Sight, BLOS) використовується для управління БПЛА на великих відстанях, особливо у військових і стратегічних місіях. Він дозволяє підтримувати зв’язок у будь-яких умовах, незалежно від прямої видимості.

Особливості:

– Використання супутників для передачі сигналів на дрон і наземну станцію.

– Придатність для дронів великого радіусу дії (понад 50 км).

Переваги:

– Глобальне покриття.

– Можливість працювати у важкодоступних районах (океани, пустелі).

Недоліки:

– Висока вартість обладнання.

– Затримка сигналу через велику відстань передачі.

Застосування мобільних мереж є перспективним рішенням для комерційних і цивільних БПЛА. Використання стандартів 4G/5G дозволяє забезпечити високу швидкість передачі даних і стабільність зв’язку.

Особливості:

– Використовуються на дронах середнього радіусу дії.

– Можливість підключення до хмарних сервісів для обробки та зберігання даних.

Переваги:

– Висока швидкість передачі даних.

– Можливість інтеграції з інтернетом речей (IoT).

Недоліки:

– Залежність від покриття мобільної мережі.

– Вразливість до кібератак у незахищених мережах.

Wi-Fi-зв’язок широко використовується у цивільних та аматорських дронах через його доступність і низьку вартість.

Особливості:

– Придатний для коротких дистанцій (до 2 км).

– Використовується у малих дронах для аерозйомки або навчання.

Переваги:

– Дешевизна реалізації.

– Простота налаштування.

Недоліки:

– Вразливість до перешкод.

– Обмежений радіус дії.

Mesh-мережі (Peer-to-Peer) забезпечують зв’язок між декількома дронами без централізованої базової станції. Цей тип зв’язку підходить для автономних місій зі складною взаємодією дронів.

Особливості:

– Використання протоколів динамічної маршрутизації для передачі даних.

– Придатність для кооперативних місій (пошуково-рятувальні операції).

Переваги:

– Висока надійність зв’язку через резервування маршрутів.

– Можливість роботи у важкодоступних місцях.

Недоліки:

– Складність налаштування.

– Високі вимоги до обладнання.

– Особливості вибору систем зв’язку

Вибір системи зв’язку залежить від типу завдання, дальності польоту, умов експлуатації та вимог до безпеки. Наприклад:

– Для аматорських дронів найкраще підходить Wi-Fi-зв’язок через простоту та низьку вартість.

– Для військових БПЛА критично важливим є використання супутникового зв’язку із застосуванням криптографічного захисту.

– У комерційних застосуваннях активно використовуються мобільні мережі 4G/5G для забезпечення реального часу передачі даних.

Для передачі даних у системах зв’язку безпілотних літальних апаратів використовуються різні протоколи, кожен з яких має свої особливості, переваги та недоліки, що визначають їх застосування залежно від завдань і типу БПЛА.

Micro Air Vehicle Link (MAVLink) – це текстовий протокол з відкритим кодом, який забезпечує обмін даними між БПЛА та наземною станцією. Він використовується для передачі команд управління, параметрів польоту та телеметрії. MAVLink підтримує двосторонній зв’язок і може працювати через різні канали зв’язку, такі як Wi-Fi, радіозв’язок або мобільні мережі.

Цей протокол широко застосовується в цивільних і комерційних дронах через свою легкість і сумісність із багатьма платформами. Однак MAVLink не має вбудованого шифрування, що робить його вразливим до атак, якщо не використовуються додаткові механізми захисту.

Transmission Control Protocol/Internet Protocol (TCP/IP) є стандартом Інтернету і забезпечує надійний зв'язок у мережах передачі даних. У БПЛА цей протокол використовується для організації стабільного з'єднання через Інтернет або локальні мережі, особливо для передачі великих обсягів даних, таких як відео або фотоматеріали [7].

TCP/IP забезпечує гарантовану доставку пакетів і підтримує протоколи шифрування, такі як SSL/TLS, для захисту даних. Це робить його популярним вибором для дронів, що виконують складні місії, наприклад, у військових або стратегічних операціях. Однак використання TCP/IP може спричиняти затримки передачі, особливо в умовах великого навантаження на мережу.

Real-Time Streaming Protocol (RTSP) – це протокол, який використовується для передачі потокового відео та аудіо в реальному часі. Він є популярним вибором для дронів, які здійснюють відеоспостереження або трансляцію даних на наземну станцію.

RTSP дозволяє налаштовувати параметри відеопотоку, такі як роздільна здатність і частота кадрів, що робить його зручним для передачі даних у режимі реального часу. Однак цей протокол не має вбудованих механізмів безпеки, тому потребує зовнішнього шифрування для запобігання перехопленню або маніпуляціям із даними.

User Datagram Protocol (UDP) є легким протоколом передачі даних, який відрізняється мінімальною затримкою і високою швидкістю роботи. Він підходить для передачі команд управління, телеметрії та інших даних, які потребують миттєвого реагування.

Основна перевага UDP – це швидкість, оскільки він не перевіряє доставку пакетів. Це дозволяє зберігати зв'язок навіть у складних умовах, але призводить до

втрати даних у разі нестабільності мережі. UDP часто використовується для управління дронами, які виконують динамічні завдання [8].

Long Range (LoRa) – це протокол передачі даних, орієнтований на велику дальність зв'язку з низьким енергоспоживанням. Він широко застосовується для дронів, що виконують автономні місії в сільському господарстві, моніторингу або екологічних дослідженнях.

Протокол LoRa забезпечує зв'язок на відстані до 10–15 км, але має низьку пропускну здатність, що обмежує його використання для передачі відео або великих обсягів даних. Однак його енергоефективність робить його ідеальним для дронів із тривалим часом роботи.

Controller Area Network (CAN) – це протокол, який використовується для обміну даними між внутрішніми компонентами дрона, такими як сенсори, контролери та виконавчі механізми. Його основною перевагою є висока надійність і низький рівень помилок навіть у складних умовах експлуатації.

CAN не підходить для передачі даних на великі відстані, але є незамінним для забезпечення взаємодії між бортовими системами дрона.

Вибір протоколу передачі даних залежить від типу дрона та завдань, які він виконує. Для цивільних і комерційних дронів переважно використовуються MAVLink і UDP, тоді як для стратегічних і військових завдань застосовуються TCP/IP із додатковими рівнями безпеки.

Одним із ключових викликів є забезпечення захисту протоколів від перехоплення даних та атак типу «глушіння». У сучасних системах все більше впроваджуються криптографічні методи для шифрування даних, а також інтегруються новітні протоколи, такі як 5G, для підвищення швидкості та стійкості зв'язку.

1.3 Сучасні загрози та вразливості у каналах зв'язку

У сучасних умовах активного впровадження безпілотних літальних апаратів (БПЛА) у різні сфери діяльності, включаючи військову, комерційну та цивільну,

безпека їхніх каналів зв’язку набуває критичного значення. Канали зв’язку є ключовим елементом управління дронами, оскільки вони забезпечують передачу команд, телеметрії та інших важливих даних між дроном і наземною станцією. Будь-яке втручання в цей процес може призвести до порушення функціонування апарата, компрометації даних, а в окремих випадках – до втрати дрона або виконання ним шкідливих дій [9].

Основними викликами для каналів зв’язку є зростання кількості кібератак, перехоплення сигналів, атаки на доступність (глушіння, DoS-атаки) та підміна сигналів (спуфінг) (табл. 1.2). Уразливість систем зв’язку особливо важлива для дронів, які виконують стратегічні завдання, наприклад, розвідку, спостереження або доставку конфіденційних матеріалів. Впровадження сучасних засобів захисту, таких як криптографічне шифрування, аутентифікація та резервування каналів, є обов’язковим для мінімізації цих загроз.

Таблиця 1.2 Аналіз загроз та їх характеристик

Загроза	Суть	Ризики	Методи реалізації атаки	Можливі заходи захисту
Перехоплення даних	Перехоплення незашифрованих даних між дроном і станцією	Витік даних, компрометація приватності	Сканування частот, перехоплення Wi-Fi або RF-сигналу	Використання шифрування (AES, TLS), аутентифікація користувачів

Продовження таблиці 1.2

Спуфінг	Підміна сигналу для перехоплення чи зміни команд	Втрата контролю, зміна маршруту	Впровадження підробленого GPS-сигналу	Захист GPS (DGPS, криптографія), перевірка цілісності сигналу
Глушіння сигналу	Створення шуму на робочій частоті	Втрата зв’язку, аварійна посадка	Використання глушників, високопотужного шуму	Резервування каналів, динамічне перемикання частот
DoS-атаки	Перевантаження каналу запитами	Неможливість передати команди, втрата зв’язку	Створення великого обсягу запитів	Фільтрація трафіку, контроль доступу, VPN
MITM-атаки	Зміна даних у процесі передачі	Спотворення даних, передача підроблених команд	Перехоплення трафіку між дроном і станцією	Використання шифрування, цифрових підписів
Фізичне втручання	Установка зловмисного ПЗ чи апаратури на дрон	Повна компрометація системи	Фізичний доступ до дрона	Використання захищеного обладнання, запобігання несанкціонованому доступу

Системи зв’язку безпілотних літальних апаратів (БПЛА) мають критичні уразливості, які можуть бути використані зловмисниками для несанкціонованого

доступу, перехоплення або порушення роботи дрона. Найбільш поширеними є слабка аутентифікація, відсутність шифрування або його низька якість, що створює значні ризики для безпеки інформації та управління БПЛА [10].

1. Аутентифікація – слабка або відсутня аутентифікація у системах зв'язку БПЛА дозволяє зловмисникам отримати доступ до управління дроном, видаючи себе за легітимного користувача. Слабкі паролі, відсутність перевірки джерела сигналу та недостатні механізми аутентифікації є основними причинами цієї вразливості.

Ризики:

– Неавторизований доступ до управління дроном.

– Виконання шкідливих дій (зміна маршруту, вимкнення дрона, передача фальшивих даних).

Приклади атак:

– Атака на Wi-Fi-зв'язок із підбором пароля.

– Використання підроблених сигналів наземної станції для видавання команд.

Методи захисту:

– Використання двофакторної аутентифікації (наприклад, пароль + одноразовий код).

– Впровадження цифрових сертифікатів для підтвердження автентичності джерела сигналу.

– Регулярне оновлення паролів та обмеження спроб авторизації.

2. Відсутність шифрування, у багатьох системах зв'язку БПЛА дані передаються у відкритому вигляді, без шифрування. Це дає змогу зловмисникам перехоплювати команди управління, телеметричні дані та відеопотік.

Ризики:

– Витік конфіденційної інформації.

– Перехоплення критичних даних, таких як координати або відеоматеріали.

Приклади атак:

– Перехоплення незашифрованого відеопотоку через Wi-Fi.

– Сканування частот для отримання даних телеметрії.

Методи захисту:

– Впровадження сучасних алгоритмів шифрування (AES-256, RSA).

– Використання VPN для захисту каналів зв’язку.

– Застосування протоколів шифрування даних у реальному часі (TLS).

3. Низька якість шифрування, використання застарілих або слабких алгоритмів шифрування, таких як WEP або прості хеш-функції, не забезпечує належного рівня безпеки. Зловмисники можуть легко зламати такі системи, застосовуючи методи грубої сили або аналізу трафіку.

Ризики:

– Злам застарілих ключів шифрування.

– Розшифровка даних у реальному часі, що дозволяє втручатися у роботу системи.

Приклади атак:

– Використання програмного забезпечення для зламу WEP.

– Аналіз трафіку для виявлення закономірностей у шифруванні.

Методи захисту:

– Перехід на сучасні стандарти шифрування (AES-256, ECC).

– Регулярна зміна ключів шифрування та використання динамічних ключів.

– Впровадження багаторівневого захисту (наприклад, подвійного шифрування).

В таблиці 2.3 наведено декілька реальних кібератак на БПЛА.

Таблиця 1.3 Приклади реальних кібератак на БПЛА

Рік	Подія	Суть атаки	Причини успіху атаки	Наслідки
2011	Злам дрона США MQ-1 Predator	Атака типу "спуфінг" на GPS-сигнал, що дозволила іранським військовим перехопити управління дроном і посадити його на території Ірану.	Відсутність захищеного GPS, слабка перевірка автентичності сигналу.	Втрата апарата, витік технологій, підвищення уваги до захисту GPS.
2009	Перехоплення відеопотоку дронів США в Іраку	Іракські хакери використали програму SkyGrabber для перехоплення незашифрованого відеопотоку з військових дронів.	Відсутність шифрування відеопотоку.	Компрометація даних про місії, необхідність впровадження шифрування.
2017	Злам комерційних дронів DJI	Хакери зламали протокол зв’язку дронів DJI, отримавши доступ до маршруту польоту, даних відеозаписів та управління.	Слабкий протокол аутентифікації, відсутність багаторівневого захисту.	Зміна маршрутів польоту, витік конфіденційних даних, випуск DJI оновлення з покращеним захистом.

Продовження таблиці 1.3

2018	Глушіння дронів у Венесуелі	Під час протестів зловмисники використовували глушники для перешкоджання роботі поліцейських дронів.	Використання незахищених частот, відсутність резервних каналів зв’язку.	Збої в роботі дронів, необхідність розробки технологій частотного рознесення (FHSS).
2021	DoS-атака на систему Amazon Prime Air	Хакери провели DoS-атаку, перевантаживши канали зв’язку тестових дронів Amazon, що унеможливило їхнє управління.	Відсутність фільтрації трафіку, недостатній захист від DoS-атак.	Затримка доставки товарів, удосконалення систем управління та захисту Amazon Prime Air.
2020	Злам приватного дрона в Нідерландах	Хакери, використавши слабкий пароль на Wi-Fi, отримали доступ до управління дроном, змінюючи маршрут і перехоплюючи відео.	Слабкий пароль Wi-Fi, відсутність шифрування відеопотоку.	Витік конфіденційних відеоданих, популяризація шифрування та використання сильних паролів.

Використання криптографічних методів для захисту інформації, що передається або зберігається на безпілотних літальних апаратах (БПЛА), є важливим через численні ризики, пов’язані з втратою або перехопленням даних. БПЛА часто передають конфіденційну інформацію, включаючи відео, телеметрію, геолокаційні дані та команди управління, яка може бути надзвичайно цінною для зловмисників. Шифрування забезпечує конфіденційність переданої інформації,

роблячи її недоступною для сторонніх осіб навіть у разі перехоплення. Це особливо важливо у військових і державних операціях, де захист інформації впливає на національну безпеку.

Крім того, криптографія дозволяє підтверджувати автентичність даних, що гарантує, що інформація не була змінена під час передачі. Застосування цифрових підписів та хеш-функцій унеможливлює підміну даних або команд для БПЛА, що суттєво знижує ризик успішних кібератак, таких як глушіння або захоплення контролю. У разі фізичної втрати апарату криптографічний захист забезпечує, що дані, які зберігаються на борту, залишаться недоступними для зловмисників. Це важливо для мінімізації втрат у випадках, коли БПЛА потрапляє в чужі руки [11].

Криптографічні протоколи також дозволяють управляти безпекою в масштабних мережах БПЛА, забезпечуючи автоматизацію шифрування, обмін ключами і управління сертифікатами. Це робить можливим ефективний захист у багатьох сферах, включаючи військові операції, наукові дослідження та комерційне використання. Криптографічний захист допомагає дотримуватися міжнародних стандартів інформаційної безпеки, що є обов’язковою вимогою для багатьох галузей.

Загалом, криптографічні методи дозволяють суттєво мінімізувати ризики, пов’язані з втраченою інформацією, і є необхідним інструментом для забезпечення надійності та безпеки використання БПЛА в сучасному середовищі, де кіберзагрози постійно зростають.

Висновок до розділу 1

У розділі було проведено детальний аналіз сучасних систем зв’язку безпілотних літальних апаратів (БПЛА), визначено їхні особливості, класифікацію та актуальні проблеми безпеки.

Розглянуто різновиди БПЛА залежно від їхніх характеристик і призначення, що дозволило виділити основні вимоги до систем зв’язку для кожного типу дронів. Виявлено, що специфіка зв’язку залежить від дальності польоту, джерела енергії, сфери використання та потреб у захищеності каналів зв’язку.

Проаналізовано архітектуру систем зв’язку БПЛА, включаючи прямий радіозв’язок, супутникові канали, мобільні мережі та інші технології. Було підкреслено значення стійкості каналів зв’язку до перешкод і залежність функціонування дронів від якості та стабільності сигналу. Особливу увагу приділено ролі сучасних протоколів передачі даних і впливу на них різних зовнішніх факторів.

Висвітлено сучасні загрози та вразливості систем зв’язку БПЛА, зокрема перехоплення даних, спуфінг, глушіння сигналів та DoS-атаки. Було представлено реальні приклади кібератак на дрони, які підтверджують актуальність проблеми. Крім того, було наголошено на важливості використання криптографічних методів і інших засобів захисту для мінімізації ризиків.

Таким чином, проведений аналіз довів, що для забезпечення надійності та безпеки систем зв’язку БПЛА необхідно впроваджувати сучасні технології, спрямовані на підвищення захисту інформації, стійкості до перешкод і загроз, а також оптимізацію архітектури зв’язку. Ці висновки слугують основою для подальшої розробки системи захищеного зв’язку, що буде розглянута в наступних розділах.

2 КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ДАНИХ

2.1 Основи криптографії: принципи та механізми симетричного та асиметричного шифрування

Алгоритми шифрування інформації розділяються на кілька типів за різними критеріями, кожен з яких визначається характерними особливостями та принципами їхньої роботи. Завдяки цьому один і той самий криптоалгоритм може одночасно належати до кількох категорій. Ось основні схеми класифікації:

1. За наявністю ключа.

- *Тайнопис* – це метод захисту інформації, за якого відправник і одержувач виконують над даними певні перетворення, відомі лише їм. Алгоритм шифрування є закритим і недоступним для сторонніх осіб. Використання тайнопису переважно характерне для стародавніх методів захисту інформації або для вузькоспеціалізованих систем безпеки.
- *Криптографія з ключем* – відрізняється тим, що сам алгоритм впливу на дані може бути відомий широкому загалу, однак для його застосування потрібен ключ. Цей ключ є конфіденційним і доступний лише сторонам, які беруть участь у передачі даних [13].

2. За типом ключів.

- *Симетричні криптоалгоритми:* у цих алгоритмах для шифрування та дешифрування використовується один і той самий ключ. Такий підхід забезпечує високу швидкість роботи, але створює проблему безпечної передачі ключа між сторонами. Популярними представниками цієї групи є алгоритми DES, AES.
- *Асиметричні криптоалгоритми:* тут для шифрування застосовується відкритий ключ, доступний усім бажаючим, а для дешифрування – закритий ключ, який зберігається лише у отримувача. Це дозволяє уникнути ризиків, пов’язаних із передачею ключів, однак потребує більше обчислювальних ресурсів. Представниками цієї категорії є RSA, ElGamal, алгоритми на основі еліптичних

кривих.

3. За типом перетворень даних.

- *Перестановочні алгоритми:* змінюється лише порядок елементів даних (байтів, бітів тощо), залишаючи їхній вміст незмінним. Такий метод ускладнює розуміння інформації сторонніми, але не змінює її структуру.
- *Підстановочні алгоритми:* самі дані змінюються відповідно до правил криптоалгоритму. Цей підхід забезпечує вищий рівень безпеки та є найбільш поширеним у сучасній криптографії.

4. За розміром оброблюваних блоків даних.

- Потокові шифри: обробляють дані побітно, причому кожен біт шифрується незалежно від інших. Це дозволяє використовувати їх у реальному часі для потокового передавання даних, таких як відео- чи аудіотрансляції. До таких алгоритмів належать скремблери.
- Блокові шифри: оперують із блоками даних фіксованого розміру (зазвичай 4-32 байти). Результат шифрування залежить від усіх даних у блоці, що підвищує стійкість алгоритму до злому. Блокові шифри активно використовуються для шифрування файлів або передачі даних у мережах. До популярних представників цієї категорії відносять AES, Blowfish, Serpent [14].

Симетричні криптографічні системи

Симетричне шифрування (або симетричні криптосистеми) – це метод шифрування, в якому для обох операцій, шифрування і дешифрування, використовується один і той самий криптографічний ключ (рис. 2.1). Цей підхід був основним способом захисту інформації до появи асиметричного шифрування.

Секретність алгоритму ґрунтується на тому, що ключ повинен залишатися конфіденційним і відомим лише обом сторонам, які беруть участь в обміні даними. Перед початком передачі інформації сторони заздалегідь узгоджують ключ і забезпечують його захищене зберігання.

Симетричні системи характеризуються високою швидкістю обробки даних, що робить їх ефективними для шифрування великих обсягів інформації, однак їхня безпека значною мірою залежить від способу передачі та збереження ключа.

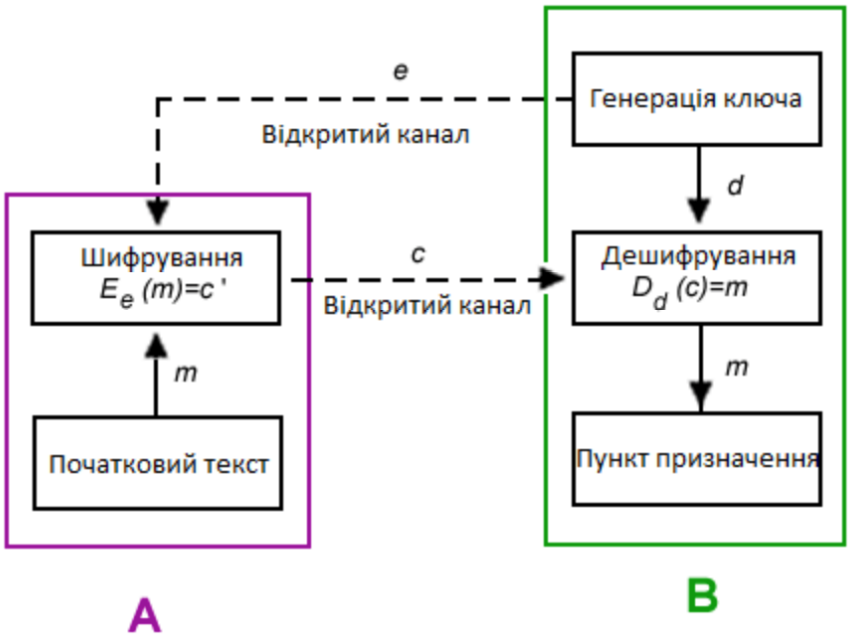

Рисунок 2.1 – Алгоритм симетричного шифрування

На сьогодні симетричні шифри поділяються на потокові та блокові.

Блокові шифри є однією з ключових складових симетричних криптосистем.

Основною їхньою особливістю є те, що шифрування даних виконується блоками фіксованого розміру (наприклад, 64 або 128 біт). Текст повідомлення розбивається на блоки, і кожен із них обробляється окремо за допомогою заданого ключа шифрування.

- Алгоритм шифрування E перетворює відкритий текст у зашифрований.
- Алгоритм дешифрування E^{-1} виконує обернене перетворення для відновлення оригінального тексту.

Формально:

$$E^{-1}(E(M,K),K) = M, \tag{2.1}$$

Де M – відкритий текст, K – ключ шифрування, $E(M,K)$ – зашифрований текст.

Для кожного ключа K, функція E реалізує перестановку вхідних блоків, яка залежить від ключа. Кількість можливих перестановок визначається як $2^n!$, де n – розмір блоку у бітах.

Основні принципи шифрування

Блокові шифри ґрунтуються на двох базових криптографічних принципах:

1. Розсіювання (diffusion): будь-яка зміна символу у відкритому тексті чи ключі впливає на велику кількість символів у шифротексті, приховуючи статистичні властивості відкритого тексту.

2. Перемішування (confusion): використання таких перетворень, які ускладнюють встановлення залежностей між відкритим текстом, ключем і шифротекстом.

Характеристики блокових шифрів

- Розмір блоку: типовими значеннями є 64, 128, 192 або 256 біт. У минулому популярними були блоки 64 біти (наприклад, DES), однак із середини 1990-х років перевага надається блокам розміром 128 біт і більше (наприклад, AES). Алгоритм роботи блокового шифру представлений на рисунку 2.2.
- Розмір ключа: варіюється від 40 біт (застарілі системи) до 256 біт. Сучасні стандарти рекомендують ключі 128, 192 або 256 біт, які забезпечують високий рівень захисту навіть від атак грубою силою.
- Режим роботи: для обробки текстів довільної довжини використовуються різні схеми шифрування, кожна з яких має свої особливості.

Режими роботи блокових шифрів

Одним із найпростіших режимів є ECB (Electronic CodeBook). У цьому режимі кожен блок відкритого тексту обробляється незалежно:

$$C_i = E(M_i, K), \tag{2.2}$$

де M_i – блок відкритого тексту, C_i – блок шифротексту, K – ключ.

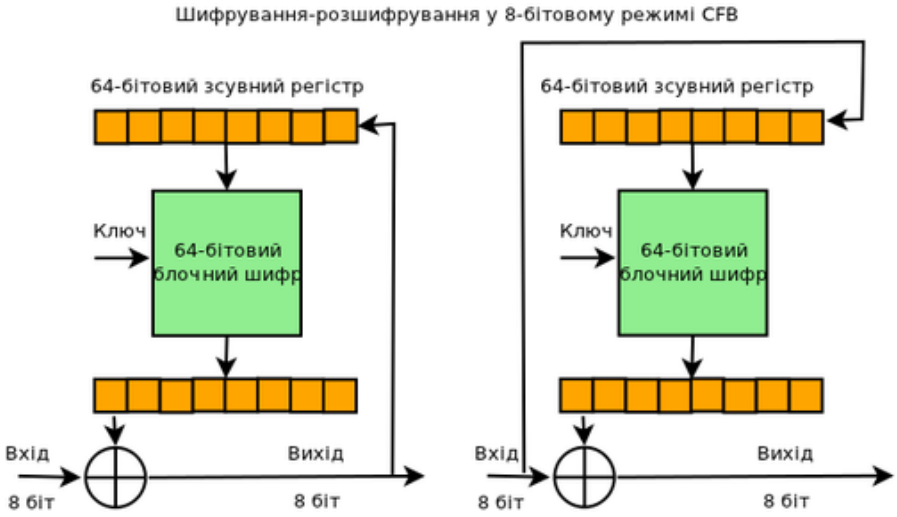

Рисунок 2.2 – Алгоритм роботи блокового шифру

Недоліком цього режиму є збереження статистичних залежностей між блоками. Наприклад, якщо у відкритому тексті кілька блоків повторюються, відповідні блоки шифротексту також будуть ідентичними. Це може призводити до витоків інформації, особливо під час шифрування великих обсягів даних, таких як зображення або відео [15].

Для усунення цієї проблеми використовують контекстно-залежні режими, наприклад:

CBC (Cipher Block Chaining): результат шифрування кожного блоку залежить від попереднього блоку, що усуває повторення. Формула:

$$C_i = E(M_i \oplus C_{i-1}, K), \tag{2.3}$$

Де C_{i-1} – шифротекст попереднього блоку, $\oplus$ – операція XOR.

Однією з проблем блокових шифрів є обробка текстів, довжина яких не кратна розміру блоку. У таких випадках "хвостовий" блок доповнюється додатковими даними (наприклад, нулями або фіксованими значеннями). Втім, таке доповнення може полегшити криптоаналіз.

Одним із рішень є гамування даних, яке передбачає поєднання блочного шифру з потоковим шифруванням. У таких режимах кожен блок обробляється із застосуванням змінного контексту, що забезпечує високу стійкість до атак.

Потоковий шифр є різновидом симетричних криптосистем (рис. 2.3), де кожен символ відкритого тексту шифрується індивідуально, враховуючи його положення в потоці даних і криптографічний ключ. На відміну від блокових шифрів, які обробляють інформацію блоками фіксованого розміру, потокові шифри працюють із даними послідовно, шифруючи кожен біт або символ одразу після його отримання [16].

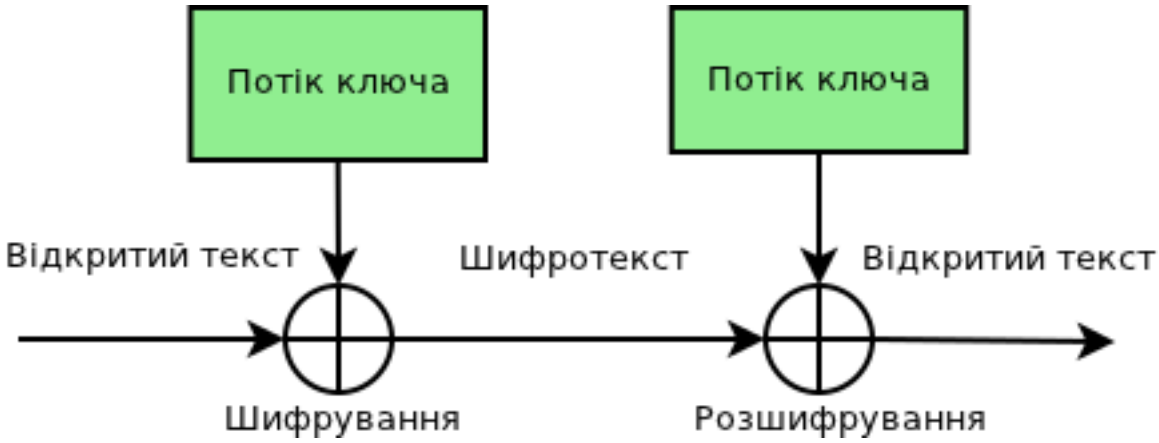

Рисунок 2.3 – Алгоритм роботи потокового шифру

У потоковому шифруванні перетворення кожного символу залежить не лише від ключа, а й від контексту, що підвищує складність криптоаналізу. Однак це вимагає ретельної синхронізації між сторонами для коректної обробки даних.

Шифр Вернама: історія та ідеал

Одним із перших ідеальних потокових шифрів був шифр Вернама, відомий також як "одноразовий блокнот" (one-time pad). У 1949 році Клод Шеннон довів, що цей метод забезпечує абсолютну криптографічну стійкість, якщо виконуються такі умови:

- Ключ має ту саму довжину, що й повідомлення.
- Ключ є випадковим і не повторюється.
- Ключ зберігається в абсолютному секреті.

Алгоритм працює за принципом побітового XOR між відкритим текстом і ключем. Формула виглядає так:

$$C_i = M_i \oplus K_i, \tag{2.4}$$

Де C_i – зашифрований біт, M_i – біт відкритого тексту, K_i – біт ключа, $\oplus$ – операція XOR.

Незважаючи на ідеальну стійкість, шифр Вернама практично важко застосувати через складнощі зберігання та передачі ключів, рівних за довжиною до повідомлень.

У реальних системах використовуються коротші ключі (наприклад, 128 біт), на основі яких генерується псевдовипадкова послідовність. Хоча це спрощує використання, такі системи стають вразливими до атак, спрямованих на передбачення цієї послідовності [15].

Синхронні потокові шифри.

У синхронних потокових шифрах обидві сторони (відправник і отримувач) повинні використовувати однакові початкові параметри й зберігати синхронізацію під час роботи. Генерація псевдовипадкової послідовності для шифрування здійснюється незалежно від вхідних даних, але залежить від початкового ключа.

Якщо в каналі зв'язку втрачається кілька бітів або додаються зайві, синхронізація порушується, і дешифрування стає неможливим. Для відновлення синхронізації можуть використовуватися спеціальні контрольні послідовності або додаткові сигнали.

Приклад

Алгоритм RC4 — один із відомих синхронних потокових шифрів, який довгий час використовувався у мережевих протоколах, таких як WEP і TLS. Однак, через виявлені вразливості його використання сьогодні обмежене.

Самосинхронізовані потокові шифри.

На відміну від синхронних, самосинхронізовані потокові шифри здатні автоматично відновлювати синхронізацію. Це досягається завдяки використанню частини попереднього шифротексту для формування наступного стану шифрування.

Формула для самосинхронізованого шифрування може виглядати так:

$$C_i = M_i \oplus \quad f(C_{i-1}, C_{i-2}, \dots\dots, C_{i-n}), \tag{2.5}$$

Де f – функція, що обчислює поточний стан на основі попередніх зашифрованих блоків.

Перевагою такого підходу є стійкість до втрати синхронізації внаслідок пошкодження даних у каналі зв'язку. Водночас, недоліком є розмноження помилок: якщо одна частина шифротексту пошкоджена, це може вплинути на кілька наступних символів.

Приклад

Алгоритм A5/1, що використовується в GSM-комунікаціях, є прикладом самосинхронізованого потокового шифру.

Переваги:

- Висока швидкість обробки даних у режимі реального часу.
- Мінімальна затримка при шифруванні та дешифруванні.
- Можливість обробляти потоки довільної довжини.

Недоліки:

- Вразливість до атак, якщо псевдовипадкова послідовність є передбачуваною.
- Необхідність надійної синхронізації між сторонами для коректної роботи.

Ефективність і надійність симетричних шифрів визначаються кількома ключовими параметрами:

- Стійкість — здатність алгоритму протистояти криптоаналітичним атакам.
- Довжина ключа — більший розмір ключа забезпечує вищу криптографічну стійкість, але впливає на швидкість.
- Кількість раундів — цикли обробки даних під час шифрування, які збільшують складність атаки, але можуть уповільнити процес.
- Розмір оброблюваного блоку — визначає обсяг даних, що шифруються за одну ітерацію.

- Стандартні значення — 64 або 128 бітів.
- Складність реалізації — апаратна чи програмна реалізація може бути критичною для ресурсоємних систем або обмежених пристроїв.

Популярні алгоритми симетричного шифрування:

DES (Data Encryption Standard) — колишній стандарт шифрування з довжиною блоку 64 біти й ключем у 56 бітів. Вважається застарілим через низьку стійкість до сучасних атак.

3DES (Triple-DES) — удосконалена версія DES, що використовує потрійне шифрування для підвищення безпеки.

AES (Advanced Encryption Standard) — сучасний стандарт із високою стійкістю, підтримує довжини ключів 128, 192 і 256 бітів.

RC2 — алгоритм із варіативною довжиною ключа, розроблений Рональдом Рівестом.

Blowfish і Twofish — швидкі й гнучкі алгоритми, орієнтовані на ефективну роботу в обмежених умовах.

IDEA (International Data Encryption Algorithm) — алгоритм із довжиною ключа 128 біт, широко використовується в системах PGP.

CAST — сімейство алгоритмів із настроюваною кількістю раундів, придатних для різних умов.

Асиметричні криптографічні системи

Асиметричне шифрування є сучасним підходом до захисту інформації, який суттєво відрізняється від симетричних методів. Основна концепція полягає у використанні двох різних ключів: відкритого (публічного) і закритого (приватного) [16].

1. Шифрування.

Для зашифрування повідомлення використовується відкритий ключ. Цей ключ доступний будь-кому й може передаватися через незахищені канали зв’язку.

Відкритий ключ генерується таким чином, що він не розкриває інформації про свій парний секретний ключ.

2. Дешифрування.

Розшифрування даних виконується виключно за допомогою відповідного закритого ключа. Цей ключ є унікальним, зберігається у таємниці й ніколи не передається іншим сторонам.

3. Односторонність функцій.

Асиметричне шифрування базується на використанні математичних функцій, які легко обчислити в одному напрямку (наприклад, множення великих простих чисел), але надзвичайно складно виконати у зворотному напрямку без спеціальної інформації (розкладання на множники).

Схематичне зображення роботи асиметричної криптографічної системи з використанням відкритого ключа наведено на рисунку 2.4.

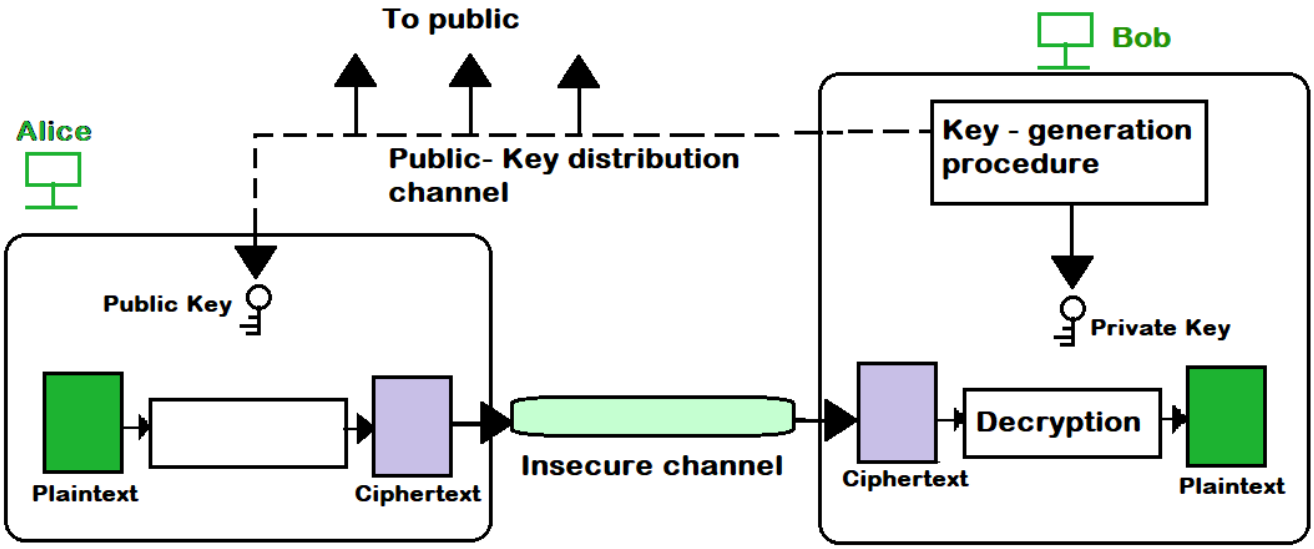

Рисунок 2.4 – Алгоритм роботи асиметричного шифрування

Обидва ключі є частинами пари, що генерується для кожного абонента. Секретний ключ повинен залишатися лише у власника та бути надійно захищений від несанкціонованого доступу. Водночас відкритий ключ може бути доступним для всіх абонентів, які потребують шифрування повідомлень для цього власника секретного ключа.

Процес використання асиметричної криптосистеми виглядає наступним чином:

1. Підготовка:

- Абонент В генерує пару ключів: секретний ключ Kv і відкритий ключ Kv.

- Відкритий ключ Kv передається абоненту А та іншим абонентам або публікується на доступному ресурсі.

2. Обмін повідомленнями:

- Абонент А шифрує повідомлення, використовуючи відкритий ключ Kv абонента В і надсилає шифротекст.

- Абонент В дешифрує отримане повідомлення, застосовуючи свій секретний ключ Kv.

Це забезпечує, що лише абонент В може дешифрувати повідомлення, оскільки тільки він володіє своїм секретним ключем. При цьому навіть абонент А не зможе дешифрувати отримане повідомлення.

Характерні особливості асиметричних криптосистем полягають у тому, що:

- Відкритий ключ Kv і зашифроване повідомлення (криптограма) C можуть бути передані через незахищені канали, оскільки доступ до них не дозволяє розшифрувати інформацію без секретного ключа.

- Алгоритми шифрування $E: M \longrightarrow C$ та дешифрування $Kv: C \longrightarrow M$ є публічними, тобто відомі усім учасникам, але їх безпека ґрунтується на таємниці секретного ключа.

У. Діффі та М. Хеллман сформулювали низку вимог, виконання яких забезпечує безпеку асиметричних криптосистем:

1. Процес генерування пари ключів (Kv, Kv) для отримувача В має бути простим і ефективним.

2. Відправник А, знаючи відкритий ключ Kv, може легко зашифрувати повідомлення M та отримати криптограму $C = E_{Kv}(M)$.

3. Одержувач В, використовуючи свій секретний ключ Kv та криптограму Cможе легко відновити оригінальне повідомлення $M = P_{Kv}(C)$.

4. Противник, знаючи відкритий ключ Kv, не може обчислити секретний ключ Kv за допомогою ефективних алгоритмів, тобто стикається з обчислювальною проблемою, яку неможливо подолати за розумний час.

5. Противник, знаючи пару (Kv, C), не може відновити вихідне повідомлення M без секретного ключа Kv, оскільки для цього необхідні обчислювальні ресурси, яких він не має.

Концепція асиметричних криптосистем з відкритим ключем базується на використанні односпрямованих функцій. Односпрямованою функцією $P(X)$ називається функція, яка має дві основні властивості:

1. Легко обчислюється, коли відомий вхід X.

2. Не існує ефективного алгоритму для відновлення вхідного значення X, знаючи тільки результат $P(X)$, що робить функцію односторонньою.

Ці властивості односпрямованих функцій гарантують безпеку асиметричних систем, оскільки навіть якщо противник отримує зашифровану інформацію чи відкритий ключ, він не може відновити вихідне повідомлення чи секретний ключ за допомогою обчислень.

Прикладом односпрямованої функції є цілочисельне множення. Пряма задача полягає в обчисленні добутку двох великих чисел P та Q, тобто знаходженні значення $N = P * Q$. Це завдання є досить простим для комп'ютера. Однак зворотне завдання — факторизація, тобто розкладання числа N на множники P та Q, — є дуже складним, а для великих значень N це завдання практично нерозв'язне за допомогою сучасних методів.

Іншим прикладом односпрямованої функції є модульна експонента з фіксованими підставою та модулем. В обох випадках (множення та модульна експонента) обчислення прямої задачі є швидким, тоді як розв'язок зворотного завдання займає значно більше часу та ресурсів, що робить ці функції підходящими для криптографії [17].

Асиметричні криптосистеми не тільки забезпечують конфіденційність, але й гарантують справжність і цілісність переданої інформації. Це досягається завдяки використанню цифрового підпису. Кожне повідомлення підписується відправником, а підпис разом із зашифрованим повідомленням передається отримувачу. Після отримання повідомлення, отримувач може перевірити підпис, тим самим підтверджуючи автентичність і цілісність інформації.

Переваги асиметричних криптосистем перед симетричними:

– Проблема розподілу ключів вирішується простіше, оскільки кожен користувач може самостійно згенерувати пару ключів. Відкриті ключі можуть публікуватися і використовуватися іншими абонентами без необхідності обміну секретними ключами.

– Лінійна залежність числа ключів: в асиметричній системі для N користувачів потрібно лише $2N$ ключів (один відкритий і один секретний для кожного користувача), в той час як у симетричних системах для кожної пари користувачів потрібен окремий ключ, що створює квадратичну залежність.

– Асиметричні криптосистеми дозволяють реалізувати протоколи взаємодії між сторонами, які не довіряють одна одній, оскільки секретний ключ залишається відомим тільки його власнику.

– *Недоліки асиметричних криптосистем:*

– Немає математичного доказу незворотності функцій, що використовуються в асиметричних алгоритмах.

– Асиметричне шифрування є повільнішим за симетричне, оскільки воно потребує більш складних та ресурсомістких обчислень. З цієї причини реалізація апаратних шифраторів для асиметричних алгоритмів є складнішою.

– Захист від підміни відкритих ключів є важливою проблемою, оскільки їх можуть замінити зловмисники, щоб отримати доступ до зашифрованих даних [18].

2.2 Застосування криптографії для захисту каналів зв’язку

Безпілотні авіаційні комплекси (БАК) зазвичай складаються з трьох основних компонентів: наземної станції управління (НСК), безпілотного літального апарата (БпЛА) та каналів зв’язку, які забезпечують їхню взаємодію. Управління безпілотниками може здійснюватися автоматично або вручну, через команди, що передаються оператором за допомогою пульта дистанційного керування (ПДК), який є частиною НСК [19].

Однією з головних проблем, пов’язаних із експлуатацією БАК, є забезпечення надійності та захищеності каналів зв’язку між НСК і безпілотником. Загрози можуть включати перехоплення управління, навмисне виведення дрона з ладу, несанкціоноване отримання чи зміну переданих даних, а також використання дрона для атак на наземну станцію або пов’язані системи.

Для протидії таким ризикам застосовуються сучасні методи захисту: шифрування даних, багаторівнева автентифікація, моніторинг аномальної активності в мережі та використання засобів радіоелектронної боротьби (РЕБ). Крім того, важливим є розробка стійких до атак протоколів зв’язку та створення систем виявлення спроб несанкціонованого втручання в роботу комплексу. Особливу увагу приділяють захисту корисного навантаження БпЛА, що часто містить критично важливу інформацію.

Ефективний захист інформації в БАК повинен враховувати кілька ключових аспектів, які прямо впливають на їхню функціональність.

1. Операційні системи реального часу (RTOS):

Переваги та виклики БпЛА працюють під керуванням спеціалізованих операційних систем, серед яких виділяються RTOS. На відміну від звичайних ОС, що орієнтовані на багатозадачність і продуктивність, RTOS має забезпечувати точність і передбачуваність у критичних ситуаціях.

❖ Співвідношення продуктивності та безпеки: захист даних не повинен порушувати детермінованість RTOS. Наприклад, надто складне шифрування може вплинути на обчислювальні цикли системи, що зменшить ефективність управління

БпЛА в умовах високого навантаження.

❖ Приклад: для забезпечення цього балансу застосовуються легкі алгоритми шифрування, такі як AES-128, що дозволяють захистити дані без значного впливу на швидкість обробки команд.

2. Структурна складність бортового обладнання та енергоефективність.

БпЛА включає численні інтегровані системи: від датчиків до бортових обчислювальних пристроїв, об'єднаних у комплекс. Енергоефективність цих систем є вирішальним фактором через обмежений ресурс живлення.

❖ Пряма залежність від енергії: захист інформації, наприклад шифрування, не повинен перевищувати 10% загального споживання енергії системи, щоб уникнути скорочення тривалості польоту.

❖ Інноваційні рішення: можна використовувати енергоефективні чіпи з апаратною підтримкою шифрування, які знижують навантаження на основний процесор дрона.

3. БАК як телекомунікаційна система.

Канал зв'язку БпЛА функціонує за спеціалізованими протоколами, які повинні забезпечувати високу швидкість обміну даними у реальному часі.

❖ Критичний параметр – затримка передачі: перевищення допустимого часу передачі може призвести до збою в управлінні. Тому засоби захисту мають враховувати це обмеження.

❖ Реалізація: використання адаптивних протоколів зв'язку, які автоматично коригують рівень шифрування залежно від обчислювальних можливостей і поточного стану системи, дозволяє мінімізувати ризики порушення передачі [20].

4. Взаємозв'язок захисту і ключових характеристик.

БпЛА Максимальна дальність польоту і вантажопідйомність безпілотника прямо залежать від економічності систем. У цьому контексті:

❖ Обмеження на вагу захисного обладнання: апаратура для шифрування та захисту повинна бути компактною і легкою, щоб не знижувати ефективність

корисного навантаження.

❖ Співвідношення: якщо вага системи захисту перевищує 5% від загальної ваги БпЛА, це може суттєво скоротити радіус дії та тривалість польоту.

Критичні канали зв'язку

1. Канал управління.

Захист цього каналу є першочерговим, оскільки атаки, спрямовані на перехоплення управління або навмисне виведення БпЛА з ладу, здебільшого здійснюються через маніпуляції з сигналами управління.

- *Ризики.* Втрата контролю над дроном, його використання для шкідливих дій або знищення.
- *Заходи захисту.* Використання шифрування команд, багаторівнева автентифікація оператора, регулярна зміна ключів шифрування.

2. Канал телеметрії.

Телеметричні дані (інформація про стан дрона, траєкторію польоту тощо) критично важливі для коректної роботи системи.

- *Ризики.* Підміна або спотворення даних може призвести до некоректного управління дроном.
- *Заходи захисту.* Перевірка цілісності даних через контрольні суми або хешування, обмеження доступу до телеметричної інформації для сторонніх.

Обмеження використання стандартних методів безпеки.

1. Залежність від структури радіоканалу та мережі:

Стандартні протоколи безпеки часто не враховують специфіки авіаційних комплексів, таких як швидкість руху об'єкта, частота зміни сигналу та віддаленість від наземної станції.

- Вирішення - розробка індивідуальних протоколів, адаптованих до швидкодії БАК.

2. Надмірність існуючих методів:

Наприклад, організація довірених центрів автентифікації або складних схем генерації ключів може виявитися зайвою в контексті БпЛА.

- Рекомендація: застосування легких, менш ресурсоємних схем

автентифікації, таких як асиметричні алгоритми (RSA або ECC) для критичних команд.

3. Навантаження на канали зв'язку:

Надмірна кількість захисних елементів знижує пропускну здатність каналів зв’язку, що може вплинути на оперативність управління дроном.

- Рішення: оптимізація шифрування, використання компресії даних до їх передачі по каналу.

4. Простота налаштувань у стандартних протоколах:

Масові рішення орієнтовані на простоту для користувача, що знижує загальний рівень захищеності.

- Вирішення: розробка спеціалізованого обладнання та програмного забезпечення для БпЛА із закритими стандартами, недоступними для сторонніх.

5. Вразливості у реалізації криптографії:

Помилки у впровадженні криптографічних алгоритмів або систем управління ключами створюють додаткові ризики.

- Рекомендація: регулярне тестування систем на вразливості, сертифікація криптографічного ПЗ за міжнародними стандартами (наприклад, FIPS 140-2).

Підходи до підвищення безпеки каналів зв’язку

1. Мобільні центри генерації ключів.

Для зниження залежності від стаціонарних центрів можна використовувати компактні пристрої на базі апаратних модулів HSM (Hardware Security Module), які виконують генерацію та зберігання ключів безпосередньо на НСК.

2. Динамічне шифрування.

Використання алгоритмів, які змінюють ключі в режимі реального часу залежно від умов зв’язку. Це ускладнює перехоплення.

3. Моніторинг загроз у реальному часі.

Впровадження системи виявлення аномалій у поведінці радіоканалу. Наприклад, різке збільшення перешкод або затримка сигналу може свідчити про спробу атаки [21].

4. Застосування вузькосмугових технологій.

Зменшення спектру використовуваних частот дозволяє уникати перехоплення, одночасно знижуючи ймовірність виявлення сигналу сторонніми.

5. Додатковий рівень захисту.

Створення резервних каналів зв’язку на альтернативних частотах для екстреного управління дроном у випадку компрометації основного каналу.

Адаптовані схеми криптографічного захисту для БпЛА

Наведемо аналіз сучасних запатентованих технологій і способів захисту, адаптованих для застосування в системах БпЛА.

1. Американський патент Lockheed Martin (US 8219799, 10.07.2012).

Особливості системи:

- Використання криптографічного модуля для перевірки ключів і визначення рівня безпеки даних.
- Можливість адаптації рівня безпеки та протоколу зв’язку у реальному часі залежно від зовнішніх умов і команд оператора.
- Підтримка динамічного перерозподілу джерела та одержувача даних, що забезпечує стійкість системи до збоїв і атак.

Практичне застосування. Така система ідеально підходить для виконання динамічних завдань, коли умови польоту можуть швидко змінюватися, наприклад, у розвідці або доставці критично важливих вантажів.

2. Система захисту від Microsoft (патент US 9531689, 27.12.2016).

Особливості:

- Використання інкапсуляції даних у кадри для зменшення ризику втрати інформації.
- Шифрування даних перед передачею, а також стиснення пакетів для зменшення навантаження на канал.

Інновації. Ця система забезпечує ефективний обмін даними навіть у мережах з обмеженою пропускною здатністю, що робить її придатною для малих дронів з мінімальними енергетичними і обчислювальними ресурсами.

3. Китайська технологія мульти-БАК (патент CN 105491564, 13.04.2016).

Особливості:

- Забезпечення безпеки комунікацій у середовищі з кількома безпілотниками.
- Уникнення помилкових запитів і відповідей через протокол взаємодії.
- Використання закритого ключа для шифрування повідомлень.

Переваги. Ця система підходить для координації роботи рою дронів, наприклад, у військових або рятувальних операціях, де важливо уникнути конфліктів між апаратами.

4. Технології SZ DJI Technology: аутентифікація та управління польотом.

Особливості:

- Центр аутентифікації та система управління польотами, які забезпечують контроль доступу до дрона.
- Аутентифікація оператора та самого БпЛА на основі унікальних ідентифікаторів.

Інновації. Така система ефективно запобігає несанкціонованому використанню дронів, що є критично важливим для комерційного застосування, зокрема в доставці вантажів або зйомці.

5. Авторизація від Microsoft Technology Licensing.

Особливості:

- Використання підписаного цифрового сертифіката для перевірки ідентифікації оператора.
- Блокування будь-яких команд, якщо сертифікат недійсний [22].

Практичне застосування. Ця технологія може бути застосована для створення захищених систем у державних організаціях або комерційних структурах, де доступ до управління дронами повинен бути суворо обмеженим.

Переваги та обмеження адаптовних систем продемоснтровано в таблиці 2.1

Таблиця 2.1 Ключові переваги та обмеження адаптованих систем

Критерій	Переваги	Обмеження
Гнучкість	Можливість адаптації до умов реального часу.	Висока складність розробки алгоритмів та протоколів.
Ефективність	Мінімізація навантаження на канал через стиснення та оптимізацію передачі даних.	Необхідність використання спеціалізованого обладнання.
Безпека	Підтримка шифрування та багаторівневої аутентифікації.	Ризик втрати продуктивності через недоліки криптографічних схем або їх некоректну реалізацію.
Придатність для рою дронів	Синхронізація між кількома дронами без конфліктів.	Висока вартість впровадження таких систем для великих парків дронів.

На додаток до рішень для забезпечення захисту каналів безпілотників з використанням алгоритмів шифрування, варто звернути увагу на ряд патентів, які забезпечують захист інформації, переданої без використання шифрування.

Наприклад, міжнародний патент на WO2005020445 датований 2005-11-10. Для управління дроном передбачена спеціальна Жовтнева антена для безпечної передачі даних, що забезпечує надійну двоточкову зв'язок в мережах бездротової передачі даних ближньої дії, а також транспондер з високою спрямованістю сигналу і додатковими сигналами перешкод в тому ж спектрі, що запобігає

переривання переданих повідомлень. Декомунізована система Northrop Grumman також надала щось більш цікаве: вони представили метод захисту зв'язку між безпілотними літальними апаратами і супутниками на частотах від 50 до 70 ГГц відповідно до патенту США № 8594662 від 26.11.2013. включаючи вибір частот сигналів в залежності від висоти літака і кута декомунізації між космічним кораблем і літаком. Крім того, значна кількість патентів присвячена методам і засобам поширення важливої інформації, які можуть використовуватися з безпілотними літальними апаратами або пристроями дистанційного керування [23].

Наприклад, патент США, 1998-11-24, США 584, в 1864 році. Motorola пропонує спосіб забезпечити односторонню аутентифікацію пристроїв та обмін ключами сеансу на основі попередньо розподіленого секрету для подальшого захисту повідомлень, що надсилаються через канали зв'язку. Найбільш близькими до запропонованих методів і систем криптографічного захисту каналів зв'язку БПЛА є методи і системи безпечного управління і моніторингу пульта дистанційного керування, запропоновані лабораторією Чарльза Старка Дрейпера (США) і описані в патенті США US9871772 від 1/16/2018 року.

Системи і методи, вивчені в якості прототипів, забезпечують досить високий рівень безпеки передачі даних для невеликих пристроїв з обмеженими обчислювальними ресурсами, керованими по радіо. Окремим випадком такого пристрою є БПЛА [24].

Методика передбачає кілька етапів, що забезпечують безпечну передачу даних між компонентами:

1. Запит параметрів RCD.

PCE запитує характеристики RCD, такі як ідентифікатор пристрою, статус системи та поточні налаштування. Це дозволяє основному керуючому елементу адаптувати команди до конкретного апарата.

2. Вибір відкритого ключа RCD.

PCE використовує відкритий ключ RCD, асоційований із його унікальним ідентифікатором. Цей ключ використовується для безпечного шифрування

переданих даних.

3. Генерація основного ключового набору.

- PCE створює набір ключів, який включає майстер-ключ для конкретної місії.
- Цей набір використовується для шифрування даних та автентифікації під час виконання завдань.

4. Шифрування ключового набору.

- Згенерований набір ключів шифрується за допомогою відкритого ключа RCD.
- Це забезпечує конфіденційність ключів під час їх передачі на пристрій.

4. Передача ключового набору на RCD.

- Ключовий набір завантажується через довірений інтерфейс завантаження ключів, який використовується одноразово в контрольованому середовищі.
- Приклад такого інтерфейсу — провідне з’єднання, яке забезпечує захист від перехоплення даних.

5. Шифрування та передача команд.

- PCE шифрує першу команду для RCD за допомогою одного з ключів, отриманих із майстер-ключа.
- Разом із командою передається мітка автентифікації, що дозволяє RCD переконатися в достовірності джерела команди.

6. Виконання місії.

Подальші команди передаються через бездротовий інтерфейс, який не є довіреним. Однак завдяки використанню майстер-ключа і сесійних ключів забезпечується надійний захист даних.

Процес виконання дій RCD відповідає на ініціативи з боку PCE, описані раніше [25].

1. RCD отримує зашифрований ключовий набір від PCE.

2. Розшифровує цей набір для видобутку свого майстер-ключа.

3. Одержує першу зашифровану команду від PCE через бездротовий зв'язок.

4. Перевіряє автентичність PCE, використовуючи мітку аутентифікації і попередньо завантажений ключ хешування.

5. Розшифровує команду за допомогою першого ключа шифрування, генерованого з майстер-ключа.

Подальші команди шифруються поточним ключем, який синхронно змінюється як на RCD, так і на PCE, залежно від кількості команд або часу. Параметри RCD можуть включати унікальний ідентифікатор або відкритий ключ. Ці дані можуть бути збережені в зовнішньому маркері (наприклад, штрих-коді) для зчитування або в пам'яті NFC мітки. Коли є додаткові станції управління (FO), вони шифрують команди для RCD за допомогою другого ключа, що забезпечує безпечний обмін даними через бездротовий канал.

Механізми генерації ключів для цих станцій аналогічні тим, що використовуються між PCE і RCD. Усі компоненти можуть одночасно керувати кількома екземплярами RCD, не змінюючи принципів взаємодії. Патент США US 9871772 детально описує апаратний модуль для захисту каналів зв'язку, що працює за цим принципом [26].

У ньому зазначається, що криптографічний модуль повинен бути окремим пристроєм, з можливістю як апаратної, так і програмної реалізації алгоритмів.

Цей модуль застосовується по-різному в залежності від пристрою, і в усіх випадках компоненти можуть бути налаштовані для різних умов використання. Патент також передбачає додаткові ключові набори для захисту даних, що передаються від RCD до PCE або FO.

Окрім описаних раніше основного (першого) та додаткового (другого) наборів ключів, метод дозволяє використовувати третій ключовий набір для захисту даних, що передаються з RCD до PCE через бездротовий канал, а також четвертий набір ключів для захисту даних, що передаються від RCD до FO.

Варіації методу захищеного управління та моніторингу віддалених пристроїв, описані в патенті США US 9871772, відрізняються такими аспектами:

– параметри, які застосовуються для ідентифікації RCD, методи їх зберігання та зчитування; принципи зміни поточних ключів шифрування;

– механізм зберігання ключів шифрування на RCD; використання електронного підпису для забезпечення цілісності ключових наборів, що завантажуються на RCD;

– чи застосовуються однакові криптографічні модулі на всіх компонентах системи; чи реалізовано безпечне встановлення з'єднання між PCE і FO;

– принципи управління ключовими наборами та їх використання за наявності кількох FO в системі;

– чи можливе одночасне керування кількома RCD з боку PCE та FO; чи використовуються третій і четвертий ключові набори для захисту даних, що передаються з RCD на PCE та FO відповідно, через бездротовий канал.

Запропонований заявниками метод криптографічного захисту каналів зв'язку

БАК має кілька переваг порівняно з методом, описаним у прототипі, які полягають у наступному:

1. Протокол розподілу ключів, запропонований у цьому методі, є більш простим у порівнянні з прототипом, не знижуючи при цьому рівень захисту. Окрім того, він забезпечує захист від атак типу «людина посередині» (MITM), чого не можна сказати про прототип, де використовувані схеми розподілу ключів не захищають від таких атак.

2. Взаємна аутентифікація БпЛА та НСК здійснюється у всіх випадках, тоді як прототип не передбачає аутентифікацію FO з боку RCD, що може призвести до загрози перехоплення управління RCD через впровадження фальшивих FO в систему.

3. Окрім криптографічного захисту, запропонований спосіб включає додатковий рівень захисту, що базується на псевдовипадковій перенастройці параметрів радіозв'язку між БпЛА та НСК.

4. Заявлений метод також передбачає шифрування не тільки каналів керування та телеметрії, але й інформації корисного навантаження БпЛА, що передається на НСК. У прототипі шифрування каналу керування є обов'язковим, канал телеметрії — опційним, а з корисного навантаження БпЛА шифрується лише

відеосигнал, і то лише за необхідності для управління RCD.

5. Запропонований спосіб дозволяє реалізувати криптографічний захист у вигляді не тільки апаратного криптографічного модуля, але й програмних модулів, які можна виконувати на польотному контролері БпЛА або на обчислювальних ресурсах НСК. Це означає, що немає потреби в установці апаратного модуля на БпЛА, що не вимагає конструктивних змін і значно менше впливає на основні характеристики БпЛА, такі як вага корисного навантаження та тривалість/дальність польоту.

6. У порівнянні з прототипом, запропонований метод покращує захист каналів зв'язку БАК, оскільки передбачає шифрування всіх повідомлень. У прототипі ж деякі службові поля («bypass») не шифруються, що створює потенційні ризики витоку інформації.

7. Також запропонований спосіб передбачає, що як апаратна, так і програмна реалізація криптографічних перетворень оснащена додатковими модулями, що забезпечують контроль працездатності цих модулів, а також їх самотестування на етапі запуску та періодичне тестування під час роботи [27].

Запропонована система криптографічного захисту каналів зв'язку БАК, яка реалізує зазначений спосіб, має додаткові переваги в порівнянні з системою прототипу, зокрема:

1) Відсутність жорсткої прив'язки до структури повідомлень і системи команд, як це передбачено в прототипі. Це дозволяє створити систему, яка є більш гнучкою і універсальною, оскільки вона може бути побудована на більш широкому спектрі обладнання для БпЛА і НСК. Прототип, в свою чергу, обмежений обладнанням, яке вже підтримує описану структуру повідомлень і команд, тобто спеціалізованим обладнанням.

2) Можливість реалізації криптографічного модуля як програмного компонента, що дозволяє знизити загальну вартість системи і використовувати більш широкий спектр існуючого обладнання для БпЛА і НСК без необхідності вносити конструктивні зміни для підключення апаратного криптографічного модуля, як у прототипі.

Заявлене пристрій є одним із варіантів реалізації способу криптографічного захисту каналів зв'язку БАК.

Технічний результат досягається наступним чином:

Крок 1. Використовуючи ключовий носій НСК, що має обчислювальні ресурси і енергонезалежну пам'ять, а також криптографічні функції, генерується пара асиметричних ключів НСК: секретний і відкритий.

Крок 2. Ключовий носій БпЛА також генерує пару асиметричних ключів БпЛА: секретний і відкритий.

Крок 3. Відкриті ключі НСК і БпЛА копіюються на відповідні носії, таким чином кожен носій містить секретні і відкриті ключі.

Крок 4. Криптографічний модуль БпЛА ініціює генерацію загального секретного пре-майстер-ключа на основі секретного ключа БпЛА і відкритого ключа НСК.

Крок 5. Ключовий носій БпЛА зчитує відкриті ключі і загальний секретний пре-майстер-ключ.

Крок 6. Криптографічний модуль НСК генерує аналогічний загальний пре-майстер-ключ на основі секретного ключа НСК і відкритого ключа БпЛА.

Крок 7. Зчитування відкритих ключів та загального пре-майстер-ключа з носіїв.

Крок 8. Криптографічний модуль БпЛА перевіряє свою готовність до роботи.

Крок 9. БпЛА відправляє повідомлення, що містить відкритий ключ і випадкове число БпЛА.

Крок 10. Криптографічний модуль НСК перевіряє наявність відкритого ключа БпЛА, інакше ігнорує повідомлення.

Крок 11. НСК ініціює відправку повідомлення з відкритим ключем НСК і випадковим числом НСК.

Крок 12. БпЛА перевіряє наявність відкритого ключа НСК, інакше повертається до кроку 9.

Крок 13. Криптографічний модуль БпЛА генерує Майстер-ключ.

Крок 14. Криптографічний модуль НСК генерує Майстер-ключ. Крок 15)

Створення сеансових ключів на основі Майстер-ключа.

Крок 16. НСК генерує аналогічні сеансові ключі.

Крок 17. БпЛА формує тестове повідомлення, зашифроване сеансовим ключем шифрування.

Крок 18. НСК перевіряє тестове повідомлення і, при виявленні помилки, повертається в режим очікування.

Крок 19. НСК формує відповідь, зашифровану сеансовим ключем, і відправляє її БпЛА.

Крок 20. БпЛА перевіряє тестове повідомлення.

Крок 21. БпЛА встановлює прапор готовності.

Крок 22. НСК встановлює прапор готовності.

Крок 23. БпЛА відкриває порт підключення.

Крок 24. НСК відкриває інтерфейс обміну з програмним забезпеченням.

Крок 25. Обмін інформацією по каналах управління і телеметрії здійснюється з використанням шифрування і контролю цілісності за допомогою сеансових ключів.

2.3 Аналіз ефективності криптографічних алгоритмів у системах зв’язку

Ключовими факторами безпеки є захист від атак типу «людина посередині» (MITM), атаки на основі підслуховування каналів зв’язку, криптоаналітичні атаки, а також рівень захисту конфіденційності і цілісності даних [28].

Ключові фактори безпеки. Криптографічні алгоритми повинні захищати передану інформацію від низки атак (табл. 2.2).

Таблиця 2.2 Типи атак та їх ключові особливості

Тип атаки	Алгоритм, який забезпечує захист	Рівень захисту	Ключова особливість
Атака «людина посередині» (MITM)	RSA, ECC, AES	Високий	икористання аутентифікації та обміну ключами, захист від підроблених повідомлень
Атаки на підслуховування каналів	AES, DES, RSA	Високий	Шифрування даних в каналах зв’язку для захисту конфіденційності
Криптоаналітичні атаки (підбір ключів)	AES, RSA, ECC	Середній до високого	Розмір ключа визначає стійкість до атак підбору та криптоаналітичних методів
Атаки на цілісність даних	AES, HMAC, SHA-256	Високий	Використання хешування для перевірки цілісності даних

Аналіз стійкості до зламу

Для оцінки стійкості криптографічних алгоритмів до зламу важливо враховувати такі фактори, як розмір ключа, криптоаналітичні методи та обчислювальні потужності, доступні зловмисникам. Різні алгоритми мають різну стійкість в залежності від їх математичної основи та розміру ключа, що забезпечує більшу або меншу складність для атаки [29].

На таблиці 2.3 наведено порівняння стійкості до атак для популярних криптографічних алгоритмів, зокрема щодо стійкості до атак на основі підбору ключів, статистичного аналізу та атаки типу "brute force".

Таблиця 2.3 Оцінка стійкості криптографічних алгоритмів до зламу

Алгоритм	Розмір ключа	Тип атаки	Час, необхідний для зламу (за умови наявності сучасних обчислювальних потужностей)	Коментарі
AES	128/256 біт	Брутфорс, криптоаналіз	Понад 10^11 років для AES-128, понад 10^33 для AES-256 (з врахуванням розвитку обчисл. Потужностей)	Стійкий до типових атак, підтримується багатьма стандартами

Продовження таблиці 2.3

RSA	2048 біт	Атаки на основі факторизації	Понад 10^5 років (для сучасних потужностей)	Вразливий до квантових атак, рекомендовано збільшувати довжину ключа
ECC	256 біт	Логарифмічні атаки (дискретний логарифм)	Понад 10^9 років (для сучасних обчисл. Потужностей)	Висока стійкість при невеликих розмірах ключів

Таблиця 2.3 демонструє різницю у стійкості до зламу для різних криптографічних алгоритмів залежно від розміру ключа і потенційних атак, що можуть бути застосовані з використанням сучасних обчислювальних ресурсів. Це дозволяє обирати найбільш відповідні алгоритми для забезпечення високого рівня безпеки в різних системах зв’язку.

Стандартні рекомендації та сертифікація.

Криптографічні алгоритми повинні відповідати певним міжнародним стандартам та сертифікаціям, які визначають мінімальні вимоги до їх безпеки в системах зв’язку. Основні стандарти, що регулюють використання криптографії в різних системах, надають вимоги до захисту інформації, а також до використання певних алгоритмів у залежності від їх стійкості та ефективності. Оцінка відповідності цим стандартам дозволяє забезпечити необхідний рівень безпеки для захисту даних у каналах зв’язку [30].

На таблиці 2.4 продемонстровано основні міжнародні стандарти, що регулюють використання криптографічних алгоритмів, а також їх вимоги до безпеки.

Таблиця 2.4 Стандарти та сертифікація криптографічних алгоритмів

Стандарт	Опис	Мінімальні вимоги	Сертифікація	Примітки
FIPS 140-2	Стандарт для оцінки безпеки криптографічних модулів в США	Мінімум 112 біт для симетричних алгоритмів, 2048 біт для RSA	Сертифікація за результатами тестування	Визнаний на міжнародному рівні
ISO/IEC 27001	Стандарт з управління інформаційною безпекою	Загальні вимоги до захисту інформації, включаючи криптографічні методи	Сертифікація після аудиту системи безпеки	Поширений у міжнародних компаніях
ISO/IEC 18033	Міжнародний стандарт для криптографії	Рекомендації щодо використання різних алгоритмів для забезпечення цілісності і конфіденційності	Без сертифікації	Містить методи для вибору криптографії

Таблиця 2.4 показує основні сертифікаційні вимоги та стандарти, яким повинні відповідати криптографічні алгоритми для забезпечення високого рівня безпеки. Ці стандарти визначають не лише технічні вимоги до алгоритмів, а й порядок їх сертифікації, що дозволяє забезпечити надійний захист переданої інформації в системах зв'язку.

Продуктивність криптографічних алгоритмів в реальних умовах

Криптографічні алгоритми повинні не лише забезпечувати високий рівень безпеки, але й бути ефективними з точки зору продуктивності, зокрема швидкості

обробки, енергоспоживання та адаптації до обмежених апаратних ресурсів. Це особливо важливо для систем зв’язку, де обмеження в обчислювальних потужностях та енергоспоживанні можуть значно вплинути на ефективність алгоритмів. Розглянемо кілька важливих аспектів продуктивності криптографічних алгоритмів.

1. Швидкість обробки та енергоспоживання Одним із критичних факторів є швидкість роботи криптографічних алгоритмів, особливо коли йдеться про передачу та прийом даних через канали зв’язку. У реальних умовах для мобільних пристроїв і БПЛА швидкість обробки алгоритмів має прямий вплив на ефективність роботи системи. Криптографічні операції, такі як шифрування, розшифрування, генерація цифрових підписів, повинні виконуватись в режимі реального часу без значних затримок.

Енергоспоживання також є важливим фактором для мобільних пристроїв, де обмежена батарея. Алгоритми, що займають багато часу для виконання або вимагають значних обчислювальних потужностей, можуть суттєво збільшити споживання енергії, що є критичним для автономних систем, таких як БПЛА або IoT пристрої [31].

Для оцінки швидкості та енергоспоживання криптографічних алгоритмів часто використовуються такі метрики:

- Час шифрування/де-шифрування: час, необхідний для виконання криптографічної операції для певного об’єму даних.
- Енергоспоживання: кількість енергії, яку алгоритм споживає на одиницю часу або операцію.

Нижче наведена таблиця, що порівнює енергоспоживання та швидкість роботи популярних криптографічних алгоритмів.

Таблиця 2.5 Швидкість та енергоспоживання криптографічних алгоритмів

Алгоритм	Швидкість (Мбіт/с)	Час шифрування (мс на 1 МБ)	Енергоспоживання (мА·с)
AES-128	150	10	50
RSA-2048	5	150	200
ECC (P-256)	100	20	60
ChaCha20	200	8	40

Як видно з таблиці, AES-128 має високу швидкість роботи, що робить його одним з найпопулярніших виборів для застосувань, де важлива швидкість обробки та зниження енергоспоживання. З іншого боку, RSA-2048 має значно більший час шифрування та енергоспоживання, що робить його менш ефективним для застосувань із обмеженими ресурсами.

Адаптація до обмежених ресурсів

Для систем з обмеженими апаратними ресурсами, таких як мікроконтролери або IoT пристрої, важливо обирати криптографічні алгоритми, які можуть працювати з обмеженим обчислювальним потенціалом, зокрема з обмеженою оперативною пам’яттю та малою обчислювальною потужністю.

Алгоритми на основі симетричних ключів, такі як AES, зазвичай потребують менше обчислювальних потужностей і пам’яті порівняно з асиметричними алгоритмами типу RSA, що робить їх більш підходящими для пристроїв з обмеженими ресурсами.

Алгоритми на основі еліптичних кривих (ECC) також є гарним вибором для таких пристроїв, оскільки вони забезпечують високий рівень безпеки при меншому розмірі ключа і кращій ефективності порівняно з RSA, що дозволяє зменшити використання ресурсів.

Час затримки

Час затримки, або латентність криптографічних операцій, є важливим для систем, де критично важливим є реальний час, наприклад, у мережах для управління БПЛА або в обміні телеметрією. Високий час затримки може призвести до зниження ефективності системи, особливо коли йдеться про передачу команд

або даних, де будь-яка затримка може вплинути на точність і своєчасність реагування системи.

Алгоритми з високою швидкістю обробки, такі як ChaCha20, можуть бути корисні для зниження латентності, оскільки вони оптимізовані для швидкої роботи в реальному часі.

Таблиця 2.6 Час затримки криптографічних операцій

Алгоритм	Час шифрування 1 МБ (мс)	Латентність (мс)	Підходить для реального часу?
AES-128	10	5	Так
RSA-2048	150	50	Ні
ECC (P-256)	20	15	Так
ChaCha20	8	3	Так

В результаті можна зробити висновок, що для систем із вимогами до низької затримки, таких як управління БПЛА, ChaCha20 і AES-128 є найбільш оптимальними виборами, оскільки вони забезпечують швидку обробку з мінімальним часом затримки [32].

Висновок до розділу 2

Розглянуто основні принципи криптографічного захисту даних, зокрема механізми симетричного та асиметричного шифрування, а також їх особливості у контексті забезпечення конфіденційності, цілісності та автентичності інформації. Симетричне шифрування, представлене алгоритмами типу AES, продемонструвало свою високу ефективність у швидкості обробки даних, тоді як асиметричні алгоритми, як-от RSA та ECC, забезпечують підвищену безпеку для автентифікації та обміну ключами. Проаналізовано використання криптографічних алгоритмів для захисту каналів зв’язку.

Продемонстровано, як різні алгоритми забезпечують стійкість до атак, таких як атаки «людина посередині» (MITM) та криптоаналітичні методи. Особливу увагу приділено аналізу ефективності алгоритмів у реальних умовах, включаючи швидкість обробки, стійкість до зламу та адаптацію до обмежених ресурсів. Цей аналіз дозволив визначити, які криптографічні методи є найбільш оптимальними для конкретних застосувань, таких як захист мобільних пристроїв або обмін даними в мережах з низькою затримкою.

Розроблено детальну оцінку продуктивності криптографічних алгоритмів у різних сценаріях використання. Представлено порівняння алгоритмів за ключовими параметрами, такими як енергоспоживання, час виконання криптографічних операцій та швидкість шифрування. Зокрема, було визначено, що алгоритми на основі еліптичних кривих (ECC) є більш енергоефективними та адаптивними для пристроїв з обмеженими обчислювальними ресурсами порівняно з RSA.

3 РОЗРОБКА СИСТЕМИ ЗАХИЩЕНОГО ЗВ'ЯЗКУ ДЛЯ ДРОНІВ

3.1 Моделювання процесу створення захищеного каналу управління БПЛА та його вплив на механіку польоту

Проведено моделювання процесу формування керуючої інформації для радіоуправління безпілотним літальним апаратом. Цей процес включав генерацію імпульсів із широтно-імпульсною модуляцією, їх перетворення в єдиний цифровий потік та шифрування за блочним алгоритмом стандарту 28147-2009.

Оцінка вимог до системи захисту каналів зв'язку (СКЗК) за криптографічними методами враховувала такі аспекти, як продуктивність, надійність, рівень шифрування та масогабаритні параметри бортової частини [33].

Ці фактори часто конфліктують між собою, особливо за умов високих вимог до пропускної здатності й зменшеної ваги обладнання БПЛА. Захищена передача даних передбачає забезпечення автентифікації, цілісності та доступності сигналів керування. Основні вимоги включають:

1) Захист від можливості заміни сигналів управління противником, що досягається використанням сертифікованого криптографічного алгоритму стандарту 28147-2009.

2) Забезпечення стійкості до перешкод помірної інтенсивності за допомогою завадостійкого кодування.

Було запропоноване комп'ютерне моделювання каналу управління БПЛА для його захисту від зловмисних дій та передачі сигналів управління БПЛА.

Для моделювання надано сигнал , який використовувався у попередньому дослідженні (описаному в Розділі). Він складається з трьох періодів по 8 імпульсів кожен загальною тривалістю ~ 60 мс.

Після запису та обробки даних у програмному середовищі MathCad 15 надходить сигнал, вигляд якого наведено на рис. 3.1.

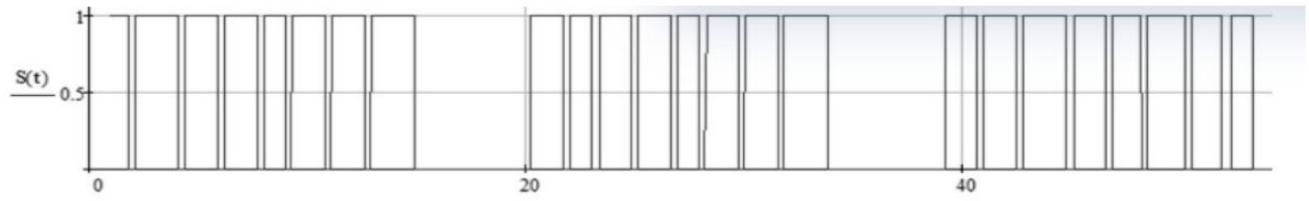

Рис. 3.1 Зображення керуючого сигналу ШІМ

Відповідно до порівняння вхідного сигналу апаратури керування БПЛА та сигналу, отриманого після всіх описаних вище операцій – шифрування/дешифрування, кодування/декодування, модуляції/демодуляції – в результаті маємо однакову послідовність цифрового керуючого сигналу, який було отримано після аналого-цифрового перетворення. Для порівняння поточний потік можна візуалізувати та представити у вигляді графіка функції, як показано на рис. 3.2.

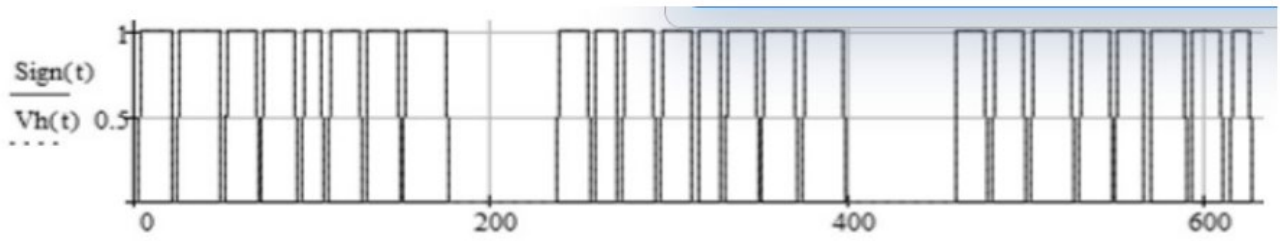

Рис. 3.2 Комбіноване зображення вхідного та вихідного цифрових потоків.

Вихідний потік даних після дешифрування представлено суцільною лінією, а вхідний цифровий потік – пунктиром. Результати моделювання процесу створення захищеного сигналу керування БПЛА показали, що в каналі зв’язку виникає затримка не менше 33 мс, яка залежить від обраної швидкості передачі даних і алгоритму [34].

Використання алгоритму AES може спричинити ще більші затримки через довжину блоку 16 байт (128 біт). Для мінімізації цих затримок необхідно забезпечити максимальну швидкість реалізації криптоалгоритму.

Перевірка впливу затримки сигналу на керування БПЛА за допомогою реальних польотів вимагає значних ресурсів, тому доцільно проводити тестування

на ранніх етапах розробки, використовуючи моделювання на робочих станціях і лабораторних стендах.

Ефективність програмного забезпечення цифрового моделювання підтверджено при стохастичному й динамічному аналізі впливу затримок сигналу. Основу моделювання становлять функціональні блоки, що відтворюють передатні функції, нелінійність та логічні операції.

Динаміка польоту БПЛА моделюється за допомогою пакету «Matlab Simulink», який дозволяє описувати систему за допомогою спеціалізованої мови. Це забезпечує високу точність і гнучкість у дослідженні характеристик системи.

Опис моделі БПЛА. На рис. 18 представлена схема моделювання БПЛА, яка включає 9 групи блоків:

- стандартний блок генератора сигналів: однокрокові функції «Крок»;
- генератор затримки вхідного сигналу типу x(t) = ax + Tp “Ramp” та генератор “білого” шуму “Band-Limited White Noise”;
- два допоміжних приціли живлення «Scope» для управління сигналами в 4-канальному управлінні;
- стандартний генератор сигналу через перемикачі «Manual Switch» підключаються до входу моделей БПЛА:
- сигнал включення єдиної функції «Крок» на вхідній моделі дозволяє оцінити якість БПЛА на перехідних кривих. Зміна амплітуди функції
- «Крок» (збільшення або зменшення) призводить до того, що модель БПЛА буде в стабільному або нестабільному стані.
- ввімкнення сигналу типу «Рампа» для оцінки якості моделі динамічного налаштування (динамічного тестування вхідного сигналу з певною затримкою) за його динамічними похибками.
- включення генератора «білого шуму» «Band-Limited White Noise» дозволяє забезпечити статистичне дослідження замкнутого контуру БПЛА [35].

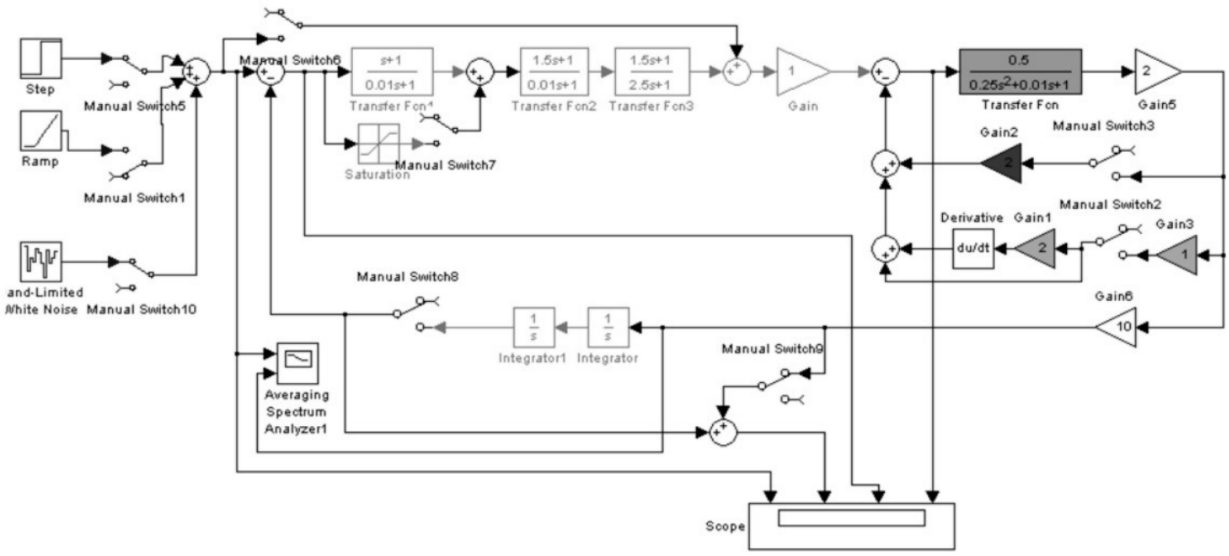

Рис. 3.3 Схема моделі передачі зв'язку БПЛА

БПЛА представлена у вигляді послідовно з'єднаних:

- дискримінатор (генератор сигналів помилки), на один вхід якого подаються стандартні сигнали, а на другий вхід – сигнали негативного зворотного зв'язку «кінематичні ланки» з двома інтеграторами;
- інтегродиференціювальний фільтр – генератор керуючого сигналу на пристрій УК:

$$K_{uc}(p) = \frac{K_{uc}(1+pT_2)}{1+pT_1} = \frac{(S+0{,}5)^2}{S+0{,}25}; \quad (3.1)$$

- пристрій передачі команд виділення з передавальними характеристиками :

$$K_{uc}(p) = \frac{K_{upc}}{1+T_{upc}} = \frac{1}{(S+10)}; \quad (3.2)$$

- генератор системи «оптимальна продуктивність» з обмеженням «Насичення»;
- узагальнений керований підсилювач БПЛА для зміщення контуру керування;
- модель БПЛА з передатною характеристикою вібраційного рівня, представлена в послідовно з'єднаних 2 аперіодичних рівнях:

$$K_{uav}(p) = \frac{K}{1+2Tp+T^2P^2}; \quad (3.3)$$

- схема БПЛА перемикається ключами К1, К2, К3, К4.

• допоміжні блоки «Область» зміни сигналів управління в часі в 4 точках БПЛА:

• сигнал помилки БПЛА;

• сигнал про помилку систем стабілізації БПЛА;

• сигнал нормального прискорення на виході БПЛА;

• робочий сигнал затримки вхідної керуючої дії на звільнення «кінематичних ланок».

В результаті модель БПЛА представлена у двох взаємно вбудованих системах:

• канал управління БПЛА з двома ланцюгами на швидкість і прискорення;

• канал керування польотом БПЛА.

Контрольні сигнали з визначеними затримками можуть бути подані кожній системі з подальшим керуванням різними точками моделі. Це можливість змінити стандартні налаштування вхідних сигналів і параметрів і структуру моделі.

Якість керування польотом БПЛА визначається похибками сталого польоту при імітації вхідного сигналу (команд) під час перешкод (рис. 3.4).

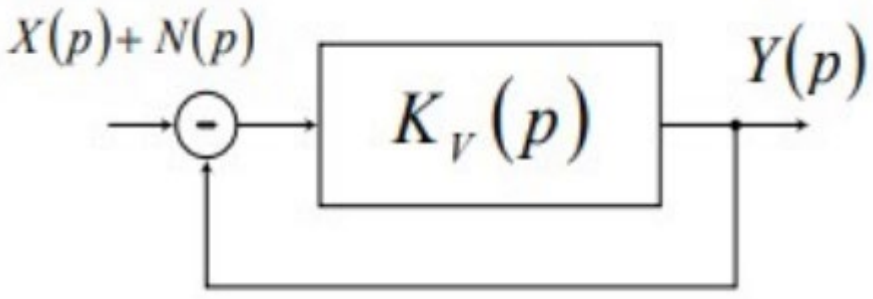

Рис. 3.4 Загальна схема керування польотом БПЛА

де X(p) – вхідний сигнал команд; N(p) – лінії радіоперешкод (включаючи затримку сигналу на операцію шифрування/дешифрування).

Нехай вхідний сигнал має спектр потужності, потужність якого зменшується разом із збільшенням частоти. Перешкодою буде вважатися «білий» шум з постійною спектральною щільністю та затримка сигналу при роботі

криптографічного перетворення.

Потім необхідно визначити динамічну похибку тестування корисного введення:

$$Z_{dyn} = \frac{1}{\pi}\int_0^{\omega_0} S_x(\omega)\,|1 - K_0(w)|^2 d\omega = \frac{1}{\pi}\int_0^{\omega_0} S_x(\omega)\,D\omega \qquad (3.4)$$

визначається тією частиною спектра сигналу, яка знаходиться за межами смуги пропускання ω0, не проходячи через систему. Діапазон коливань похибки визначається спектром перешкод, який знаходиться в межах смуги пропускання:

$$Z_{fl} = \frac{1}{\pi}\int_0^{\omega_0} S_N(\omega)\,K_0^2(\omega) = \frac{1}{\pi}\int_0^{\omega_0} S_N(\omega)\,D\omega \qquad (3.5)$$

З рис. 3.5 легко побачити наступне.

1) Збільшення смуги пропускання ω0 призводить до зменшення динамічних помилок і збільшення помилок динамічних флуктуацій.

2) Зменшення смуги пропускання ω0 призводить до збільшення динамічних помилок і зменшення динамічних флуктуацій.

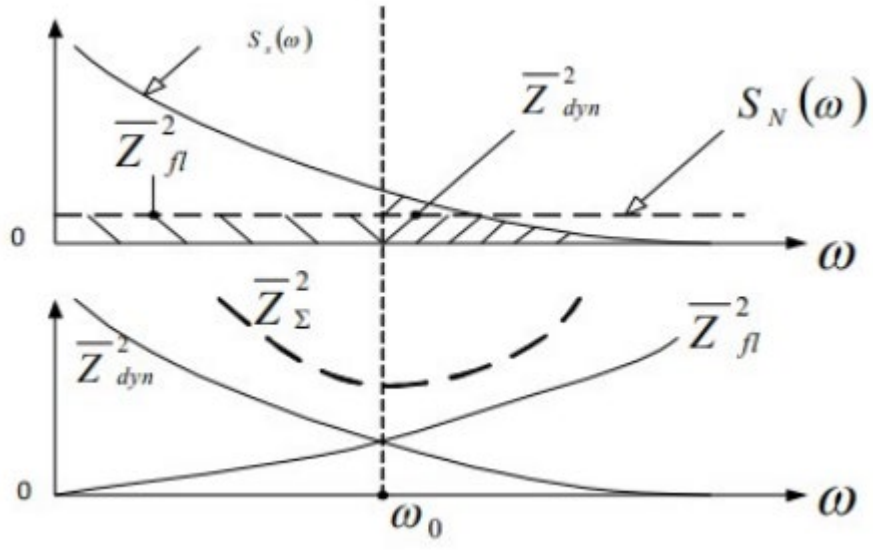

Рис. 3.5 Смуга пропускання БПЛА.

Існує оптимальна смуга ω0 opt, коли сумарна похибка буде мінімальною:

$$Z_{\sum min} \vee ¿_{\omega_0 \omega_{opt}} = Z_{dyn} + Z_{fluc} ¿$$

Для цього пітч-каналу повинна бути виконана система, що забезпечує його оптимальну смугу. Для комп'ютерного дослідження смуги пропускання БПЛА (виявлення динамічної похибки) на вхід каналу управління необхідно подати сигнал «Рампа». Тоді за допомогою ключів можна забезпечити задіяність усіх контурів. Динамічна похибка визначається різницею вхідних і вихідних функцій (рис. 3.6).

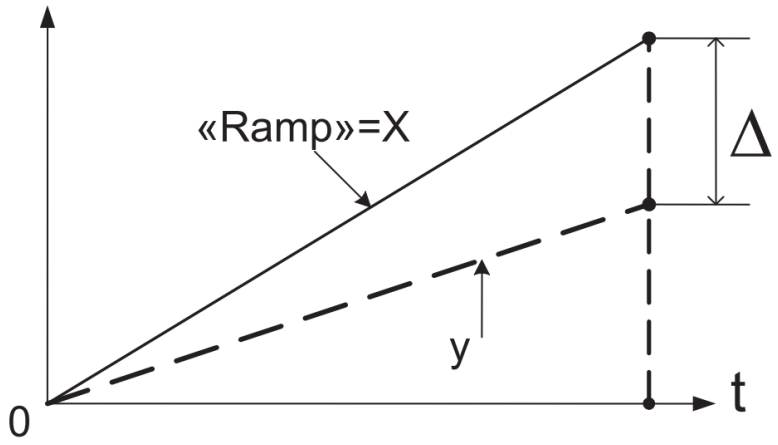

Рис. 3.6 – Динамічна похибка

3.2 Реалізація криптографічного захисту у каналах передачі даних

У якості основного мікрокомп'ютера для прототипу було обрано Raspberry Pi 3 Model B. Це рішення базувалося на попередніх дослідженнях і практичних випробуваннях, які підтвердили, що RPi 3 є достатньо потужною платформою для реалізації функціональних можливостей безпілотного літального апарата.

Ключовими факторами вибору мікрокомп'ютера стали: достатня кількість портів для підключення периферійних пристроїв, потужність, що дозволяє виконувати шифрування потоку даних разом із менш ресурсозатратними задачами, а також наявність корисних функцій, таких як вбудований Wi-Fi модуль і графічний процесор. Raspberry Pi 3 повністю відповідає цим вимогам, забезпечуючи підключення всіх необхідних компонентів, зокрема DVB-T модему, пристрою захоплення відео, порту телеметрії, контролера, RTC, GPIO-індикаторів тощо. Його процесор здатний обробляти всі задачі одночасно навіть у режимі

максимального навантаження.

Варто також відзначити, що популярність Raspberry Pi значно спрощує процес розробки програмного забезпечення. Завдяки великій кількості готових збірок операційних систем, бібліотек та інших програмних компонентів, створення робочої платформи на базі Raspbian Jessie (модифікованого Debian Jessie для RPi) із необхідними налаштуваннями займає лише кілька годин.

Для створення прототипу було обрано бюджетну FPV-камеру 1/3-inch Sony Super HAD Color CCD з максимальною роздільною здатністю 752 x 582 (PAL). Цей вибір обґрунтований тим, що камера забезпечує достатню якість зображення, зважаючи на обмеження роздільної здатності пристрою захоплення відео (720 x 576).

Для генерації відеопотоку використовується фреймворк GStreamer. Його архітектура базується на пайплайнах, які складаються з плагінів, що дозволяє створювати різноманітні конфігурації відеопотоку. Завдяки широкому спектру доступних плагінів та можливостям їх кастомізації, фреймворк забезпечує гнучкість і адаптивність. Відкритий код плагінів дозволяє додатково змінювати їхній функціонал для специфічних завдань.

Серед ключових переваг GStreamer — підтримка плагіна OpenMax (OMX), який оптимізований для Raspberry Pi 3 і ефективно використовує можливості VideoCore IV 3D. При порівнянні навантаження процесора під час кодування відео у формат H.264 за допомогою стандартного плагіна та плагіна OMX було встановлено значну перевагу останнього. У першому випадку використання відео в форматі 576i є малоефективним через високе навантаження на процесор (середнє завантаження близько 300%), тоді як застосування плагіна OMX знижує цей показник до 80%, передаючи частину обчислень VideoCore IV 3D.

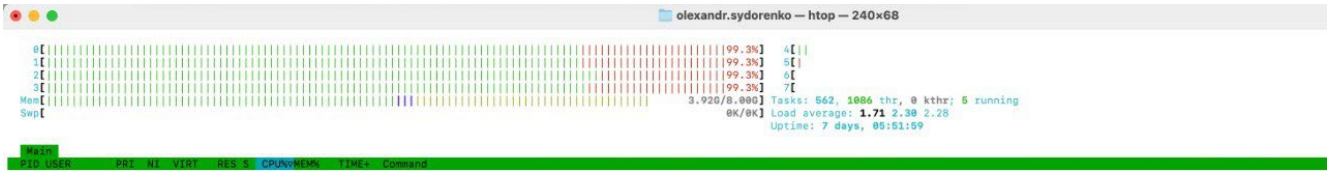

Рис. 3.7 – CPU Usage з підключеним плагіном x264

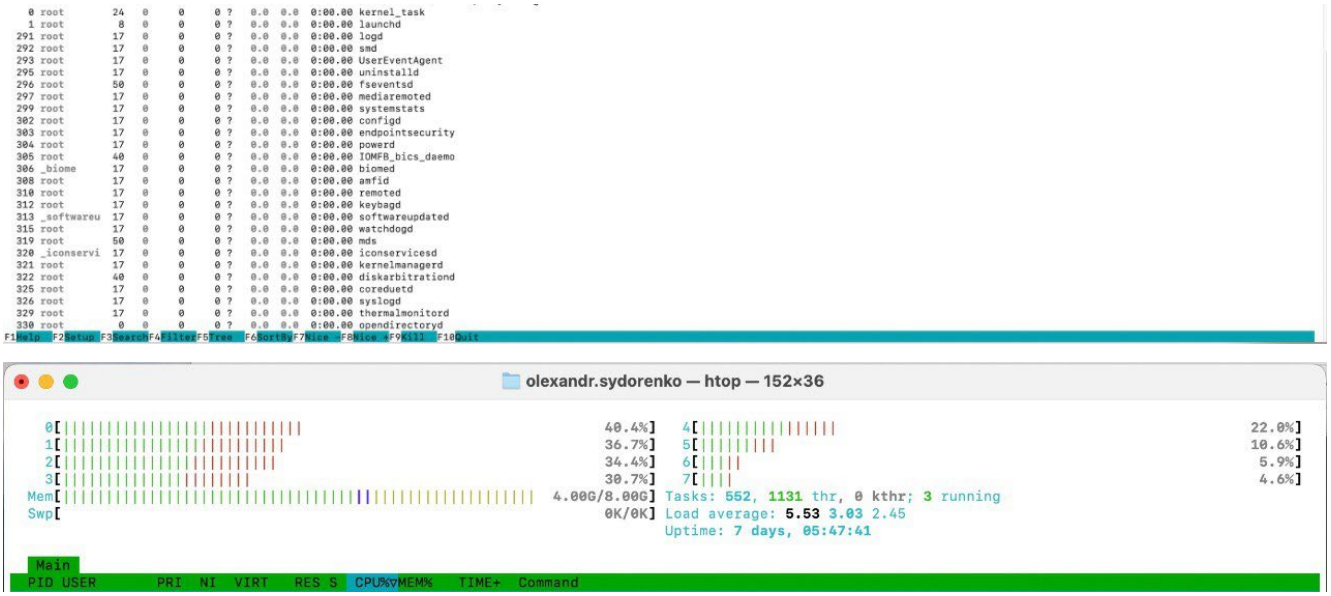

Рис. 3.8 – CPU Usage з підключеним плагіном OMX

Для організації передачі даних між наземним і повітряним модулями було обрано стандарт DVB-T, який використовується в європейських системах наземного цифрового мовлення. DVB-T забезпечує передачу єдиного транспортного потоку MPEG-TS з цифровими сервісами (мультиплексом), використовуючи модуляцію COFDM, зі швидкістю до 31 Мбіт/с.

Для забезпечення стабільного зв’язку було обрано компактний повнодуплексний передавач DVB-T, характеристики якого відповідають вимогам роботи лінії зв’язку. Зокрема, він дозволяє рознести частоти приймачів на наземному і повітряному модулях БПЛА та налаштовувати велику кількість частот для реалізації алгоритмів протидії радіоелектронним перешкодам (РЕБ).

Таблиця 3.1 Характеристики DVB-T модему

Параметр	Значення	
Полоса пропускання	Передавач	2/3/4/5/6/7/8 MHz
	Приймач	5/6/7/8 MHz
Frequency range	Передавач	50~950 MHz та 1200~1350 MHz з кроком 1KHz
	Приймач	50~950 MHz з кроком 1KHz
Вихідний рівень RF	0 dBm (108 dBuV)	
Цифрове підсилення	Діапазон: +6/-25 dB , з кроком 1 dB	

Програмна частина лінії зв’язку є центральним і найбільш складним компонентом проєкту. Вона охоплює такі процеси, як мультиплексування та демультиплексування потоку, фільтрацію пакетів, створення інтерфейсів для роботи з драйвером радіопередавача/приймача, збір статистики й взаємодію з іншими компонентами.

Для обміну повідомленнями і сигналами управління між польотним контролером і наземною станцією використовується бібліотека MavLink. Всі дані, включаючи керуючі сигнали, телеметрію, відеопотік та іншу інформацію, інтегруються в єдиний потік MPEG-TS. До пакетів додаються додаткові дані, які забезпечують контроль над передачею, підвищуючи захищеність інформації.

Внутрішній обмін повідомленнями всередині кожного з модулів здійснюється через бібліотеку LCM. Це забезпечує швидкий обмін даними з мінімальними затримками, що критично важливо для ефективності роботи системи.

Для шифрування даних у проєкті використовується стандартний алгоритм AES-128, реалізований за допомогою однієї з наявних криптографічних бібліотек. Реалізація алгоритмів захисту від підміни пакетів і протидії радіоелектронним перешкодам є важливим елементом проєкту, однак через їх конфіденційність ці

деталі не можуть бути розкриті в роботі.

Значну увагу у дослідженні приділено аналізу та розробці алгоритму синхронізації часу між наземним і повітряним модулями системи зв’язку з БПЛА. Синхронізація потрібна для двох основних задач:

1. Синхронізація часу для логування з точністю до однієї секунди.
2. Синхронна зміна радіочастот у межах алгоритму протидії перешкодам із точністю до 20 мс або більше.

Оскільки зв’язок базується на радіомодемах, затримка прийому даних може досягати 50 мс і має нерівномірний характер. Це враховується під час розробки алгоритму.

Наземний модуль отримує еталонний час через протокол NTP перед польотом, коли є доступ до мережі. Якщо мережа недоступна, для синхронізації використовується RTC (реальний годинник), хоча його точність нижча і потребує періодичних налаштувань. Еталонний час із наземного модуля використовується для синхронізації часу повітряного модуля.

Для реалізації синхронізації обрано алгоритм Крістіана, який ефективно працює в мережах з низьким навантаженням. Недоліки алгоритму вирішуються наступними способами:

1. Еталонний час забезпечується наземним модулем із підключенням до NTP або RTC.

2. Годинники синхронізуються перед польотом, коли ключові системи ще не запущені. Це запобігає можливим проблемам, якщо час буде переведено назад.

3. Початковий час встановлюється як половина середнього часу передачі між запитом і відповіддю, усередненого за декілька ітерацій. Для більш точного налаштування відправляється еталонний час із наземного модуля з подальшою перевіркою і корекцією затримки.

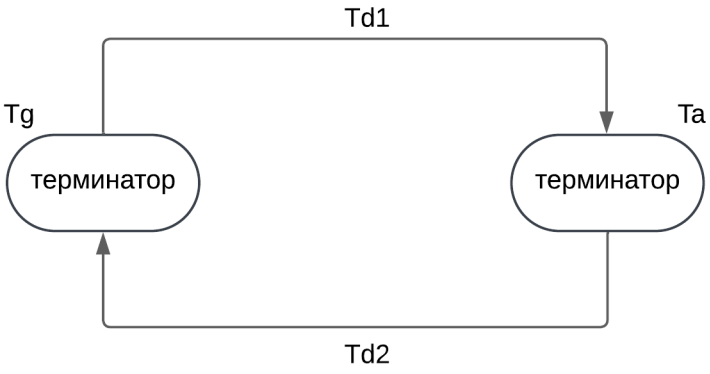

Рис. 3.9 – Зміщення за часом

Затримки передачі даних з наземного модуля на повітряний (Td1) і з повітряного на наземний (Td2) заздалегідь невідомі та можуть відрізнятися [рис. 3.3]. Однак можливо визначити затримку повного кола (Td1 + Td2) і, використовуючи алгоритм Крістіана, апроксимувати значення як Td1 = Td2 = (Td1 + Td2) / 2. Для підвищення точності виконується серія з десяти обчислень затримки повного кола, з яких обирається найменше значення, що вважається найбільш точним. На основі цієї затримки час на повітряному модулі встановлюється за формулою Ta = Tg + (Td1 + Td2) / 2.

На наступному етапі виконується корекція отриманого часу. Це здійснюється шляхом передачі таймстампів із наземного модуля на повітряний. На повітряному модулі повторюється обчислення мінімальної затримки при передачі таймстампу. Ця затримка порівнюється з поточним часовим зміщенням (визначеним як (Td1 + Td2) / 2) на наземній станції. Якщо похибка потрапляє в допустимий діапазон точності синхронізації, годинники вважаються синхронізованими. У разі перевищення похибки час коригується, зменшуючи різницю між затримками на обох модулях удвічі.

Таким чином, синхронізація досягається з точністю до половини затримки повного кола, що теоретично становить близько 30 мс. Практичні результати показали, що завдяки відносній стабільності затримок у двох напрямках похибка не перевищує 5 мс, що є достатнім для використання цього алгоритму в системі.

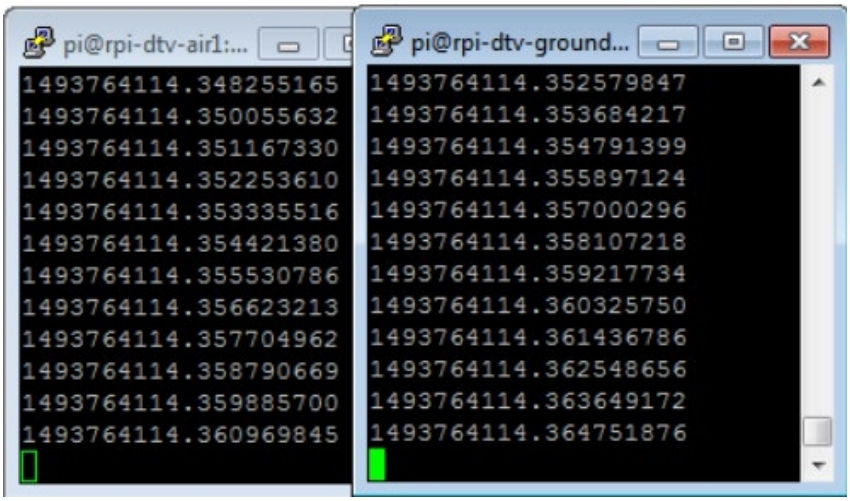

Рис. 3.10 – Синхронізація за часом

3.3 Математична модель системи захищеного вз'язку

Компоненти системи

1. Вхідні дані.

- D $= \{d_1, d_2, \ldots., d_n)$ – множина даних, що передаються через канал зв’язку.
- T_{delay} – затримка передачі даних через канал зв’язку.
- P_{error} – ймовірність втрати або спотворення пакета даних.
- $K_{encryption}$ – ключ шифрування.

2. Ресурси системи.
    - P_{proc} – обчислювальні ресурси для шифрування та дешифрування.
    - $P_{bandwidth}$ – пропускна здатність каналу зв’язку.
    - T_{proc} – час обробки одного пакета даних.
3. Цілі системи.
    - Забезпечення конфіденційності, цілісності та доступності даних під час передачі.
    - Мінімізація затримок передачі й обробки.
    - Максимізація надійності зв’язку.

Логіка передачі даних

1. Шифрування даних

Вхідні дані шифруються за допомогою алгоритму AES-128:

$$C_i = E_{Kencryption}(d_i), i = 1, 2, \ldots., n \quad (3.6)$$

де C_i — зашифрований пакет даних, $E_{Kencryption}$ — функція шифрування з використанням ключа $Kencryption$.

2. Передача даних через канал

Затримка передачі одного пакета визначається як:

$$T_{total} = T_{delay} + T_{proc} \quad (3.7)$$

де T_{delay} — затримка в каналі, T_{proc} — час обробки пакета.

3. Дешифрування даних

Отриманий пакет розшифровується на приймальній стороні:

$$d_i = D_{Kencryption}(C_i), i = 1, 2, \ldots., n \quad (3.8)$$

де $D_{Kencryption}$ — функція дешифрування.

4. Оцінка надійності передачі

Надійність системи визначається через ймовірність успішної доставки пакетів:

$$R_{success} = (1 - P_{error})^n \quad (3.9)$$

Синхронізація часу

1. Затримка передачі

Середня затримка повного циклу визначається як:

$$T_{cycle} = \frac{T_{d1}+T_{d2}}{2} \quad (3.10)$$

де T_{d1} і T_{d2} — затримки передачі даних в обох напрямках.

2. Корекція часу

Час на повітряному модулі коригується за формулою:

$$T_a = T_g + T_{cycle} \quad (3.11)$$

де T_a — синхронізований час на повітряному модулі, T_g — еталонний час на наземному модулі.

Оптимізаційна мета.

Мінімізувати сумарну затримку передачі та обробки:

$$min(T_{total})$$

за умови збереження конфіденційності та надійності передачі:

$$R_{success} \geq R_{threshold}$$

де $R_{threshold}$ — мінімально допустимий рівень надійності.

Переваги моделі

1) Висока ефективність у мережах із невеликими затримками та стабільною пропускною здатністю.
2) Забезпечення синхронізації часу для критичних задач, таких як протидія радіоелектронним перешкодам.
3) Можливість адаптації до різних сценаріїв завдяки модульності та масштабованості.

Висновок до розділу 3

У цьому розділі розроблено систему захищеного зв’язку для безпілотних літальних апаратів (БПЛА), що забезпечує надійний канал управління з використанням сучасних криптографічних методів. Розглянуто основні аспекти моделювання процесу створення захищеного каналу управління БПЛА, зокрема його вплив на механіку польоту, що дозволяє забезпечити стабільність і ефективність управління апаратом навіть у складних умовах.

Проаналізовано реалізацію криптографічного захисту в каналах передачі даних, що включає методи шифрування, аутентифікації та цілісності даних для запобігання несанкціонованому доступу і забезпечення конфіденційності комунікацій між наземними станціями та БПЛА. Особлива увага приділена вибору оптимальних криптографічних алгоритмів для забезпечення високої швидкості передачі даних без втрат в ефективності зв’язку.

Продемонстровано математичну модель системи захищеного зв'язку, що враховує різноманітні параметри впливу, такі як зсуви в частотному спектрі, затримки сигналів, а також фактори зовнішнього середовища. Ця модель дозволяє оцінити вплив захисту на загальну ефективність системи управління БПЛА, що є важливим для забезпечення її надійності та стійкості до атак.

ВИСНОВКИ

У розділі було проведено детальний аналіз сучасних систем зв’язку безпілотних літальних апаратів (БПЛА), визначено їхні особливості, класифікацію та актуальні проблеми безпеки.

Розглянуто різновиди БПЛА залежно від їхніх характеристик і призначення, що дозволило виділити основні вимоги до систем зв’язку для кожного типу дронів. Виявлено, що специфіка зв’язку залежить від дальності польоту, джерела енергії, сфери використання та потреб у захищеності каналів зв’язку.

Проаналізовано архітектуру систем зв’язку БПЛА, включаючи прямий радіозв’язок, супутникові канали, мобільні мережі та інші технології. Було підкреслено значення стійкості каналів зв’язку до перешкод і залежність функціонування дронів від якості та стабільності сигналу. Особливу увагу приділено ролі сучасних протоколів передачі даних і впливу на них різних зовнішніх факторів.

Висвітлено сучасні загрози та вразливості систем зв’язку БПЛА, зокрема перехоплення даних, спуфінг, глушіння сигналів та DoS-атаки. Було представлено реальні приклади кібератак на дрони, які підтверджують актуальність проблеми. Крім того, було наголошено на важливості використання криптографічних методів і інших засобів захисту для мінімізації ризиків.

Таким чином, проведений аналіз довів, що для забезпечення надійності та безпеки систем зв’язку БПЛА необхідно впроваджувати сучасні технології, спрямовані на підвищення захисту інформації, стійкості до перешкод і загроз, а також оптимізацію архітектури зв’язку. Ці висновки слугують основою для подальшої розробки системи захищеного зв’язку, що буде розглянута в наступних розділах.

Розглянуто основні принципи криптографічного захисту даних, зокрема механізми симетричного та асиметричного шифрування, а також їх особливості у контексті забезпечення конфіденційності, цілісності та автентичності інформації. Симетричне шифрування, представлене алгоритмами типу AES, продемонструвало

свою високу ефективність у швидкості обробки даних, тоді як асиметричні алгоритми, як-от RSA та ECC, забезпечують підвищену безпеку для автентифікації та обміну ключами. Проаналізовано використання криптографічних алгоритмів для захисту каналів зв’язку.

Продемонстровано, як різні алгоритми забезпечують стійкість до атак, таких як атаки «людина посередині» (MITM) та криптоаналітичні методи. Особливу увагу приділено аналізу ефективності алгоритмів у реальних умовах, включаючи швидкість обробки, стійкість до зламу та адаптацію до обмежених ресурсів. Цей аналіз дозволив визначити, які криптографічні методи є найбільш оптимальними для конкретних застосувань, таких як захист мобільних пристроїв або обмін даними в мережах з низькою затримкою.

Розроблено детальну оцінку продуктивності криптографічних алгоритмів у різних сценаріях використання. Представлено порівняння алгоритмів за ключовими параметрами, такими як енергоспоживання, час виконання криптографічних операцій та швидкість шифрування. Зокрема, було визначено, що алгоритми на основі еліптичних кривих (ECC) є більш енергоефективними та адаптивними для пристроїв з обмеженими обчислювальними ресурсами порівняно з RSA.

ПЕРЕЛІК ПОСИЛАНЬ

1. How to choose FPV camera for drones. URL: https://oscarliang.com/best-fpv-camera-quadcopter/ (дата звернення: 15.10.2024).

2. Трунов О. М. Розвиток методів та засобів створення аск глибоководними технологічними комплексами: автореф. дис. … д-ра техн. наук: 05.13.07 – автоматизація процесів керування / Чорном нац. ун-т ім. Петра Могили. Херсон, 2017. 44 с.

3. Тимочко О. І., Голубничий Д. Ю., Третяк В. Ф. та ін. Класифікація безпілотних літальних апаратів. Системи озброєння і військова техніка. 2007. Вип. 1 (9). С. 61–66. URL: http://www.hups.mil.gov.ua/periodic-app/article/1045/soivt_2007_1_19.pdf. (дата звернення: 16.10.2024).

4. Тимочко О. І., Голубничий Д. Ю., Третяк В. Ф. та ін. Класифікація безпілотних літальних апаратів. Системи озброєння і військова техніка. 2007. Вип. 1 (9). С. 61–66. URL: http://www.hups.mil.gov.ua/periodic-app/article/1045/soivt_2007_1_19.pdf. (дата звернення: 18.10.2024).

5. Трунов О. М. Розвиток методів та засобів створення аск глибоководними технологічними комплексами: автореф. дис. д-ра техн. наук: 05.13.07 – автоматизація процесів керування / Чорном нац. ун-т ім. Петра Могили. Херсон, 2017. 44 с.

6. Фісун М. Т., Журавська І. М., Горбань Г. В. Використання OLAP-технології для аналізу мережевого трафіку засобами об’єктної СКБД. Комп’ютерні системи та мережеві технології (CSNT’2012) / Нац. авіац. ун-т.: тези доп. V Міжнар. наук.-техн. конф. Київ, 13–15 черв. 2012 р. С. 129.

7. Рудницький В. М., Костирка О. В. Стійке стеганоперетворення в просторовій області зображення-контейнера. Інформатика та математичні методи в моделюванні. 2013. Вип. 3, № 4. С. 353–360.

8. Румянков Д. І., Журавська І. М. Проектування системи керування безпілотним літальним пристроєм на основі мікроконтролерів Atmega на базі Arduino. Інтелектуальні інформаційні системи – 2017 / Чорном. нац. ун-т ім. Петра

Могили: тези доп. Всеукр. наук.-практ. конф., Миколаїв, 15–17 лют. 2017 р. С. 126–128.

9. Харченко О.В. Класифікація та тенденції створення безпілотних літальних апаратів військового призначення / О.В. Харченко, В.В. Кулєшин, Ю.В. Коцуренко // Наука і оборона. – 2015. – № 6 – С. 47-54

10. В. Фурашев. Питання законодавчого визначення понятійнокатегоріального апарату у сфері інформаційної безпеки // “Інформація і право”. – № 1(4)/2012.

11. Державна авіаційна служба України. Тимчасовий порядок використання повітряного простору України. 2018.

12. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К.: НІСД, 2011.

13. О.І. Тимочко, Д.Ю. Голубничий, В.Ф. Третяк, І.В. Рубан. Харківський університет Повітряних Сил ім. Івана Кожедуба, Харків. Класифікація літальних апаратів. 2007.

14. Петров В.Ф., Барунін А.А., Терентьєв А.І. Модель системи автоматичного управління безпілотним літальним апаратом. Известия Тульського державного університету. Технічні науки, 2014. № 12-2

15. Полинкін А.В. Дослідження характеристик радіоканалу зв'язку з безпілотними літальними апаратами. 2013.

16. Семенова Л.Л. Сучасні методи навігації безпілотних літальних апаратів. 2015. 30. Скляр Б. Цифрова зв'язок. Теоретичні основи і практичне застосування, Изд. 2-е, испр.: Пер. з англ. / Б. Скляр. - М.: Видавничий дім «Вільямс», 2003.

17. Явіся В.С. Спосіб забезпечення високошвидкісної передачі даних безпілотними літальними апаратами // Одинадцята міжнародна науковотехнічна конференція „Проблеми телекомунікацій”. Матеріали конференції. - К.: КПІ ім. І. Сікорського. 2017. С. 362 – 365.

18. Явіся В.С., Вакуленко О.В. Особливості побудови телекомунікаційних мереж на базі БПЛА для передачі інформації на великі відстані // IX Науково-

практична конференція „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в АТО". Збірник тез. - К.: ВІТІ. 2016. С. 208 – 209.

19. Indesteege S., Keller N., Dunkelman O., Biham E., Preneel B. A practical attack on KeeLoq // Smart N. (eds) Advances in Cryptology – EUROCRYPT 2008. Springer, 2008. Lecture Notes in Computer Science. V. 4965. P. 1–18.

20. Zhuravska I., Kulakovska I., Musiyenko M. Development of a method for determining the area of operation of unmanned vehicles formation by using the graph theory. Eastern-European Journal of Enterprise Technologies. 2018. Vol. 2, No. 3 (92). P. 4–12. DOI: 10.15587/1729-4061.2018.128745.

21. Courtois N.T., Bard G.V., Wagner D. (2008) Algebraic and slide attacks on KeeLoq//. In: Nyberg K. (eds) Fast Software Encryption. FSE 2008. Springer, 2008. Lecture Notes in Computer Science. V. 5086. P. 97–115.

22. Khan A. Hacking the Drones // Open Web Application Security Project. 2016. – URL: https://owasp.org/www-chapterlondon/assets/slides/ OWASP201604_Drones.pdf (дата звернення: 26.10.2024).

23. Rodday N. Hacking a Professional Drone // Black Hat Asia 2016. 2016. – URL: https://www.blackhat.com/docs/asia16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf (дата звернення: 10.11.2024).

24. Petrovsky O. Attack on the drones: security vulnerabilities of unmanned aerial vehicles // 25th Virus Bulletin International Conference. 2015. – URL: https://www.virusbulletin.com/conference/vb2015/abstracts/attack-drones-securityvulnerabilities-unmanned-aerial-vehicles (дата звернення: 12.11.2024).

25. Whyte S. Analysis of RF remote security using software defined radio. Carleton University: COMP 4905: Honours Project. 2013. 65 p.

26. Carr E. Unmanned Aerial Vehicles: Examining the Safety, Security, Privacy and Regulatory Issues of Integration into U.S. Airspace / E. Carr – 2012. – с. 15. – (Safety Issues) (Security Issues) (Privacy Issues)

27. Правила повітряної експлуатації безпілотних повітряних суден в Україні (концепція) / Р. Байдуж: презентація; опубл. 6.10.2017. URL:

https://www.slideshare.net/ SAAU2017/ss-80646310. (дата звернення: 26.11.2024).

28. Zhuravska I. M., Popel M. I. Automation of pharmaceutical warehouse using groups robots with remote climate control and video surveillance. Science and Innovation in the XXI century: Collection of Conference Materials of International Scientific-Practical Conference, London, the United Kingdom, 11–12 Dec., 2014. P. 30–32. DOI: 10.5281/zenodo.14090

29. Tokyo's solution to rogue drones? Drones with nets. URL: https://www.engadget.com/2015/12/11/tokyo-drone-net/ – (дата звернення: 26.11.2024).

30. Network Time Protocol. URL: https://fr.wikipedia.org/wiki/Network_Time_Protocol (дата звернення: 28.11.2024).

31. Advanced Encryption Standard. URL: https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard (дата звернення: 29.11.2024).

32. Unmanned Aircraft Systems (UAS) Roadmap / USA: Office of the Secretary of Defense. – 2005. – c. 33 – (Joint Land Attack Elevated Netted Sensor).

33. Overview of UCLA MinuteMan-Project. URL: www.icsl.ucla.edu (дата звернення: 29.11.2024).

34. Бойко А. Blighter AUDS // RoboTrends, 2015. – URL: http://robotrends.ru/pub/1542/bespilotnik-v-polete-ostanovit-blighter-auds (дата звернення: 30.11.2024).

35. Сальник Ю.П. Аналіз технічних характеристик і можливостей безпілотних авіаційних комплексів оперативно-тактичного та тактичного радіуса дії армій розвинених країн / Ю.П. Сальник, І.В. Матала // Військовотехнічний зб. – 2013. – № 7 – С. 70-74

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ