УДК 004.056

Палій О.М.

ЗАХИСТ ДАНИХ У РОЗВІДУВАЛЬНИХ ДРОНАХ: ШИФРУВАННЯ ТА БЕЗПЕЧНЕ ПЕРЕДАВАННЯ

Анотація

У статті розглянуто проблему захисту даних, що передаються та зберігаються розвідувальними безпілотними літальними апаратами (БПЛА). Обґрунтовано важливість шифрування інформації та використання безпечних протоколів зв'язку для запобігання несанкціонованому перехопленню розвідданих. Проведено аналіз основних методів шифрування, що застосовуються у дронах, та протоколів безпечного передавання даних. Розглянуто потенційні ризики кібератак на канали зв'язку дронів (перехоплення, спуфінг, втручання), а також надано порівняльний аналіз популярних алгоритмів шифрування з точки зору їх стійкості та продуктивності в умовах обмежених ресурсів БПЛА. На основі аналізу запропоновано рекомендації щодо впровадження сучасних засобів криптографічного захисту в розвідувальних дронах з урахуванням галузевих стандартів та перспектив розвитку (зокрема, постквантових методів). Зроблено висновки про необхідність комплексного підходу до захисту даних розвідувальних дронів для забезпечення конфіденційності, цілісності та доступності критичної інформації.

Ключові слова: *розвідувальні дрони, захист даних, шифрування, безпечна передача, криптографічні протоколи, ризики, конфіденційність.*

Abstract

The paper addresses the issue of data protection in reconnaissance unmanned aerial vehicles (UAVs) by focusing on encryption and secure data transmission. It substantiates the importance of encrypting information and using secure communication protocols to prevent unauthorized interception of reconnaissance data. The study analyzes key encryption methods used in drones and secure data transmission protocols. Potential cyber threats to drone communication channels (interception, spoofing, interference) are examined, as well as a comparative analysis of popular encryption algorithms in terms of their security strength and performance under the resource constraints of UAVs. Based on the analysis, recommendations are provided for implementing state-of-the-art cryptographic protection in reconnaissance drones, taking into account industry standards and future developments (including post-quantum methods). Conclusions emphasize the need for a comprehensive approach to data security in reconnaissance drones to ensure the confidentiality, integrity, and availability of critical information.

Key words: *reconnaissance drones, data protection, encryption, secure transmission, cryptographic protocols, risks, confidentiality.*

Вступ

Сучасні розвідувальні безпілотні літальні апарати широко застосовуються у військовій сфері, правоохоронних органах та для цивільного моніторингу. Вони збирають і передають великий обсяг чутливої інформації (відео, фото, координати тощо), яка потребує надійного захисту. З поширенням дронів зростає і кількість потенційних кібератак на них – зловмисники можуть намагатися перехопити канал зв'язку, отримати несанкціонований доступ до даних або навіть втрутитися в управління апаратом. Відомо, що дрони є вразливими до глушіння сигналу, підробки (spoofing) навігаційних даних та перехоплення телеметрії. Особливо для розвідувальних БПЛА, які працюють з секретними відомостями, компрометація переданих даних може призвести до серйозних наслідків – від зриву операцій до міжнародних інцидентів. Таким чином, захист інформації у каналах зв'язку дронів є критично важливим завданням [1]. Одним з головних підходів до вирішення цієї проблеми є використання криптографії: шифрування даних, автентифікація повідомлень та надійне керування ключами шифрування. У цьому дослідженні проаналізовано сучасні методи шифрування, що можуть застосовуватися на борту розвідувальних дронів, протоколи безпечної передачі даних, а також пов'язані ризики. Наведено

порівняння різних криптоалгоритмів та надано рекомендації щодо впровадження найкращих практик для забезпечення конфіденційності та цілісності даних розвідки.

Методи шифрування у розвідувальних дронах

Основою захисту даних є сильні криптографічні алгоритми, впроваджені як в бортові системи зберігання, так і в канали передачі даних. У розвідувальних дронах зазвичай використовується симетричне шифрування для захисту переданих масивів даних (відеопотоки, телеметрія), оскільки симетричні алгоритми забезпечують високу швидкість шифрування/дешифрування при обмежених обчислювальних ресурсах. Галузевим стандартом де-факто є алгоритм AES (Advanced Encryption Standard) із довжиною ключа 256 біт, який вважається одним із найнадійніших сучасних шифрів. Наприклад, провідні виробники дронів впроваджують AES-256 для захисту радіоканалу: у дронах DJI технологія OcuSync шифрує телеметрію та відео AES-256, що запобігає перехопленню даних та атакам «людина посередині» [2]. Також AES-256 використовується для шифрування збережених на борту файлів (наприклад, дані на SD-карті) з метою захисту інформації у випадку захоплення пристрою. Окрім AES, в деяких системах застосовуються альтернативні симетричні алгоритми, такі як ChaCha20, які забезпечують співставний рівень безпеки. Важливо відмітити, що симетричне шифрування вимагає попереднього обміну ключами між дроном і наземною станцією. Для цієї мети використовуються методи асиметричної криптографії (шифрування з відкритим ключем). Зокрема, протокол обміну ключами ECDH (Elliptic Curve Diffie–Hellman) дозволяє двом сторонам встановити спільний секретний ключ по незахищеному каналу зв'язку, використовуючи криптографію на еліптичних кривих. Такий підхід забезпечує конфіденційність ключа шифрування навіть за умови, що зловмисник прослуховує канал. Надалі цей сесійний ключ використовується для швидкого симетричного шифрування даних. Додатково, для гарантування цілісності та автентичності даних застосовуються криптографічні геш-функції та коди автентифікації повідомлень (MAC/HMAC). У комплексі, комбінація симетричного шифрування (для конфіденційності) та криптографічних підписів або MAC (для автентичності) формує основу захисту даних у БПЛА [2].

Сучасні стандарти безпеки вимагають, щоб кожен розвідувальний дрон мав унікальні криптографічні ключі, якими він обмінюється з центром управління. У військових системах практикується виділення пар ключів для кожного дрона, де приватний ключ зберігається тільки у авторизованого персоналу на наземній станції. Такий розподіл, разом з використанням надійних алгоритмів, гарантує, що дані, зібрані дроном, залишаться зашифрованими і захищеними від сторонніх осіб навіть у разі втрати або компрометації самого апарату.

Протоколи безпечного передавання даних

Окрім вибору алгоритму шифрування, критичним є правильне впровадження протоколів захисту даних при передачі від дрона до наземної станції або між дронами. Існують різні рівні захисту каналу зв'язку. На рівні бездротового з'єднання (Wi-Fi, радіомодем) слід застосовувати протоколи з шифруванням. Якщо дрон використовує Wi-Fi для передачі даних, рекомендується увімкнути найсильніший доступний режим безпеки, наприклад WPA2 або WPA3 з шифруванням AES [3]. Необхідно встановлювати складні паролі/ключі до мережі та регулярно їх змінювати, уникаючи предбачуваних назв мережі (SSID), що могли б видати модель дрона або відомство. У випадку передачі даних через інтернет-протоколи, варто використовувати транспортні шифровані протоколи (VPN, TLS/SSL). Якщо програмно-апаратний комплекс дрона підтримує протокол TLS, його слід ввімкнути на максимальний підтримуваний рівень (наприклад TLS 1.3) для захисту телеметрії, відеопотоку та команд управління. У військових та урядових застосуваннях часто використовуються власні закриті протоколи зв'язку, що мають вбудоване шифрування. Наприклад, протоколи сімейства STANAG для БПЛА передбачають захищене передавання команд та даних, а виробники можуть додатково накладати поверх стандарту свої шифровані канали. Відомо, що компанія DJI реалізувала власний протокол OcuSync, який не лише використовує AES-256, але й пройшов сертифікацію криптомодулів за стандартом FIPS 140-2 рівня 1 [4]. Це означає, що реалізація шифрування відповідає урядовим вимогам до криптографічних модулів, що підвищує довіру до безпеки рішення. З іншого боку, деякі відкриті протоколи, які історично застосовувались для зв'язку з дронами, не забезпечують конфіденційності. Зокрема, популярний протокол телеметрії MAVLink (широко використовуваний в любительських та деяких комерційних

дронах) підтримує тільки криптографічний підпис повідомлень (автентифікацію) і не здійснює їх шифрування.

Отже, якщо зловмисник перехопить трафік MAVLink, він зможе прочитати передані дані (напряму не втручаючись, але отримуючи розвідінформацію). Це демонструє важливість використання саме шифрування, а не лише аутентифікації, для захисту каналу зв'язку. Для посилення безпеки відкритих протоколів були запропоновані розширення: існують модифіковані версії MAVLink (наприклад, MAVLink Sec або шифрування на рівні транспортного потоку) з використанням алгоритмів AES або ChaCha20, що додають шифрування без значного впливу на пропускну здатність. Крім того, перспективним напрямом є створення нових спеціалізованих протоколів зв'язку для дронів. Дослідники пропонують протоколи, які включають взаємну автентифікацію дронів і станцій, розподіл групових ключів для рою дронів (FANET), а також механізми забезпечення прямої та зворотної секретності сеансів (perfect forward/backward secrecy). Наприклад, один із підходів передбачає встановлення захищеного каналу між дроном і станцією з використанням подвійного протоколу: спочатку виконується обмін ключами з автентифікацією (на основі сертифікатів або безсертифікатних схем), потім дані передаються в зашифрованому вигляді з оновленням сеансових ключів для забезпечення perfect forward secrecy (неможливості розшифрувати раніше перехоплені дані навіть у разі компрометації поточного ключа).

Таким чином, правильне проектування протоколу безпечного передавання даних є не менш важливим, ніж вибір алгоритму, і має враховувати усі аспекти: шифрування для конфіденційності, підписи або MAC для цілісності, взаємну аутентифікацію та захист від повторних атак (через використання одноразових чисел/нонсів у сеансах).

Аналіз ризиків

Без впровадження належних засобів захисту, канали зв'язку розвідувального дрона можуть стати ціллю для противника. Одним із основних ризиків є прослуховування та перехоплення даних: зловмисник, оснащений відповідним радіообладнанням, може перехопити незашифрований потік відео або телеметрії, отримавши тим самим доступ до розвідданих. Якщо дані передаються у відкритому вигляді, противник легко їх прочитає. Приклади реальних інцидентів свідчать, що уразливі безпілотники можуть бути «перехоплені» електронними засобами; зокрема, відомі випадки перехоплення відеопотоків з дронів, що не були належно зашифровані. Несанкціонований доступ та крадіжка даних є ризиком не лише при передачі, а й при зберіганні: якщо розвідувальний дрон впаде або буде захоплений противником, вся записана на ньому інформація (фото, журнали польотів) потрапить до рук ворога, якщо вона не зашифрована на носіях. Підробка даних та атака «людина посередині» (MITM) – ще одна категорія загроз. Зловмисник, що інтегрувався у канал зв'язку, може не тільки читати, а й змінювати дані або команди [5]. Наприклад, підмінивши координати або відеосигнал, він може дезінформувати операторів. Відсутність криптографічного захисту і автентифікації відкриває шлях для таких атак. Спуфінг і втручання в управління: якщо канал управління дроном не захищено, противник може послати власні команди (наприклад, посадити дрон чи відключити камери) або обманути навігаційну систему (GPS-спуфінг). Належна автентифікація команд і шифрування унеможливлюють обробку дроном неправомірних команд. Відмова в обслуговуванні (DoS) через радіоелектронне придушення – це окремий ризик, якого шифрування прямо не запобігає (глушіння можна здійснювати незалежно від шифрування). Проте застосування деяких захищених протоколів (з частотним перескакуванням, перевіркою послідовності пакетів) може ускладнити реалізацію деяких видів атак на доступність. Компрометація криптографічних ключів є внутрішнім ризиком самої системи захисту: якщо ключ шифрування стане відомим стороннім (через витік або криптоаналітичний злам занадто слабкого алгоритму), то всі перехоплені дані легко розшифровуються. Тому потрібно використовувати стійкі алгоритми та достатню довжину ключів.

На щастя, сучасні алгоритми на кшталт AES-256 наразі не зламані і при правильному використанні забезпечують високий рівень безпеки [3]. Практика показує, що застосування шифрування значно підвищує захищеність БПЛА: так, шифрований канал унеможливив випадки перехоплення або викрадення дронів, які раніше були можливі при незашифрованому зв'язку. Якщо навіть сам дрон буде скомпрометовано чи збито, дані на ньому залишаться недоступними для противника за умови їх шифрування на носіях. Іншими словами, криптографія забезпечує конфіденційність (чужі не прочитають розвіддані), цілісність (дані не можуть бути непомітно змінені) та автентичність (гарантія, що дані та

команди надходять від свого дрона, а не від нападника). Відсутність хоча б одного з цих компонентів створює лазівку для атак. Наприклад, якщо є лише автентифікація без шифрування (як у згаданому MAVLink 2), конфіденційність не забезпечується. Якщо є шифрування без автентифікації, можливі активні атаки (підміна даних). Таким чином, комплексний підхід до захисту потрібен для нейтралізації широкого спектру ризиків.

Порівняльний аналіз методів шифрування

Існує багато криптографічних алгоритмів, але не всі однаково придатні для використання на борту дрона. Порівняння методів шифрування варто проводити за кількома критеріями: рівень безпеки (стійкість до зламу), вимоги до обчислювальних ресурсів (процесора, пам'яті, енергоспоживання) та швидкодія, особливо при передачі потокових даних (відео в реальному часі). Блочні шифри такі як AES, Serpent, Twofish тощо забезпечують високий рівень безпеки; серед них AES-256 визнаний міжнародним стандартом і широко використовується, у тому числі в оборонних системах. Його перевагою є наявність апаратних реалізацій і оптимізацій – багато сучасних процесорів мають вбудовані інструкції для прискорення AES, що робить шифрування дуже швидким з мінімальним впливом на продуктивність і затримки. Дослідження показують, що AES може ефективно працювати навіть на мікроконтролерах за умови наявності щонайменше ~0.5 КБ пам'яті, а за швидкодією випереджає більшість альтернатив. Натомість легковагові алгоритми (lightweight cryptography), розроблені спеціально для пристроїв з обмеженими ресурсами, можуть мати менший розмір коду та менші вимоги до пам'яті [6].

Прикладом є алгоритм ASCON – один з нових легких шифрів, стандартизованих NIST. Випробування показали, що ASCON має продуктивність, порівняну з AES, але при цьому менший об'єм коду та пам'яті, що робить його привабливим для найменших бортових систем. Таким чином, у дронах з дуже слабким апаратним забезпеченням (наприклад, крихітні розвідпристрої) легковагові шифри можуть бути вигідні, хоча на потужніших платформах AES також працює ефективно. Потокові шифри (напр. ChaCha20, RC4) зручні для шифрування потокових даних і можуть мати переваги на певних платформах без апаратного AES. Наприклад, ChaCha20 демонструє високу швидкість на процесорах, що не мають прискорювачів AES, і тому його використовують у деяких протоколах (TLS/SSL) як альтернативу AES. В плані стійкості ChaCha20 і AES-256 вважаються еквівалентно надійними при правильній реалізації. Асиметричні алгоритми (RSA, ECDSA, ECDH) слугують переважно для встановлення секретів та цифрового підпису, оскільки вони на кілька порядків повільніші [7]. RSA з ключем 2048 біт або еліптичні криві (наприклад, Curve25519) забезпечують високий рівень безпеки для обміну ключами та автентифікації, але не підходять для шифрування великих масивів даних у реальному часі через значне навантаження. Тому на практиці асиметричні методи завжди поєднуються з симетричними: спершу здійснюється обмін ключами (RSA/ECC), а потім дані шифруються симетрично. Стійкість алгоритмів. На сьогодні AES і широко використовувані асиметричні схеми (RSA/ECC) вважаються криптостійкими проти відомих атак з класичними обчислювальними можливостями. Втім, із розвитком квантових обчислень постає питання їх довгострокової стійкості. Наприклад, великі квантові комп'ютери потенційно зможуть зламати RSA та ECC через алгоритм Шора. AES-256 натомість вважається стійким навіть проти квантового зламу (алгоритм Гровера дає лише квадратичний виграш, що означає ефективну довжину ключа ~128 біт, чого все ще достатньо). Тому вже сьогодні обговорюється впровадження постквантових алгоритмів шифрування і підпису. NIST у 2022–2024 роках провів конкурс PQC (Post-Quantum Cryptography) і стандартизував перші алгоритми, рекомендуючи поступово переходити до них у критичних системах.

У перспективі розвідувальні дрони можуть отримати оновлення протоколів з використанням постквантових схем для захисту від майбутніх загроз. Порівняльні характеристики. Узагальнюючи, для більшості застосувань наразі оптимальним вибором є AES-256 як основний шифр завдяки балансу швидкодії та надійності. Легковагові альтернативи можуть використовуватися у спеціальних випадках (дуже слабкий пристрій, де навіть реалізація AES утруднена). Важливо використовувати стандартні, добре перевірені алгоритми та протоколи, оскільки "власні" нестандартизовані методи часто містять приховані вразливості. Також слід регулярно оновлювати прошивку дронів, щоб виправляти знайдені уразливості в реалізаціях криптографії [3].

Рекомендації щодо впровадження

На основі проведеного аналізу можна сформулювати низку рекомендацій для забезпечення максимального захисту даних у розвідувальних дронах:

1. Використання сучасних перевірених алгоритмів. Рекомендується впроваджувати шифрування AES-256 для всіх конфіденційних даних, що передаються і зберігаються на дроні. Цей алгоритм відповідає міжнародним стандартам безпеки і застосовується провідними виробниками дронів. Для обміну ключами та цифрового підпису слід застосовувати алгоритми на еліптичних кривих (ECDH, ECDSA), які забезпечують короткі ключі та високу швидкість порівняно з класичним RSA.
2. Повний захист даних у транзиті та на зберіганні. Дані повинні бути зашифровані як під час передачі (по радіоканалу), так і в стані спокою на борту дрона. Реалізація шифрування "на льоту" не має надто впливати на роботу; для цього варто використовувати апаратне прискорення (крипточіпи або інструкції CPU) та оптимізовані реалізації.
3. Надійне керування ключами. Потрібно забезпечити генерацію криптографічних ключів із достатньою ентропією та їх захищене зберігання. Ключі не повинні бути прошиті у відкритому вигляді в програмному забезпеченні дрона. Краще реалізувати схему, коли основні ключі зберігаються лише на наземній станції, а дрон отримує сесійні ключі перед вильотом. Необхідно регулярно змінювати (ротувати) ключі, особливо після завершення місії або при найменшій підозрі на компрометацію. Паролі та ключі доступу до каналів зв'язку повинні бути складними та випадковими, уникати заводських налаштувань.
4. Аутентифікація і цілісність. Окрім шифрування, протокол зв'язку має гарантувати, що обмін даними відбувається лише між довіреними сторонами. Для цього слід використовувати цифрові підписи або MAC для кожного повідомлення. Наприклад, можливе впровадження електронного підпису наземної станції на командах управління і підпису дрона на телеметричних повідомленнях. Це запобігатиме сторонньому втручанню та спуфінгу команд.
5. Захист від компрометації та реагування. Система повинна бути стійкою до захоплення дрона: збережені ключі та дані мають автоматично знищуватися або принаймні бути надійно зашифрованими (можливо, з використанням апаратного модуля TPM на дроні). Пропонується реалізувати механізм аварійного видалення даних на борту при втраті зв'язку або при команді з центру, щоб запобігти аналізу захопленого пристрою. Такі підходи досліджуються (наприклад, використання хеш-ланцюжків і таймерів для ініціювання видалення) і можуть суттєво підвищити рівень захисту на випадок втрати дрона.
6. Дотримання стандартів та сертифікація. Рекомендується дотримуватись галузевих стандартів безпеки. Наприклад, керуватися настановами NIST щодо шифрування і використання перевірених криптобібліотек. Корисно, щоб використовувані рішення проходили незалежну оцінку, як-от сертифікацію FIPS 140-2 для криптографічних модулів. Це підтвердить, що реалізація шифрування відповідає встановленим критеріям безпеки.
7. Перспективні заходи. Плануючи довгостроково, варто враховувати появу квантових обчислювальних технологій. Організації, відповідальні за безпеку, вже зараз рекомендують поступово впроваджувати постквантові алгоритми шифрування там, де потрібна максимальна стійкість на роки вперед. Тому в перспективі доцільно закласти можливість оновлення прошивки дронів із підтримкою постквантових схем (наприклад, алгоритму обміну ключами CRYSTALS-Kyber або схем цифрового підпису Dilithium та ін., які стандартизовані NIST). По можливості, слід використовувати криптостійкі до квантового зламу рішення для захисту особливо цінних даних уже в найближчому майбутньому.

Висновок

Захист даних у розвідувальних дронах є комплексним завданням, що вимагає поєднання надійного шифрування, безпечних протоколів передачі та правильної експлуатації. Проведений аналіз підтвердив, що застосування сучасних криптографічних методів (AES-256, ECDH, цифрові підписи тощо) значно підвищує безпеку БПЛА, забезпечуючи конфіденційність розвідданих навіть у разі перехоплення каналу або захоплення апарату противником. Виявлено, що недостатність захисту (наприклад, відсутність шифрування у деяких протоколах) створює серйозні ризики несанкціонованого доступу та маніпуляцій з даними. В тезах наведено порівняння алгоритмів шифрування, яке показало, що стандартні рішення на кшталт AES залишаються оптимальними за критерієм «безпека-продуктивність» для більшості дронів, тоді як легковагові алгоритми є альтернативою для пристроїв з екстремально

обмеженими ресурсами. Надано рекомендації, спрямовані на практичне впровадження захисту: шифрувати дані в транзиті й на носіях, використовувати складну систему керування ключами, регулярну зміну ключових параметрів, а також враховувати перспективні криптографічні технології. Загалом, щоб гарантувати надійність розвідувальних операцій, організаціям слід дотримуватися найкращих світових практик кібербезпеки та постійно удосконалювати засоби захисту даних дронів. Це дозволить зберегти інформаційну перевагу та запобігти витокам чутливої інформації у все більш технологічно складному середовищі протидії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ko, Y.; Kim, J.; Duguma, D.G.; Astillo, P.V.; You, I.; Pau, G. Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone. Sensors 21(6), 2057 (2021). DOI: 10.3390/s21062057.
2. Heliguy. Addressing Data Security Concerns with DJI Drones. Heliguy Blog, 2022. – [Електронний ресурс]. Режим доступу: https://www.heliguy.com/blogs/posts/data-security-with-dji-enterprise-drones/ (дата звернення: 18.03.2025).
3. Dimitrijevic, K. Defense Sector – Secure Drone Data Storage and Transmission. PriviCore – The Key to Your Data, 2023. – [Електронний ресурс]. Режим доступу: https://privicore.com/use-case/secure-drone-data-system/ (дата звернення: 18.03.2025).
4. Cybersecurity and Infrastructure Security Agency (CISA). Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems (UASs). USA, 2019. – [Електронний ресурс]. Режим доступу: https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Best%20Practices%20for%20Operating%20Commerical%20UAS%20(508).pdf.
5. Xia, T.; Wang, M.; He, J.; Lin, S.; Shi, Y.; Guo, L. Research on Identity Authentication Scheme for UAV Communication Network. Electronics 12(13), 2917 (2023). DOI: 10.3390/electronics12132917.
6. MathWorks. MAVLink Support – Message Signing (Authentication). MathWorks Documentation, 2023. – [Електронний ресурс]. Режим доступу: https://www.mathworks.com/help/uav/ug/mavlink-support.html (дата звернення: 18.03.2025).
7. National Institute of Standards and Technology (NIST). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. NIST News, Aug 13, 2024. – [Електронний ресурс]. Режим доступу: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

Палій Олексій Миколайович — *інженер програмного забезпечення; LAMPA Software, м. Вінниця, email: alexey.paliy1337@gmail.com*

Oleksii Palii *– Software Engineer, LAMPA Software, Vinnytsia, e-mail: alexey.paliy1337@gmail.com*