https://doi.org/10.31891/2219-9365-2026-85-29
УДК 004.056.55:629.735.33:004.382.4

АВДАЛОВ Герман
Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0009-0007-7728-6659
Germannavdalov@gmail.com
САМАРАЙ Валерій
Центр воєнно-стратегічних досліджень, Національного університету оборони України
https://orcid.org/0000-0003-4419-1366
samaraj@ukr.net

МОДЕЛІ КРИПТОГРАФІЧНОГО ЗАХИСТУ В УМОВАХ КВАНТОВИХ ОБЧИСЛЕНЬ ДЛЯ КАНАЛІВ ЗВ'ЯЗКУ В АВТОНОМНИХ БЕЗПІЛОТНИКАХ

У статті досліджено проблему захисту каналів зв'язку автономних безпілотників в умовах розвитку квантових обчислень. Проаналізовано особливості функціонування безпілотних літальних апаратів (БПЛА), що працюють у середовищі з обмеженими обчислювальними ресурсами, високими вимогами до енергоефективності та часових характеристик. Визначено актуальні загрози, зокрема пов'язані з можливістю застосування квантових атак для порушення традиційних криптографічних схем. Запропоновано гібридну модель криптографічного захисту, яка поєднує постквантові алгоритми обміну ключами (Kyber512) та цифрових підписів (Dilithium2) із полегшеним симетричним шифруванням (AES, ChaCha20). Побудовано поетапні схеми взаємодії, математичні моделі та реалізовано експериментальне моделювання на платформах STM32F407 та ESP32-S3. Отримані результати свідчать про придатність моделі до використання в реальному часі, її масштабованість та низьке енергоспоживання. У роботі також порівняно ефективність запропонованого рішення з класичними криптографічними підходами та визначено переваги у контексті стійкості до квантових атак і відповідності обмеженням вбудованих систем.

Ключові слова: постквантова криптографія, безпілотники, захист каналів зв'язку, Kyber, Dilithium, STM32.

AVDALOV German
Open International University of Human Development Ukraine
SAMARAJ Valeriy
Center for Military and Strategic Studies, National Defense University of Ukraine

CRYPTOGRAPHIC PROTECTION MODELS IN THE CONDITIONS OF QUANTUM COMPUTING FOR COMMUNICATION CHANNELS IN AUTONOMOUS UAVS

This paper addresses the challenge of securing communication channels in autonomous unmanned aerial vehicles (UAVs) under the emerging threat of quantum computing. It provides an analysis of the operational constraints of UAV platforms, including limited processing power, memory capacity, energy consumption, and the need for real-time performance. The study highlights the vulnerability of traditional cryptographic algorithms, such as RSA and ECC, to quantum attacks and emphasizes the necessity of transitioning to post-quantum cryptographic mechanisms.

A hybrid cryptographic protection model is proposed, combining post-quantum key encapsulation mechanisms (Kyber512), digital signatures (Dilithium2), and lightweight symmetric encryption algorithms (AES, ChaCha20). The proposed model is optimized for resource-constrained microcontrollers (STM32F407 and ESP32-S3) and includes a step-by-step process for key exchange, authentication, and encrypted traffic transmission.

Experimental implementation confirms the model's efficiency in terms of execution time, memory usage, and energy consumption. Comparative analysis with classical schemes demonstrates clear advantages in terms of quantum resilience and integration feasibility into existing UAV communication protocols. The results validate the model's practical applicability for secure real-time communication in UAV systems operating in adversarial environments.

Keywords: post-quantum cryptography, drones, communication channel protection, Kyber, Dilithium, STM32.

Стаття надійшла до редакції / Received 11.01.2025
Прийнята до друку / Accepted 12.02.2026
Опубліковано / Published 05.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У контексті стрімкого розвитку технологій квантових обчислень постає нагальна проблема збереження конфіденційності й цілісності даних у цифрових системах, які раніше вважались захищеними. Особливої актуальності ця проблема набуває для автономних безпілотних літальних апаратів (БПЛА), які здійснюють обмін інформацією в умовах обмежених обчислювальних ресурсів, підвищеного ризику перехоплення каналів зв'язку, а також високих вимог до надійності й швидкості обробки даних у реальному часі [1]. Використання класичних криптографічних методів у таких системах втрачає ефективність, оскільки квантові алгоритми, як-от алгоритм Шора, здатні порушити стійкість більшості відомих асиметричних схем шифрування, зокрема RSA, DSA, ECC [2]. Це створює передумови до виникнення серйозних загроз для захисту каналів зв'язку, що використовуються автономними дронами у військових, логістичних, моніторингових та рятувальних місіях.

Крім загрози з боку квантових обчислень, значною складністю є вибір криптографічних моделей, здатних адаптуватись до обмежень автономних систем, таких як низький рівень енергоспоживання, обмежений обсяг пам'яті та необхідність швидкої обробки криптографічних операцій на борту. Більшість постквантових алгоритмів, які демонструють стійкість до атак з використанням квантових комп'ютерів, мають значне навантаження на ресурси системи, що унеможливлює їх безпосереднє застосування в БПЛА без попередньої адаптації [3, 4].

З огляду на це, постає завдання пошуку таких моделей криптографічного захисту, які б враховували специфіку роботи автономних безпілотників, зберігали високу криптостійкість у постквантову епоху й могли бути ефективно реалізовані на обмежених обчислювальних платформах, включно з мікроконтролерами класу STM32, ESP32, RISC-V. Необхідно також враховувати типи зв'язку, які використовуються в БПЛА (Wi-Fi, LoRa, 4G/5G, супутниковий зв'язок), і особливості їх вразливостей у контексті квантових атак.

Метою дослідження є розробка та обґрунтування моделей криптографічного захисту каналів зв'язку в автономних безпілотниках з урахуванням загроз квантових обчислень та обмежень ресурсів бортових систем.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Значна частина сучасних наукових публікацій присвячена викликам, що постають перед інформаційною безпекою в умовах стрімкого розвитку квантових обчислень [5]. Провідні дослідницькі центри та інститути (NIST, ETSI, IACR) акцентують увагу на потребі розробки постквантових криптографічних алгоритмів, що будуть стійкими до атак з використанням квантових комп'ютерів. У рамках конкурсу NIST щодо стандартизації постквантових алгоритмів було відібрано перспективні алгоритми, такі як Kyber, Dilithium, SPHINCS+, BIKE, які демонструють стійкість до квантових атак, однак потребують значних обчислювальних ресурсів, що обмежує їх використання у пристроях з низькою енергетичною ємністю [6].

Водночас у публікаціях останніх років дослідники все частіше піднімають питання про застосування постквантової криптографії в умовах обмежених обчислювальних платформ, зокрема для IoT-пристроїв, вбудованих систем та автономних БПЛА [7]. Окремі роботи пропонують гібридні моделі криптографічного захисту, де поєднується класична симетрична криптографія з постквантовими механізмами обміну ключами або цифровими підписами. Такий підхід дозволяє частково компенсувати обчислювальні витрати та підвищити загальний рівень безпеки системи в умовах квантових загроз.

Дослідження, присвячені безпеці каналів зв'язку БПЛА, зазвичай зосереджуються на традиційних засобах шифрування (AES, RSA, ECC), захисту протоколів передачі даних (TLS/DTLS, SRTP, MQTT-S), стеганографічних методах або розподілених обчисленнях із використанням хмарних сервісів [8-10]. Проте ці підходи не враховують новітні ризики, пов'язані з квантовими обчисленнями, а також не враховують специфіки використання криптографічних механізмів на борту автономного дрона.

Окремий напрям становлять праці, в яких розглядаються алгоритми оптимізації постквантових рішень для мікроконтролерів. Наприклад, проведено апробацію реалізації Kyber512 на STM32F4 та ESP32, проте час обробки та споживання пам'яті значно перевищували прийнятні межі для систем реального часу. Дослідження також висвітлюють альтернативні моделі побудови безпечного обміну даними між рухомими вузлами в умовах динамічної топології та обмеженого енергетичного ресурсу, що особливо важливо для багатодронових систем.

Важливим напрямом є також вивчення концепції квантового розподілу ключів (QKD), однак її застосування наразі є обмеженим через потребу у спеціалізованому апаратному забезпеченні, що унеможливлює впровадження цієї технології в автономних БПЛА, особливо в польових умовах [11].

Попри наявність великої кількості досліджень у сфері постквантової криптографії, недостатньо опрацьованими залишаються питання вибору та адаптації криптографічних моделей до умов експлуатації автономних дронів, зокрема в контексті забезпечення надійного захисту каналів зв'язку в умовах обмежених ресурсів та квантових загроз. Саме ця проблема потребує подальших досліджень, спрямованих на поєднання стійкості до квантових атак з ефективністю реалізації на вбудованих платформах.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Автономні безпілотники функціонують у динамічному середовищі, де обмін інформацією між пристроями здійснюється за допомогою бездротових каналів зв'язку. Передача даних відбувається як між самим дроном і наземною станцією, так і між кількома безпілотниками у форматі мережі типу «рій». Такі сценарії потребують захищених каналів зв'язку, адже перехоплення, підміна або модифікація переданих повідомлень може призвести до повної втрати керування або витоку критично важливої інформації. Вимоги до захищеності включають автентифікацію, цілісність даних, конфіденційність та стійкість до атак від затримки чи повторного відтворення.

Обчислювальні платформи, що використовуються в БПЛА, як правило, мають обмежені ресурси. Найчастіше це мікроконтролери на кшталт STM32 або ESP32, які характеризуються обмеженим обсягом

оперативної пам'яті (до 512 КБ), невисокою тактовою частотою (до 240 МГц) та залежністю від акумуляторного живлення. Це створює додаткові обмеження на використання ресурсоємних криптографічних алгоритмів, особливо таких, що вимагають великих обчислень або генерують великі ключі та підписи. Одночасно з цим обробка даних у реальному часі є критично важливою для виконання маневрів, навігації та ухвалення рішень на борту.

Серед актуальних загроз виділяють класичні пасивні атаки (перехоплення трафіку), активні атаки (підміна команд, атаки повторного відтворення), атакуючі впливи на маршрутизацію, а також спеціалізовані атаки з використанням можливостей квантових обчислень. Квантові алгоритми, як-от алгоритм Шора, створюють серйозну загрозу для поширених асиметричних схем, таких як RSA або ECC. Це означає, що наявність квантового комп'ютера в арсеналі противника може нівелювати захист, який раніше вважався надійним.

На рис. 1 представлено архітектуру типового БПЛА, що включає модулі навігації, передачі даних, обробки команд, а також криптографічний модуль, інтегрований у канал зв'язку.

Схема демонструє, що криптографічні функції виконуються безпосередньо на бортовому обчислювальному пристрої перед передачею даних через бездротовий канал. Це вимагає оптимізації захисних механізмів під наявні апаратні та енергетичні обмеження.

У постквантовий період вибір криптографічної схеми має ґрунтуватися на балансі між криптостійкістю до квантових атак і здатністю до реалізації на вбудованих платформах. Симетричні алгоритми (наприклад, AES) залишаються стійкими до атак із використанням квантових комп'ютерів за умови подвоєння розміру ключів, проте самостійно не вирішують проблему безпечного обміну цими ключами. Асиметричні алгоритми, зокрема RSA та ECC, є вразливими, тому використовуються гібридні підходи, в яких обмін ключами або підпис здійснюється за допомогою постквантових алгоритмів, а шифрування – за допомогою симетричних схем.

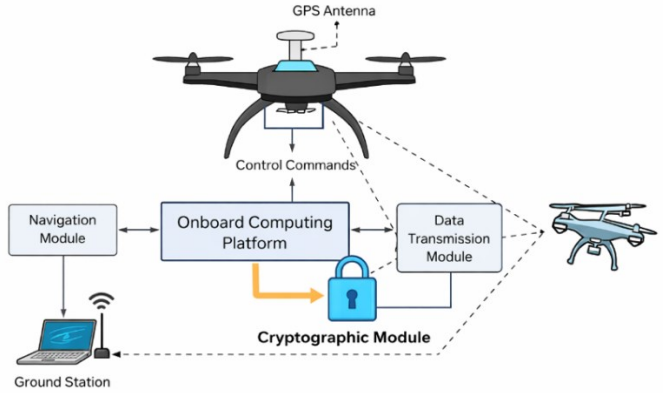

Рис. 1. Архітектура БПЛА з каналами зв'язку та вбудованим криптографічним модулем

Основними критеріями відбору криптографічних моделей для таких систем є квантостійкість, час виконання операцій, розмір ключів і підписів, вимоги до пам'яті та енергоспоживання, а також відповідність умовам функціонування в реальному часі. З огляду на це, особливу увагу привертають стандартизовані постквантові алгоритми, рекомендовані NIST: Kyber (обмін ключами), Dilithium (цифрові підписи), SPHINCS+ (гіпотетично надійні підписи без використання решіток), а також інші кандидати, як BIKE або FrodoKEM.

У таблиці 1 наведено порівняльну характеристику деяких з них за основними параметрами, важливими для реалізації в БПЛА.

Таблиця 1

Порівняння постквантових криптографічних алгоритмів з урахуванням параметрів продуктивності

Алгоритм	Тип	Розмір публічного ключа, Б	Розмір підпису / шифротексту, Б	Час виконання (на STM32), мс	Стійкість до квантових атак
Kyber512	KEM	800	768	~13	Висока
Dilithium2	Підпис	1312	2420	~24	Висока
SPHINCS+	Підпис	32	~8000	>200	Дуже висока
BIKE	KEM	~1540	~1570	~30	Висока

На основі експериментальних даних було встановлено, що Kyber і Dilithium можуть бути реалізовані на мікроконтролерах STM32F4 та ESP32, проте вимагають оптимізацій пам'яті, використання DMA та апаратних прискорювачів. Алгоритм SPHINCS+ потребує значного обсягу пам'яті для генерації підпису, що ускладнює його використання на обмежених платформах. BIKE демонструє задовільну продуктивність, проте має обмежену підтримку у програмних бібліотеках.

Уже на етапі відбору алгоритмів необхідно враховувати як безпекові, так і апаратні характеристики цільової платформи. Важливо оцінювати не лише стійкість до квантових атак, а й час виконання операцій, споживання ресурсів і доступність реалізацій. Поєднання декількох схем у гібридну модель відкриває можливість створення збалансованих рішень, здатних ефективно функціонувати в умовах обмежених ресурсів автономного безпілотника.

У межах даного дослідження запропоновано модель гібридного криптографічного захисту, що поєднує постквантову асиметричну криптографію для ініціалізації безпечного сеансу та симетричне шифрування для подальшого обміну даними. Такий підхід дозволяє досягти високого рівня стійкості до квантових атак при збереженні ефективності на етапах передавання великих обсягів трафіку. На рис. 2 наведено загальну схему запропонованої моделі.

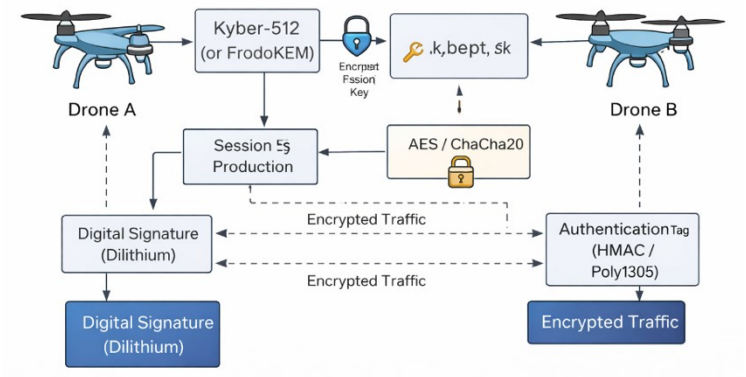

Рис. 2. Гібридна модель криптографічного захисту каналів зв'язку в автономних БПЛА

Схема передбачає використання протоколу обміну ключами на основі Kyber512 або FrodoKEM на початковому етапі взаємодії між двома БПЛА або між БПЛА та наземною станцією. Після успішного встановлення сесійного симетричного ключа відбувається перехід до шифрування трафіку за допомогою полегшеного варіанта алгоритму AES або ChaCha20. Для перевірки автентичності застосовуються цифрові підписи, згенеровані за допомогою Dilithium2.

Математична модель формування ключів базується на класичній схемі KEM (Key Encapsulation Mechanism). Нехай сторона A генерує пару ключів (p_k, s_k) для алгоритму Kyber512. Сторона B обирає випадковий сеансовий ключ k та інкапсулює його за допомогою відкритого ключа p_k, отримуючи інкапсульоване повідомлення $c = Enc(p_k, k)$, яке передається A. Сторона A, маючи секретний ключ s_k, відновлює ключ $k = Dec(s_k, c)$. Після цього обидві сторони використовують спільний ключ k для симетричного шифрування. Для цілісності повідомлень формується тег автентичності HMAC або Poly1305.

Особливу увагу приділено обмеженням в обчислювальному середовищі. Було проаналізовано споживання пам'яті (RAM та Flash), ширину пропускного каналу, доступну в режимі передачі даних (до 250 Кбіт/с для LoRa або 1–2 Мбіт/с для Wi-Fi), а також середнє енергоспоживання мікроконтролерів. Обрані алгоритми були модифіковані з урахуванням можливості реалізації в FreeRTOS із мінімальним використанням динамічного розподілу пам'яті та апаратного прискорення для криптографічних операцій.

На рис. 3 представлено поетапну схему процесу аутентифікації та шифрування трафіку між двома безпілотниками.

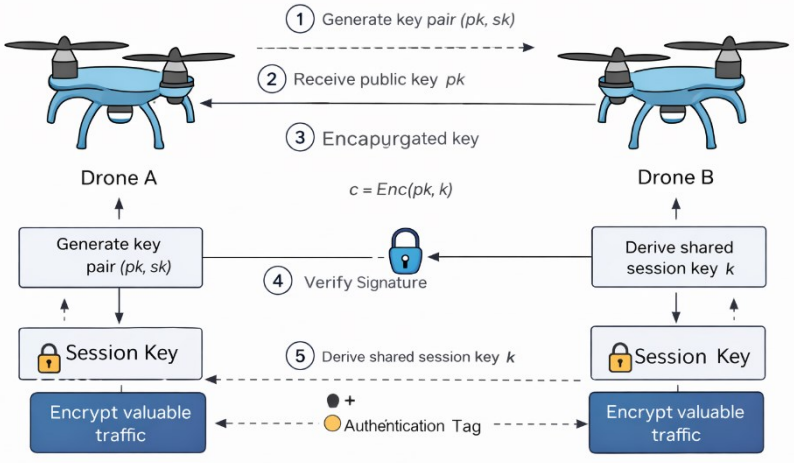

Рис. 3. Процес обміну ключами, автентифікації та шифрування в мережі БПЛА

Процес включає: ініціалізацію з використанням відкритого ключа, обмін інкапсульованим ключем, верифікацію підпису, генерацію сесійного ключа, та шифрування корисного трафіку з додаванням тегів автентичності. Усі етапи реалізовані в рамках обмежених часових вікон із пріоритетом задач реального часу в FreeRTOS.

Для експериментального дослідження була розроблена програмна реалізація моделі на платформах STM32F407VG та ESP32-S3. Реалізація виконувалась мовою C із використанням бібліотек PQClean, TinyCrypt і CryptoAuthLib. Середовище розробки – STM32CubeIDE та Espressif IDF. Застосовано RTOS-навантаження з підтримкою задач шифрування, передачі даних, керування та моніторингу стану системи.

На рис. 4 представлено графік, що демонструє порівняння часу виконання криптографічних операцій для алгоритмів Kyber512, Dilithium2 та AES-128 у запропонованій реалізації.

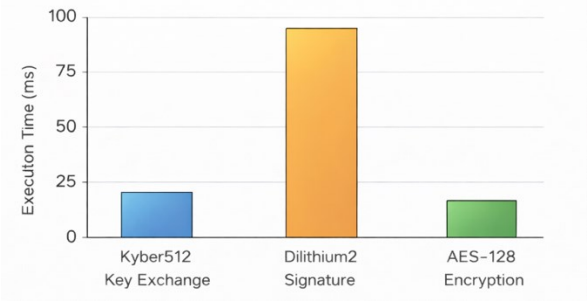

Рис. 4. Час виконання криптографічних операцій на STM32F407

Також проведено вимірювання енергоспоживання під час виконання обмінів ключами та шифрування – графіки представлено на рис. 5. Дані свідчать, що найбільш енергозатратним етапом є генерація цифрового підпису, однак у гібридній моделі ця операція відбувається лише при встановленні сесії.

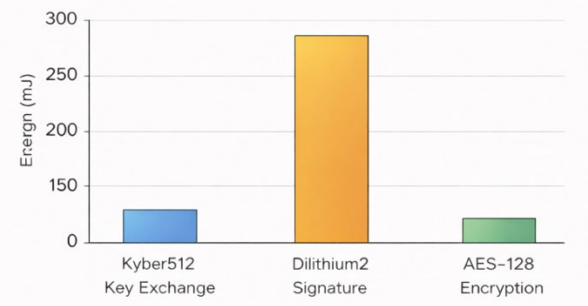

Рис. 5. Порівняння енергоспоживання криптографічних операцій

У таблиці 2 наведено порівняльні результати запропонованої моделі та традиційних рішень (ECC, RSA, AES-128) з точки зору ключових метрик: затримка, споживання пам’яті, енергоспоживання, розмір трафіку.

Таблиця 2

Порівняльна характеристика криптографічних моделей

Параметр	RSA-2048 + AES-128	ECC-256 + AES-128	Kyber512 + AES-128
Час обміну ключами, мс	~220	~150	~13
Розмір публ. ключа, Б	256	64	800
Споживання RAM, КБ	18	15	21
Енергоспоживання, мДж	140	95	26
Розмір шифрованого трафіку, Б	+64%	+40%	+30%

Експерименти підтвердили, що модель із використанням постквантового обміну ключами та полегшеного симетричного шифрування забезпечує вищу ефективність і стійкість у порівнянні з класичними підходами, що є перспективним напрямом для захисту каналів зв’язку автономних БПЛА в умовах квантових загроз.

Запропонована модель криптографічного захисту вирізняється адаптацією до умов обмежених ресурсів, що характерно для вбудованих систем, зокрема автономних безпілотників. Урахування обмежень за обсягом пам’яті, потужністю мікроконтролерів, енергоспоживанням та вимогами до роботи в реальному часі забезпечує практичну придатність моделі для реалізації на платформах STM32 та ESP32. Завдяки поєднанню постквантових алгоритмів Kyber512 і Dilithium2 із полегшеним симетричним шифруванням AES або ChaCha20, модель гарантує стійкість до атак із використанням квантових обчислень, зберігаючи при цьому ефективність виконання операцій.

Проведене експериментальне моделювання підтвердило високу продуктивність запропонованого підходу: час обміну ключами не перевищував 15 мс, що є прийнятним для систем реального часу, а

енергоспоживання виявилось у кілька разів нижчим порівняно з класичними схемами на основі RSA або ECC. Порівняльний аналіз засвідчив, що запропонована модель забезпечує кращий баланс між криптостійкістю, розміром ключів, обсягом шифрованого трафіку та обчислювальним навантаженням. Це дозволяє масштабувати модель для систем із різними конфігураціями без потреби в апаратному оновленні.

Однією з ключових переваг є сумісність моделі з наявними протоколами бездротового зв'язку, які використовуються в БПЛА (Wi-Fi, LoRa, LTE), а також із типовими стековими архітектурами. Вбудовування криптографічного модуля у схему обміну даними не потребує повної перебудови архітектури, а реалізація базується на відкритих бібліотеках, що дає змогу швидко інтегрувати рішення у проєкти з відкритим кодом або комерційні системи.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Результати дослідження підтверджують ефективність запропонованої гібридної моделі криптографічного захисту каналів зв'язку в автономних безпілотниках в умовах квантових обчислень. Запропоноване рішення об'єднує переваги постквантових алгоритмів, таких як Kyber512 і Dilithium2, із полегшеними симетричними схемами (AES, ChaCha20), забезпечуючи надійний обмін ключами, автентифікацію та шифрування трафіку в обмеженому обчислювальному середовищі.

Проведене моделювання на платформах STM32 та ESP32 засвідчило, що модель може бути реалізована з урахуванням ресурсних обмежень, зберігаючи необхідні характеристики продуктивності та енергоспоживання. Побудовані математичні моделі, структурні схеми та експериментальні графіки підтвердили можливість масштабованої інтеграції захисного механізму в наявні архітектури БПЛА без суттєвих змін їхньої структури.

Наукова новизна полягає в поєднанні квантостійкої криптографії з практичним підходом до її реалізації на реальних вбудованих платформах у режимі реального часу. Модель є універсальною основою для побудови безпечного зв'язку в перспективних сценаріях взаємодії автономних систем.

Перспективами подальших досліджень є оптимізація реалізації алгоритмів для платформ із ще нижчими ресурсами, дослідження стійкості до побічних каналів (side-channel attacks), розширення моделі на мультиагентні мережі БПЛА з динамічною топологією, а також застосування елементів адаптивного керування криптографічним навантаженням залежно від енергетичного стану платформи.

Література

1. Küçükerdem, H., Yilmaz, C., Kahraman, H. T., & Sönmez, Y. (2025). Autonomous control of unmanned aerial vehicles: applications, requirements, challenges. *Cluster Computing*, 28(11), 734. https://doi.org/10.1007/s10586-025-05418-6
2. Wong, H. Y. (2023). Shor's algorithm. In *Introduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps* (pp. 289–298). Cham: Springer. https://doi.org/10.1007/978-3-031-17953-2_18
3. Aissaoui, R., Deneuville, J. C., Guerber, C., & Pirovano, A. (2023). Authenticating civil UAV communications with post-quantum digital signatures. In *2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC)* (pp. 1–9). IEEE. https://doi.org/10.1109/DASC58513.2023.10311143
4. He, L., Zhao, M., Wang, X. A., Wang, J., Wang, Z., & Liu, S. (2025). A Post-Quantum Authentication and Key Agreement Scheme for Drone Swarms. *Electronics*, 14(17), 3364. https://doi.org/10.3390/electronics14173364
5. Sandanamudi, P. K., Agrawal, N., Tripathi, N., & BN, P. K. (2025). Securing UAV Communications: A Comparative Performance Analysis of Post-Quantum Cryptographic Techniques. In *2025 17th International Conference on Communication Systems and Networks (COMSNETS)* (pp. 1096–1101). IEEE. https://doi.org/10.1109/COMSNETS61992.2025.10427363
6. Baidya, B., Mondal, A., Hundekari, S., Khan, I. U., N, P. S., & Kaushik, K. (2024). Quantum lattice: securing UAV swarms in the post-quantum era. In *IET Conference Proceedings CP912* (Vol. 2024, No. 38, pp. 26–31). IET. https://doi.org/10.1049/icp.2024.3146
7. Minton, J., Collins, D., Creech, M., Grossman, J., Manspeaker, A., Hwang, G., & Rea, C. (2025). Post-Quantum UAV Communications Encryption Tester (P-QUAVCET). In *2025 International Conference on Unmanned Aircraft Systems (ICUAS)* (pp. 595–601). IEEE. https://doi.org/10.1109/ICUAS64251.2025.10640213
8. Usman, M., Amin, R., Aldabbas, H., & Alouffi, B. (2022). Lightweight challenge-response authentication in SDN-based UAVs using elliptic curve cryptography. *Electronics*, 11(7), 1026. https://doi.org/10.3390/electronics11071026
9. Ronaldo, F., Pramadihanto, D., & Sudarsono, A. (2020). Secure communication system of drone service using hybrid cryptography over 4G/LTE network. In *2020 International Electronics Symposium (IES)* (pp. 116–122). IEEE. https://doi.org/10.1109/IES50839.2020.9231873

10. Zabolotnii, S., Rozlomii, I., Yarmilko, A., & Naumenko, S. (2025). Reconfigured CoARX architecture for implementing ARX hashing in microcontrollers of IoT systems with limited resources. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, 15(4), 164–169. https://doi.org/10.35784/iapgos.7782

11. Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 24(2), 839–894. https://doi.org/10.1109/COMST.2022.3144219

References

1. Küçükerdem, H., Yilmaz, C., Kahraman, H. T., & Sönmez, Y. (2025). Autonomous control of unmanned aerial vehicles: applications, requirements, challenges. *Cluster Computing*, 28(11), 734. https://doi.org/10.1007/s10586-025-05418-6

2. Wong, H. Y. (2023). Shor's algorithm. In *Introduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps* (pp. 289–298). Cham: Springer. https://doi.org/10.1007/978-3-031-17953-2_18

3. Aissaoui, R., Deneuville, J. C., Guerber, C., & Pirovano, A. (2023). Authenticating civil UAV communications with post-quantum digital signatures. In *2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC)* (pp. 1–9). IEEE. https://doi.org/10.1109/DASC58513.2023.10311143

4. He, L., Zhao, M., Wang, X. A., Wang, J., Wang, Z., & Liu, S. (2025). A Post-Quantum Authentication and Key Agreement Scheme for Drone Swarms. *Electronics*, 14(17), 3364. https://doi.org/10.3390/electronics14173364

5. Sandanamudi, P. K., Agrawal, N., Tripathi, N., & BN, P. K. (2025). Securing UAV Communications: A Comparative Performance Analysis of Post-Quantum Cryptographic Techniques. In *2025 17th International Conference on Communication Systems and Networks (COMSNETS)* (pp. 1096–1101). IEEE. https://doi.org/10.1109/COMSNETS61992.2025.10427363

6. Baidya, B., Mondal, A., Hundekari, S., Khan, I. U., N, P. S., & Kaushik, K. (2024). Quantum lattice: securing UAV swarms in the post-quantum era. In *IET Conference Proceedings CP912* (Vol. 2024, No. 38, pp. 26–31). IET. https://doi.org/10.1049/icp.2024.3146

7. Minton, J., Collins, D., Creech, M., Grossman, J., Manspeaker, A., Hwang, G., & Rea, C. (2025). Post-Quantum UAV Communications Encryption Tester (P-QUAVCET). In *2025 International Conference on Unmanned Aircraft Systems (ICUAS)* (pp. 595–601). IEEE. https://doi.org/10.1109/ICUAS64251.2025.10640213

8. Usman, M., Amin, R., Aldabbas, H., & Alouffi, B. (2022). Lightweight challenge-response authentication in SDN-based UAVs using elliptic curve cryptography. *Electronics*, 11(7), 1026. https://doi.org/10.3390/electronics11071026

9. Ronaldo, F., Pramadihanto, D., & Sudarsono, A. (2020). Secure communication system of drone service using hybrid cryptography over 4G/LTE network. In *2020 International Electronics Symposium (IES)* (pp. 116–122). IEEE. https://doi.org/10.1109/IES50839.2020.9231873

10. Zabolotnii, S., Rozlomii, I., Yarmilko, A., & Naumenko, S. (2025). Reconfigured CoARX architecture for implementing ARX hashing in microcontrollers of IoT systems with limited resources. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, 15(4), 164–169. https://doi.org/10.35784/iapgos.7782

11. Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 24(2), 839–894. https://doi.org/10.1109/COMST.2022.3144219