УДК 004.056.5:629.7.052; 519.725:629.7.052 **DOI:10.30837/rt.2025.4.223.07**

С.Я. ГІЛЬГУРТ, д-р техн. наук, Л.В. КОВАЛЬЧУК, д-р техн. наук,
А.М. ДАВИДЕНКО, д-р техн. наук

ОГЛЯД ПІДХОДІВ ДО ПОБУДОВИ ЗАХИЩЕНИХ ЗАВАДОСТІЙКИХ СИСТЕМ ПЕРЕДАЧІ ПОТОКОВОГО ВІДЕО З БПЛА[1]

Вступ

Останнім часом набуває масового поширення як в цивільних застосуваннях, так і у військовій сфері такий підклас безпілотних літальних апаратів (БпЛА), як FPV-дрони (від англ. First Person View). На фронті вони використовуються для розвідки та коригування вогню, але найбільш дієво зарекомендували себе в якості баражуючих боєприпасів (так звані FPV-дрони-камікадзе), що вражають цілі методом самознищення. Їх переваги – низька вартість (кілька сот доларів за одиницю) та висока точність ураження завдяки прямому відеоконтролю оператором (тобто віртуальної присутності людини безпосередньо у місці подій) протягом всього польоту.

Ключова вразливість таких дронів – радіоканал керування та передачі відеозображення. Особливо важливим є відеосигнал, що передається радіоканалом з бортової відеокамери БпЛА на наземну базову станцію, перехоплення якого ворожою стороною наражає на небезпеку дроновода. Тому цей канал зв’язку має бути захищений засобами захисту інформації. На сьогодні відомо багато підходів, методів та алгоритмів крипостійкого шифрування. Але внаслідок своєї реурсоємності вони вносять суттєву затримку в тракт передачі даних, і для їх реалізації потрібні обчислювальні ресурси, якими складно забезпечити легкий та дешевий модуль, придатний для використання у одноразових FPV-дронах-камікадзе.

З іншого боку, такі алгоритми, як правило, критичні до спотворення інформації в каналі зв’язку: заміна лише одного біту у повідомленні може призводити до втрати цілого блоку даних, або навіть всього повідомлення. Але в бойових умовах на відеоканал здійснюється вплив з боку ворожих засобів радіоелектронної боротьби (РЕБ). Ефективні глушники мають обмежену зону дії, але здатні виводити з ладу зв’язок FPV-дронів на критичній відстані. Це робить актуальним друге завдання – підвищення завадостійкості каналу передачі відеоданих. Відомо багато методів завадостійкого кодування, які втім не вирішують задачу захисту інформації і можуть бути легко декодовані противником. Методи скремблювання, яки традиційно використовуються для закриття аналогових каналів відеозв'язку, згідно з практичним досвідом використання FPV-дронів-камікадзе у бойових умовах, не забезпечують потрібного рівня захищеності відеоканалу, оскільки дозволяють противнику за допомогою нескладних пристроїв зламати такий захист протягом одиниць хвилин.

Отже виникає важливе та нетривіальне завдання створення систем передачі відеоданих, які дозволяли б захищати інформацію, одночасно забезпечуючи надійність зв’язку в умовах штучних завад. В якості першого кроку на шляху вирішення даного завдання потрібно проаналізувати наявну інформацію про відомі підходи та методи як до захисту інформації, так і до підвищення завадостійкості каналів зв’язку.

Метою дослідження є попередній огляд останніх досягнень в галузі захисту інформації та корекції помилок, які можуть бути використані в якості прототипів для створення захищених завадостійких систем передачі потокового відео, придатних до інтеграції в існуючі безпілотні платформи FPV-дронів-камікадзе.

Отримані результати дозволять просунутися у напрямі створення концепції захищеної завадостійкої системи передачі відеоданих з БпЛА на наземну станцію, яка в свою чергу

[1] Дослідження виконане за фінансової підтримки з боку Національного фонду досліджень України, проєкт 2025.6/0109 "Захищена завадостійка система передачі відеоінформації з безпілотного літального апарата", номер державної реєстрації 0125U003164.

дозволить підвищити ефективність застосування FPV-дронів-камікадзе як у військових застосуваннях, так і в цивільних сферах (безпечний зв’язок для рятувальних дронів, правоохоронних органів тощо).

Огляд публікацій

В роботі [1] експлуатація безпілотних літальних апаратів розглядається як нова сфера кіберпротистояння, аналізуються ризики перехоплення, зламу чи глушіння сигналів управління та передачі даних. На основі прикладів з реальних бойових дій в Україні автори досліджують як поєднання військових і цивільних БпЛА змінює характер конфліктів гібридного типу. Робота звертає увагу на проблеми ідентифікації джерел керування, захисту від електронних атак і контролю за використанням цивільних безпілотників, що створює нові виклики для безпеки. Окрему увагу приділено питанням кіберзахисту та протидії зловмисному використанню безпілотних технологій, що підкреслює зростаючу роль кіберпростору у воєнних операціях.

Відомо, що противник активно застосовує переносні та встановлені на техніці засоби РЕБ для створення радіоперешкод на частотах передачі відеосигналів з дронів [2]. При цьому дружні засоби радіоелектронної боротьби також впливають на зв'язок з БпЛА через те, що свої пункти керування знаходяться ближче, як правило, РЕБ ефективніший проти них, ніж проти ворога [3].

Радикально вирішити проблему дозволяє заміна радіоканалу на оптоволоконну лінію зв’язку [4]. Однак такий підхід має суттєві недоліки – обмеження радіусу дії довжиною кабелю, ускладнення маневреності та ризик втрати зв’язку внаслідок пошкодження волоконного кабелю. Тому радіозв’язок досі залишається основним рішенням для забезпечення керування та передачі відеосигналу, отже проблема закриття каналу та підвищення завадостійкості залишається гострою.

Відомі рішення, що використовують криптографічні алгоритми шифрування, такі, як AES-256, та самоналагоджуванні MESH-мережі та частотний хопінг для протидії глушінню і перехопленню сигналу [5, 6].

Щодо підвищення завадостійкості, деякі сучасні цифрові системи (DJI FPV, Autel, тощо) використовують модульовані протоколи (OFDM на 2.4/5 ГГц) та розширення спектру для підвищення завадостійкості. Використовується також частотне перестрибування (FHSS) і пряме розширення спектру для каналів управління та ортогональне частотне мультиплексування (COFDM) для передачі а відео, що забезпечує вищу стійкість до шумів і перешкод [7]. Розробляються також спеціалізовані завадостійкі радіомодеми для БпЛА, які здатні динамічно змінювати частоту та знаходити "вікна" в спектрі ворожих глушників.

Відомі й інші рішення, пов’язані з безпекою передачі відеосигналу та використання БпЛА [8–12.] Але всі згадані розробки є складними та дорогими рішеннями, використання яких є доцільним на потужних, наприклад, розвідувальних БпЛА. До того ж важливим недоліком будь-яких цифрових систем є відчутна затримка, що є неприйнятним недоліком при застосуванні на дронах-камікадзе. З іншого боку, аналогові системи відеозв'язку, які завдяки малій затримці та природній властивості зберігати "картинку" навіть при великому відсотку втраченого сигналу найбільш поширені зараз саме на FPV-дронах, особливо вразливі, оскільки зазвичай працюють на фіксованих частотах (5.8 ГГц) і не шифрують радіосигнал. А методи захисту аналогового каналу на основі скремблювання не забезпечують потрібного рівня захищеності.

Деякі особливості передачі потокового відео з БпЛА

В роботах [13, 14] сформульовано основні вимоги та обмеження, які накладаються в реальних бойових умовах на тракт передачі відеоданих з бортової відеокамери на станцію керування. Час затримки передачі інформації вздовж всього каналу повинен мати порядок 20–100 мс. При цьому вимоги до стійкості криптозахисту такої системи набагато менш жорсткі порівняно з традиційним використанням криптозахисту – час, потрібний зловмиснику

для злому системи захисту з використанням потужних обчислювальних засобів, має бути порядку одиниць годин. Фактично, йдеться про тимчасову стійкість системи передачі відеозображення. Як наслідок, алгоритми, які шифрують відеопотік даних з БпЛА, мають належати скоріш до класу так званих малоресурсних алгоритмів [15], які за рахунок можливості зниження крипостійкості дозволяють скоротити ресурсні витрати та підвищити пропускну здатність. Тому доцільно ретельно проаналізувати роботи, присвячені саме таким алгоритмам.

Нижче розглянуто відомі розробки, присвячені малоресурсним алгоритмам шифрування та деякім іншим суміжним питанням, пов'язаним з забезпеченням захищеного завадостійкого відеозв'язку з БпЛА.

Малоресурсні алгоритми шифрування

У роботі [16] розглянуто питання автентифікації в системах керування БпЛА. Автори пропонують використовувати для цього малоресурсний асиметричний алгоритм HIGHT і зазначають, що для шифрування може застосовуватись також схема Фейстеля. Водночас у публікації не наведено конкретного алгоритму, який би відповідав вимогам щодо швидкодії та обсягу пам'яті, необхідним для оброблення відеоданих. Результати цієї роботи не можуть бути використані безпосередньо для захисту відеоданих, оскільки така задача вимагає значно більшої швидкодії.

У роботі [17] досліджується використання алгоритму AES у режимі EAX (encrypt-then-authenticate-then-translate) для шифрування відео- та аудіопотоків, що передаються з БпЛА. Експериментальні результати продемонстрували хороші показники при обробленні аудіосигналів навіть за умов помилок, проте показали низьку ефективність при шифруванні відео. Це пояснюється недостатньою швидкодією алгоритму AES, оскільки цей алгоритм першочергово розроблявся для досягнення високої криптостійкості, а не продуктивності.

У публікації [18] представлено малоресурсний блоковий шифр Piccolo з довжиною блоку 64 біти та ключем 80 або 128 біт. Це узагальнена схема Фейстеля з чотирма 16-бітними гілками, яка виконує 25 або 31 раунд залежно від довжини ключа. За обсягом пам'яті Piccolo подібний до поширеного шифру PRESENT [19], проте його пропускна здатність сягає лише 21,54 байта на секунду, що є недостатнім для відеошифрування, де допустима затримка не повинна перевищувати 0,03 секунди. Навіть зі зменшенням кількості раундів цей алгоритм залишається занадто повільним для оброблення відео.

У роботі [20] розглянуто застосування AES для шифрування даних, що передаються з БпЛА. Автори зазначають, що цей алгоритм використовується в українських дронах PD-2 та Shark для захисту телеметрії (швидкість, висота, координати тощо). Проте обсяг таких даних набагато менший, ніж у відеопотоці, і їх не обов'язково передавати безперервно в реальному часі. Тому AES, який добре підходить для невеликих обсягів інформації, не може бути ефективно застосований до відеошифрування через недостатню швидкодію.

У дослідженні [21] представлено алгоритм шифрування зображень дикої природи, що передаються з БпЛА, побудований на поєднанні одно- та двовимірних клітинних автоматів (1D MCA і 2D MCA) із побітовими операціями додавання та перемішування. Основна увага приділена оцінці стійкості алгоритму та механізму генерації ключів. Проте в роботі відсутні дані щодо швидкодії та вимог до пам'яті, тому придатність цього методу для шифрування відео в реальному часі залишається невизначеною.

Робота [22] описує загальний фреймворк криптографічного захисту для малих дронів, який, за твердженням авторів, є енергоефективним і перевершує стандартні методи за швидкістю. До нього входить інфраструктура відкритих ключів (PKI) та алгоритми на еліптичних кривих. Однак конкретних алгоритмів для шифрування відео або даних про їх продуктивність не наведено.

У публікації [23] представлено малоресурсний шифр HANK-1, побудований за узагальненою схемою Фейстеля з чотирма гілками та вісьмома раундами. Його рекомендовано використовувати в режимі CBC. Алгоритм потребує 64 Кбайт пам'яті та забезпечує швидкість 84,1468 Кбіт/с, що робить його потенційно придатним для систем з обмеженими ресур-

сами. Водночас через малу кількість раундів і відсутність аналітичних оцінок стійкості застосування HANK-1 пов'язане зі значними ризиками. Автори наводять певні евристичні міркування та застосовують статистичні тести з пакету NIST [24], не отримуючи якихось аналітичних оцінок крипостійкості.

У роботі [25] запропоновано ультрамалоресурсний шифр Sriram, орієнтований на використання в RFID-мітках і сенсорних мережах. Це блоковий шифр Фейстеля зі SP-мережею, 64-бітовим блоком і ключем 96 або 128 біт, який виконує 27 раундів. Проте автори не надають кількісних характеристик щодо пам'яті чи пропускної здатності, тому придатність Sriram для відеошифрування оцінити неможливо.

У роботі [26] представлено блоковий алгоритм CARX для БпЛА, але зазначається, що для шифрування відео краще підходить потоковий алгоритм ZUC-128 [27], який має швидкість генерації гами 33,74 Кбіт/с і швидкість шифрування 23,31 Кбіт/с. Попри це, без тестування в реальних умовах не можна гарантувати необхідну затримку, а значний час ініціалізації робить ZUC-128 непридатним для використання в реальному часі.

У роботі [28] описано сімейство малоресурсних блокових шифрів SHIPHER, що базуються на динамічних операціях у різних алгебраїчних системах, подібно до шифру IDEA [29]. Автори заявляють про кращі показники швидкодії та пам'яті порівняно з AES, але не надають підтверджуючих даних. Використання операцій, відмінних від XOR, імовірно знижує продуктивність, тому питання часової затримки залишається відкритим.

У публікації [30] обговорюються проблеми безпеки БпЛА в аграрному секторі, зокрема ризик викрадення через підробку сигналів керування. Як контрзахід пропонується використання шифру Вернама, однак питання ресурсомісткості та швидкодії не розглядаються. Зберігання або генерація достатньо довгої гами без повторень вимагає великих обсягів пам'яті, що робить цей підхід малопридатним для реального застосування.

Стійкість до радіоелектронної боротьби

Робота [31] присвячена оцінюванню енергетичної доступності каналів зв'язку безпілотних літальних апаратів у контексті протидії засобам радіоелектронної боротьби противника. У роботі здійснено порівняльний аналіз різних технологій радіозв'язку для БПЛА з точки зору їхньої стійкості до радіоперешкод і ефективності використання енергетичних ресурсів. Автори показують, що більшість технологій вразливі до радіопридушення, проте використання широкосмугових систем із завадостійким кодуванням може істотно підвищити їхню надійність. На основі аналітичних розрахунків запропоновано рекомендації щодо використання типів модуляції, які забезпечують компроміс між енергетичною ефективністю та завадостійкістю, що має практичне значення для побудови безпечних комунікаційних каналів у складних електронних умовах.

В роботі [32] запропоновано метод багатоканальної компенсації завад для захисту комунікацій автономних літальних апаратів від радіопридушення. Розроблений підхід дозволяє одночасно здійснювати синхронізацію за часом і частотою та ефективно усувати вплив перешкод без потреби в попередньому знанні характеристик каналу чи сигналу завад. Метод ґрунтується на використанні відомої преамбули передавача, що спрощує реалізацію в існуючих протоколах зв'язку. Результати експериментів на апаратній платформі показали, що навіть за умови, коли потужність завад у 40 дБ перевищує потужність корисного сигналу, запропонована система здатна успішно відновлювати передану інформацію, забезпечуючи надійний і захищений зв'язок у складних умовах радіоелектронної боротьби.

В роботі [33] запропоновано міжрівневу архітектуру для передавання потокового мультимедіа з безпілотних літальних апаратів, що враховує динамічні зміни їхнього положення та швидкості. Створена система Client-Server-Ground&User (C-S-G&U) реалізує алгоритм розподілу навантаження Splitting-Merging Stream (SMS), який забезпечує одночасну передачу даних кількома каналами для підвищення пропускної здатності та зменшення затримки. Додатково застосовано механізми прямого виправлення помилок (Forward Error Correction – FEC), шифрування та динамічної адаптації режимів передавання відповідно до поточних

умов мережі. Експериментальна реалізація показала стабільність роботи системи при змінних параметрах польоту, що підтверджує ефективність запропонованої архітектури для надійної та безпечної передачі відеопотоку з БПЛА.

В роботі [34] досліджено задачу безпечного розподілу ресурсів у когнітивних MIMO-мережах для внутрішніх приміщень із залученням безпілотних літальних апаратів. Автори інтегрують технології когнітивного радіо, MIMO та O-RAN для створення енергоефективних і стійких до радіопридушення систем зв'язку. Розроблений алгоритм підвищує стійкість системи до атак заглушення та зменшує загальні енергетичні витрати при збереженні пропускної здатності мережі.

Препроцессінг та стиснення інформації перед шифруванням

В роботі [35] пропонується метод попередньої обробки відеоданих із безпілотних апаратів на основі вдосконаленого алгоритму стискання цифрових зображень. Запропонований підхід спрямований на зменшення обсягу даних без суттєвих втрат якості зображення перед подальшим шифруванням. Метод поєднує інваріантні перетворення та виділення фону, що дозволяє досягати високого рівня стиснення та підвищити ефективність подальших етапів криптографічної обробки. Мета такої попередньої обробки – зменшити обсяг даних на борту БпЛА перед шифруванням. Скорочення бітрейту знижує вимоги до ресурсноємності процедури шифрування, але припускає можливість втрати якості, що може ускладнити подальше використання відеозображення.

Додаткові питання автентифікації

Автори роботи [36] пропонують інноваційний підхід до захисту каналів зв'язку безпілотних літальних апаратів, який ґрунтується на використанні біометричних характеристик оператора, отриманих із сигналів електроенцефалограма (ЕЕГ). Метод передбачає генерування криптографічного ключа на основі коефіцієнтів Бета-хвиль, оброблених за допомогою поліномів Лежандра та кодів Боуза–Чоудхурі–Хоквінгема. Такий ключ використовується для шифрування комунікації між БпЛА та базовою станцією, забезпечуючи унікальність і неможливість підробки. У разі виявлення атаки система автоматично переводить дрон у безпечний режим повернення. Проведені експерименти довели працездатність концепції на комерційному БпЛА, що підтверджує потенціал біометричного підходу до захисту бездротових каналів зв'язку. Висунута авторами дослідження ідея цікава з точки зору підвищення безпеки зв'язку, але додає складнощів при практичній реалізації та використанні, особливо в польових/ бойових умовах.

Швидкодія та використання ПЛІС / SoC

В роботі [37] докладно розглянуто моделювання потоку керуючих даних радіоканалу безпілотного літального апарата. Автори досліджують вплив криптографічних перетворень на динамічні характеристики каналу, зокрема затримки сигналів і можливі похибки під час польоту апарата. Експериментальні результати, отримані в умовах, наближених до реальних, демонструють, як криптографічні механізми впливають на часові параметри управління та точність реакції системи. Отримані результати зокрема свідчать про потребу в швидких засобах реалізації криптографічних алгоритмів.

Робота [38] демонструє переваги використання ПЛІС типу FPGA для реалізації шифрування/дешифрування, які дозволяють знизити як затримку обробки інформації, так і енергоспоживання порівняно з реалізаціями на мікропроцесорах та мікроконтролерах. Програмована логіка відкрила шлях до апаратного шифрування не лише телеметричних даних, але й також відеоданих. Апаратна реалізація дозволяє забезпечити потрібну пропускну здатність для повнофороматного відео. Зворотній бік застосування ПЛІС – вища порівняно з традиційним програмуванням складність проєктування, більша ціна FPGA-чіпів та певна спеціалізована "обв'язка" мікросхем програмованої логіки порівняно з відпрацьованими цифровими схемами на мікроконтролерах.

Запропонована в роботі [39] схема шифрування відео QuVench побудована на принципах квазигрупового перетворення, орієнтована на забезпечення безпечної передачі стиснено-

го відео в реальному часі. Реалізовано її на так званій системі-на-кристалі (System on the Chip – SoC), яка є об’єднанням в одному електронному пристрої реконфігуровної матриці, як в ПЛІС, та потужного апаратного мікропроцесорного ядра. У дослідженні підкреслюється важливість швидкої обробки відеоданих у пристроях із обмеженими ресурсами, зокрема в безпілотних апаратах. Використання SoC демонструє можливість досягнення майже миттєвого шифрування та дешифрування майже без затримки, мінімізуючи апаратні витрати.

Аналіз інформації

Аналіз літературних джерел дозволяє поділити дослідження у сфері захищеного відеозв'язку з БпЛА на кілька напрямів.

Першу групу становлять роботи, що стосуються шифрування зображень або невеликих обсягів даних, наприклад, такі як [16, 18, 21, 30]. Ці алгоритми призначені для автентифікації, захисту телеметрії чи одиничних кадрів і не відповідають вимогам систем реального часу. Хоча вони демонструють високу криптостійкість, їхня швидкодія та обчислювальні потреби є надмірними для FPV-дронів, що працюють у режимі низьких затримок.

Другу групу утворюють дослідження, такі як [20, 26, 28], в яких запропоновано високостійкі, проте ресурсомісткі рішення, орієнтовані на потужні розвідувальні або інші багаторазові платформи. Використання повновимірних блокових алгоритмів шифрування забезпечує надійність, але не задовольняє обмеженням щодо затримки та енергоспоживання. Подібні підходи практично непридатні для легких, дешевих одноразових FPV-дронів-камікадзе.

До третьої групи можна віднести праці, де розглядаються малоресурсні алгоритми, орієнтовані на енергоефективність та простоту реалізації, наприклад [23, 25]. Розглянуті в них алгоритми потенційно придатні для шифрування відеопотоку, однак їх криптостійкість не має теоретичного обґрунтування, а швидкодія не перевірена експериментально.

Решта робіт, такі як [17, 22, 31], описують експерименти з використанням традиційних алгоритмів шифрування, але демонструють суттєві затримки чи відсутність практичних результатів.

Щодо забезпечення завадостійкості каналів, у низці публікацій запропоновано застосування широкосмугових технологій, когнітивного радіо, MIMO-архітектур, алгоритмів багатоканальної компенсації завад та адаптивних методів кодування [31–34]. Ці підходи показують ефективність у протидії засобам РЕБ, однак не враховують одночасної потреби у шифруванні відеопотоку з мінімальною затримкою.

В дослідженнях [37–39] показано, що апаратні рішення на базі програмованої логіки надає можливість скоротити час обробки та знизити енергоспоживання, що відкриває перспективу апаратних рішень.

Таким чином, аналіз свідчить про відсутність готового комплексного рішення, здатного одночасно забезпечити потрібний криптографічний захист і достатню стійкість до радіоперешкод в режимі реального часу. Це створює передумови для розробки нових методів, що поєднують малоресурсне шифрування та корекцію помилок, які можна реалізовувати у вигляді легких та дешевих апаратно-програмних бортових модулів для БпЛА.

Невирішеність даного питання обумовлена об’єктивними причинами. Це, насамперед, стрімкий розвиток безпілотних технологій, особливо – БпЛА типу FPV, які суттєво змінили картину сучасних бойових дій. В результаті посилилися вимоги до швидкісних, масогабаритних та вартісних характеристик бортового електронного обладнання. З іншого боку, набагато більш короткий період життя таких апаратів дозволяє покращити характеристики каналу передачі відеоданих за рахунок зниження стійкості алгоритмів шифрування. Саме з цього випливає необхідність при подальших дослідженнях приділити найбільшу увагу малоресурсним алгоритмам шифрування при одночасному підвищенні їх завадостійкості.

Висновки

Огляд літературних джерел підтвердив, що наявні методи шифрування відеоданих, які передаються з безпілотних літальних апаратів, або забезпечують високу криптостійкість за рахунок задіяння надмірних ресурсів, або не гарантують достатньої криптостійкості. При цьому сучасні засоби радіоелектронної боротьби створюють суттєві перешкоди для каналу

передачі даних, тому завдання шифрування відеопотоку необхідно розглядати спільно з проблемою завадостійкості.

Жодне з відомих рішень не задовольняє одночасно вимогам як до швидкодії, енергоспоживання та крипостійкості, так і до потрібної стійкості щодо радіоперешкод, щоб їх можна було безпосередньо використати для створення систем передачі відеосигналу з FPV-дронів-камікадзе.

Ефективним шляхом зменшення затримки та енергоспоживання є використання апаратних рішень на базі ПЛІС або систем-на-кристалі, які дозволяють реалізувати у реальному часі паралельну реалізацію алгоритмів обробки відеопотоку, здійснюючи одночасно шифрування та корекцію помилок.

Отримані результати свідчать про потребу у створенні нової концепції захищеної завадостійкої системи передачі потокового відео з БпЛА, що базуватиметься на принципах тимчасової криптостійкості, адаптивної завадостійкості та апаратної оптимізації. Подальші дослідження мають бути спрямовані на моделювання таких систем, експериментальну перевірку їх ефективності та розробку прототипів для практичного використання на військових і цивільних безпілотних платформах.

Список літератури:

1. Hartmann K., Giles K. UAV exploitation: a new domain for cyber power. 2016 8th international conference on cyber conflict (CyCon), Tallinn, 31 May – 3 June 2016. Tallinn, 2016. P. 205–221. https://doi.org/10.1109/CYCON.2016.7529436.
2. Способи протидії FPV-дронам (з ворожого довідника «Тактика применения противником FPV-дронов и способы противодействия). Статті компанії «FPV-дрони та аксессуари для аеророзвідки». "FPV-дрони та аксессуари для аеророзвідки" – контакти, товари, послуги, ціни. Режим доступу: https://drone.in.ua/ua/a506352-sposobi-protidiyi-fpv.html.
3. Гліб, Керівник інструкторського напрямку БПЛА фонду «Повернись живим». Чому дрони не падають під РЕБом. Режим доступу: https://savelife.in.ua/materials/blogs/chomu-drony-ne-padayut-pid-rebom/.
4. Focus: Why jamming isn't a solution against FPV anymore in Ukraine's offensive initiative. Defense News security global military army equipment industry. Режим доступу: https://armyrecognition.com/news/aerospace-news/2024/focus-why-jamming-isnt-a-solution-against-fpv-anymore-in-ukraines-offensive-initiative.
5. Litnarovych V. Himera, Skiftech & More: How ukraine's defense tech companies are breaking into the US market. UNITED24 Media. Режим доступу: https://united24media.com/latest-news/himera-skiftech-more-how-ukraines-defense-tech-companies-are-breaking-into-the-us-market-6942.
6. Secure Real-Time Multimedia Data Transmission from Low-Cost UAVs with A Lightweight AES Encryption / N. Cecchinato et al. // IEEE communications magazine. 2023. Vol. 61, no. 5. P. 160–165. https://doi.org/10.1109/MCOM.001.2200611.
7. Drone defense system : patent US10339818B2 United States : G08G 5 / 00, H04W 76 /10. No. 15 /358574 ; applied on 22.11.2016 ; published on 25.05.2017. https://patentimages.storage.googleapis.com/96/9b/c4/04589f6c523d45/US10339818.pdf.
8. UAV anti-jamming video transmissions with qoe guarantee: a reinforcement learning-based approach / L. Xiao et al. // IEEE transactions on communications. 2021. Vol. 69, no. 9. P. 5933–5947. https://doi.org/10.1109/tcomm.2021.3087787.
9. Psilias D., Milidonis A., Voyiatzis I. Secure video transmission system for UAV applications / ed. by M. G. Vassilakopoulos, N. N. Karanikolas. Association for Computing Machinery, 2021. https://doi.org/10.1145/3503823.3503882.
10. Samanth S., K V P., Balachandra M. Security in internet of drones: a comprehensive review // Cogent engineering. 2022. Vol. 9, no. 1. https://doi.org/10.1080/23311916.2022.2029080.
11. Encryption and decryption of media data : patent EP3695560B1 United States : H04L 9/40, H04L 9/06, H04L 9/08, H04W 4/44. No. 18796555.3 ; applied on 12.10.2018 ; published on 09.10.2024, Bulletin no. 2024/41. https://data.epo.org/publication-server/rest/v1.2/publication-dates/2024-10-09/patents/EP3695560NWB1/document.pdf.
12. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions / S. Singh et al. // Journal of ambient intelligence and humanized computing. 2017. https://doi.org/10.1007/s12652-017-0494-4.
13. Гільгурт С. Аналіз вимог до системи передачі відеоінформації з FPV-дрона-камікадзе на наземну базову станцію // Проблеми інформатики та моделювання (ПІМ-2025) : Тези двадцять третьої міжнар. науково-техн. конф., м. Харків, 25–28 верес. 2025 р. Харків, 2025. С. 15. https://web.kpi.kharkov.ua/pim/?page_id=327.
14. Гільгурт С., Яблоков І. Застосування ПЛІС для захисту каналу передачі відеоінформації з БПЛА з використанням штучного інтелекту // Безпека сучасних інформаційно-комунікаційних систем : зб. доп. Міжнар. наук.-техн. конф. SMICS-2025, м. Львів, 16–18 жовт. 2025 р. Львів, 2025.

15. Survey on the authentication and key agreement of 6LoWPAN: open issues and future direction / F. F. Ashrif et al. // Journal of network and computer applications. 2024. Vol. 221. P. 103759. https://doi.org/10.1016/j.jnca.2023.103759.

16. Al-Ta'i Z. T. M., Ismael H. M. Authentication and encryption drone communication by using HIGHT lightweight algorithm // Turkish journal of computer and mathematics education. 2021. Vol. 12, no. 11. P. 5891–5908. https://www.researchgate.net/publication/392193717_Authentication_and_Encryption_Drone_Communication_by_Using_HIGHT_Lightweight_Algorithm.

17. A secure real-time multimedia streaming through robust and lightweight AES encryption in UAV networks for operational scenarios in military domain / N. Cecchinato et al. ; ed. by G. L. Foresti, C. Drioli. Elsevier B.V., 2022. Vol. 205. https://doi.org/10.1016/j.procs.2022.09.006.

18. Rahiyanath T. Y. A novel architecture for lightweight block cipher, piccolo // International journal of research in engineering and technology. 2015. Vol. 04, no. 09. P. 97–103. https://doi.org/10.15623/ijret.2015.0409017.

19. PRESENT: an ultra-lightweight block cipher / A. Bogdanov et al. Cryptographic hardware and embedded systems - CHES 2007. Berlin, Heidelberg. P. 450–466. https://doi.org/10.1007/978-3-540-74735-2_31.

20. Сафронов Т. AES-256: В Ukrspecsystems розкрили деталі шифрування даних БПЛА Shark. MILITARNY. https://militarnyi.com/uk/news/zahyst-danyh-vid-bpla-shark-posylyly-shyfruvannyam-aes-256/.

21. Belazi A., Migallón H. Drone-Captured wildlife data encryption: A hybrid 1D–2D memory cellular automata scheme with chaotic mapping and SHA-256 // Mathematics. 2024. Vol. 12, no. 22. P. 3602. https://doi.org/10.3390/math12223602.

22. Ozmen M. O., Yavuz A. A. Dronecrypt – an efficient cryptographic framework for small aerial drones // MILCOM 2018 - IEEE military communications conference, Los Angeles, CA, 29–31 October 2018. 2018. https://doi.org/10.1109/milcom.2018.8599784.

23. HANK-1, A new efficient and secure block cipher algorithm for limited resources devices / H. Eldeeb et al. The international conference on electrical engineering. P. 1–12. https://doi.org/10.21608/iceeng.2012.30662.

24. Special Publication 800-22 Revision 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Official edition. 2010. https://doi.org/10.6028/nist.sp.800-22r1a.

25. Ramudu S., Shanthi G. Implementation of an ultra-lightweight block cipher // International journal & magazine of engineering, technology, management and research. 2015. Vol. 2, no. 2. P. 233–242. http://www.ijmetmr.com/olfebruary2015/SriRamudu-GShanthi-39.pdf.

26. LWED: Lightweight white-box encryption communication system for drones over CARX algorithm / Y. Yang et al. // Journal of king saud university - computer and information sciences. 2023. P. 101727. https://doi.org/10.1016/j.jksuci.2023.101727.

27. WBZUC:novel white-box ZUC-128 stream cipher / Y. Yatao et al. // The journal of china universities of posts and telecommunications. 2023. Vol. 11, no. 78. P. 96–106. https://doi.org/10.19682/j.cnki.1005-8885.2022.0022.

28. Hei X., Song B., Ling C. SHIPHER: a new family of light-weight block ciphers based on dynamic operators // ICC 2017 - 2017 IEEE international conference on communications, Paris, France, 21–25 May 2017. 2017. https://doi.org/10.1109/icc.2017.7996731.

29. Lai X., Massey J. L. A proposal for a new block encryption standard. Advances in Cryptology – EUROCRYPT ’90. Berlin, Heidelberg, 1991. P. 389–404. https://doi.org/10.1007/3-540-46877-3_35.

30. A method of encrypting the traffic of quadrocopters through an A nalog path during monitoring of agricultural ground objects / Y. Meleshko et al. // National interagency scientific and technical collection of works. design, production and exploitation of agricultural machines. 2021. No. 51. P. 216–226. https://doi.org/10.32515/2414-3820.2021.51.216-226.

31. Evaluating the uav’s communication channels energy availability in the context of enemy electronic countermeasures / D. Bakhtiiarov et al. // 2024 IEEE 7th international conference on actual problems of unmanned aerial vehicles development (APUAVD), Kyiv, Ukraine, 22–24 October 2024. 2024. P. 159–164. https://doi.org/10.1109/apuavd64488.2024.10765900.

32. Jamming-Resistant AAV communications: a multichannel-aided approach / B. Wang et al. // IEEE wireless communications letters. 2025. Vol. 14, no. 7. P. 1939–1943. https://doi.org/10.1109/LWC.2025.3559501.

33. Liu Z., Jiang Y. Cross-Layer design for uav-based streaming media transmission // IEEE transactions on circuits and systems for video technology. 2022. Vol. 32, no. 7. P. 4710–4723. https://doi.org/10.1109/TCSVT.2021.3125864.

34. Bany Salameh H., Al-Obiedollah H., Aloqaily M. Secure batch-based resource allocation for green cognitive MIMO indoor flying networks // IEEE transactions on green communications and networking. 2024. Vol. 8, no. 3. P. 1090–1098. https://doi.org/10.1109/TGCN.2024.3387899.

35. Advanced method for compressing digital images as a part of video stream to pre-processing of UAV data before encryption / Z. Hu et al. // Springer Science and Business Media Deutschland GmbH, 2023. Vol. 181. https://doi.org/10.1007/978-3-031-36118-0_33.

36. Singandhupe A., La H. M., Feil-Seifer D. Reliable security algorithm for drones using individual characteristics from an EEG signal // IEEE access. 2018. Vol. 6. P. 22976–22986. https://doi.org/10.1109/ACCESS.2018.2827362.

37. Bakhtiiarov D., Konakhovych G., Lavrynenko O. Protected system of radio control of unmanned aerial vehicle // Institute of Electrical and Electronics Engineers Inc., 2016. https://doi.org/10.1109/MSNMC.2016.7783141.

38. Secure video and telemetry FPGA architecture for uavs / D. Psilias et al. // Institute of Electrical and Electronics Engineers Inc., 2024. https://doi.org/10.1109/SEEDA-CECNSM63478.2024.00021.

39. Real-Time compressed video encryption: based on quasigroup on system on chip (SOC) / D. Haridas et al. // SN computer science. 2021. Vol. 2, no. 5. https://doi.org/10.1007/s42979-021-00793-4.

Надійшла до редколегії 17.09.2025

Відомості про авторів:

Гільгурт Сергій Якович – д-р техн. наук, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, ст. наук. співробітник, зав. відділу математичного та економетричного моделювання; Україна; e-mail: hilgurt@ukr.net; ORCID: https://orcid.org/0000-0003-1647-1790

Ковальчук Людмила Василівна – д-р техн. наук, професор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, пров. наук. співробітник; Україна; e-mail: lusi.kovalchuk@gmail.com; ORCID: https://orcid.org/0000-0003-2874-7950

Давиденко Анатолій Миколайович – д-р техн. наук, професор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, пров. наук. співробітник; Україна; e-mail: davidenkoan@gmail.com; ORCID: https://orcid.org/0000-0001-6466-1690