

ДОСЛІДЖЕННЯ ТА АНАЛІЗ СИСТЕМ ЗАХИСТУ ЗВ'ЯЗКУ ТА ПРОТИДІЇ ВОРОЖИМ БПЛА

Вернигора В.Ю., науковий керівник Шкарупило В.В.

Безпілотні літальні апарати (БПЛА) відіграють дедалі важливішу роль у сучасних умовах як у військовій, так і в цивільній сферах. Однак активне використання дронів створює значні виклики в контексті забезпечення безпеки каналів зв'язку та протидії ворожим БПЛА. Надійний захист зв'язку між оператором і безпілотним апаратом є критично важливим для запобігання перехопленню керування, втрати управління або витоку чутливої інформації. Одночасно з цим, протидія ворожим БПЛА потребує розробки ефективних засобів виявлення, ідентифікації та нейтралізації потенційних загроз.

Метою даного дослідження є аналіз методів і технологій захисту зв'язку між пілотом і БПЛА, а також сучасних систем протидії ворожим безпілотним апаратам, із подальшим формуванням рекомендацій щодо підвищення ефективності цих систем у різних умовах експлуатації.

Розгляд методів захисту зв'язку включає дослідження технологій шифрування, автентифікації, частотного хопінгу (FHSS), використання VPN та засобів захисту від радіоелектронної боротьби (РЕБ). Також розглядається застосування SDR-рішень (програмно-конфігурованих радіостанцій) для динамічного перемикання каналів та протоколів у режимі реального часу.

GPS є ключовим елементом управління БПЛА, оскільки забезпечує точне визначення місцезнаходження апарату, стабільну траєкторію польоту та автономний контроль, що важливо для підтримки зв'язку і запобігання втраті контролю. Воно також необхідне для виконання завдань, таких як моніторинг або доставка вантажу, та забезпечує безпеку, дозволяючи БПЛА повертатися до бази або приймати інші заходи у разі потреби [1].

Криптографія дозволяє вирішити ряд завдань, серед яких – захист цілісності передаваної інформації та забезпечення виконання апаратом команд лише від легітимного передавача (тобто автентифікація оператора), що підкреслює важливість шифрування для захисту каналу зв'язку від несанкціонованого доступу. Методи частотного переплутування дозволяють змінювати частоту передачі сигналу відповідно до певного алгоритму, що ускладнює перехоплення сигналу та підвищує захищеність зв'язку, що допомагає уникнути виявлення і перехоплення сигналів ворожими силами [2].

Відомо, що GCS використовується для бездротового зв'язку з дроном, щоб стежити за тим, куди він летить, встановлювати маршрутні точки або виконувати нові команди. Він реалізує протокол послідовного з'єднання MAVlink, що створює додаткові ризики перехоплення або втручання в процес управління при відсутності належного захисту. Прикладами програмного забезпечення GCS є: QGroundControl, Mission Planner, APM Planner. [3].

Контролери польоту, які обробляють сигнали від пілота, сенсорів та здійснюють стабілізацію польоту, виконують ключову роль у забезпеченні стабільності та навігації БПЛА. Залежно від призначення, в таких контролерах можуть застосовуватись мікроконтролери з архітектурами FPGA, ARM, Atmel та Raspberry Pi, що визначає рівень обчислювальної потужності, можливість реалізації складних алгоритмів обробки даних та шифрування, а також стійкість до зовнішніх впливів [4].

У роботі буде проведено порівняння ефективності цих технологій в умовах впливу перешкод, спроб глушіння та несанкціонованого втручання.

Аналіз систем протидії ворожим БПЛА охоплює пасивні та активні методи виявлення — радарні, акустичні, оптико-електронні сенсори, а також методи нейтралізації, включаючи радіочастотні подавлювачі, перехоплення сигналу керування, кінетичне ураження (наприклад, засобами ППО або дрон-дронами) та системи лазерного ураження. Окрема увага приділяється сучасним комплексам типу DroneShield, Dedrone, EnforceAir, які реалізують багаторівневий підхід до захисту повітряного простору.

Основою невогневого ураження системи є комплекси радіоелектронної боротьби (РЕБ), призначенням якого є порушення управління БПЛА з наземних та повітряних пунктів управління, зниження ефективності його бойового застосування, обмеження можливостей добування інформації за допомогою радіоелектронних засобів (РЕЗ), які розміщені на БПЛА [5].

У дослідженні буде проведено оцінку вразливостей систем зв'язку БПЛА до різних типів атак.

На основі отриманих результатів буде сформовано рекомендації щодо впровадження комбінованих підходів до захисту: інтеграція криптографічного захисту з адаптивним управлінням частотами, впровадження систем машинного навчання для автоматичного виявлення підозрілих об'єктів, використання мультисенсорних систем моніторингу та протидії.

Очікувані результати дослідження включають визначення оптимальних методів захисту зв'язку та ефективних стратегій нейтралізації ворожих БПЛА для підвищення стійкості безпілотних систем у сучасному інформаційно-бойовому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Танасійчук С., Говорущенко Т. Аналіз методів управління бпла(gps позиціонування та інтелектуальні методи управління). *Вісник Хмельницького національного університету*. 2024. Т. 331 : Технічні науки. С. 462–468. URL: <https://heraldts.khmnpu.edu.ua/index.php/heraldts/article/view/183>
2. Кутень Р. Б., Ахмедова А. С. Підвищення рівня захищеності та життєздатності безпілотних авіаційних пристроїв. *Український науковий журнал інформаційної безпеки*. 2024. Т. 30 : Безпека інформації. С. 88–94. URL: <https://jrnlnau.edu.ua/index.php/Infosecurity/article/view/18609>
3. Кучеренко О. І., Вакалюк Т. А. Огляд технічних та програмних засобів керування бпла. *ВІСНИК ХНТУ*. 2024. Т. 2 : Інформаційні Технології. С. 170–176. URL: https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/643/617
4. Дуднік А., Тищенко О., Яременко Д. Огляд сучасних технічних та програмних рішень для управління бпла. *Інформаційні технології та суспільство*. 2024. Т. 4(15). С. 44–50. URL: <https://journals.maup.com.ua/index.php/it/article/view/4581>
5. Шевчук В., Кривошеєв В., Швець М. Вимоги до системи боротьби з безпілотними літальними апаратами. *Modern Information Technologies in the Sphere of Security and Defence*. 2023. Т. 47(2) : Інтерактивні моделі розвитку науково-освітнього простору у сфері безпеки та оборони. С. 133–138. URL: <https://sit.nuou.org.ua/article/view/285170>

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
*24 квітня 2025 року***

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів