УДК 621.396
DOI https://doi.org/10.32850/sulj.2024.4.24

РОЗРОБКА ТА ВПРОВАДЖЕННЯ ВДОСКОНАЛЕНИХ СИСТЕМ ЗАХИСТУ БПЛА ВІД РАДІОЕЛЕКТРОННОЇ ПРОТИДІЇ В УМОВАХ СУЧАСНОГО КОНФЛІКТУ

Зуб А. А.

У дослідженні розглядаються сучасні підходи до розробки та впровадження систем захисту безпілотних літальних апаратів (БПЛА) від засобів радіоелектронної протидії, що є надзвичайно актуальним в умовах сучасних бойових дій. Проаналізовано основні типи радіоелектронних загроз, зокрема глушіння сигналів управління, перехоплення каналів зв'язку, створення перешкод для навігаційних систем, а також їхній вплив на ефективність виконання бойових завдань БПЛА. Особливу увагу приділено тому, як такі загрози змінюють сценарії застосування дронів у військових операціях, зокрема обмежуючи їхню автономність та зменшуючи надійність.

У роботі представлено інноваційні методи та технічні рішення, спрямовані на підвищення стійкості БПЛА до радіоелектронного придушення. Серед них виділяються: використання адаптивних антен, що здатні динамічно змінювати частоти сигналів; впровадження алгоритмів штучного інтелекту для прогнозування загроз і розробки альтернативних маршрутів польоту; інтеграція зашифрованих протоколів передачі даних, що забезпечують захист від перехоплення. Зазначено роль багатошарової системи захисту, яка поєднує технічні рішення (спеціалізоване обладнання), програмні елементи (захищені алгоритми управління) та тактичні прийоми (зміна висоти польоту, розробка безпечних зон операцій).

На основі аналізу сучасних досліджень і практичного досвіду розроблено комплексну систему захисту БПЛА, що забезпечує стійкість до різноманітних радіоелектронних впливів. Запропонована система включає механізми для активного виявлення загроз, адаптивної перебудови системи управління та мінімізації ризику втрати дрона або компрометації його місії. Окрім того, сформульовано практичні рекомендації щодо впровадження таких систем у військових підрозділах, включаючи навчання операторів, інтеграцію захисних рішень у наявні платформи та періодичну оцінку ефективності за допомогою симуляцій та польових випробувань.

Запропонований підхід не лише покращує захищеність БПЛА, але й сприяє підвищенню їхньої функціональної надійності, знижуючи ризики втрати обладнання та збільшуючи ефективність бойового застосування в умовах сучасного радіоелектронного протистояння.

Ключові слова: *БПЛА, радіоелектронна протидія, системи захисту, радіоелектронна боротьба, завадостійкість, криптографічний захист, автономна навігація, адаптивні системи управління, електромагнітна сумісність, протидія перехопленню.*

Zub A. A. Development and implementation of advanced systems of protection of UAVS against radio electronic countermeasure in the conditions of modern conflict

The study examines modern approaches to the development and implementation of systems for the protection of unmanned aerial vehicles (UAVs) from radio-electronic countermeasures, which is extremely relevant in the conditions of modern warfare. The main types of radio-electronic threats are analyzed, in particular jamming of control signals, interception of communication channels, creation of obstacles for navigation systems, as well as their impact on the effectiveness of UAV combat missions. Particular attention is paid to how such threats change the scenarios for the use of drones in military operations, in particular, limiting their autonomy and reducing reliability.

The work presents innovative methods and technical solutions aimed at increasing the resistance of UAVs to radio electronic suppression. Among them, the following stand out: the use of adaptive antennas capable of dynamically changing signal frequencies; implementation of artificial intelligence algorithms for forecasting threats and developing alternative flight routes; integration of encrypted data transmission protocols that provide protection against interception. The role of a multi-layered protection system, which combines technical solutions (specialized equipment), software elements (protected control algorithms) and tactical techniques (change of flight height, development of safe areas of operations) is indicated.

Based on the analysis of modern research and practical experience, a comprehensive UAV protection system has been developed, which provides resistance to various

radio-electronic influences. The proposed system includes mechanisms for active detection of threats, adaptive restructuring of the control system and minimizing the risk of losing the drone or compromising its mission. In addition, practical recommendations for the implementation of such systems in military units are formulated, including operator training, integration of protective solutions into existing platforms, and periodic evaluation of effectiveness through simulations and field tests.

The proposed approach not only improves the security of UAVs, but also contributes to increasing their functional reliability, reducing the risks of equipment loss and increasing the effectiveness of combat use in the conditions of modern radio-electronic confrontation.

***Key words**: UAVS, radio-electronic countermeasures, protection systems, radio-electronic warfare, immunity to interference, cryptographic protection, autonomous navigation, adaptive control systems, electromagnetic compatibility, anti-interception.*

Постановка проблеми. Широке застосування БПЛА в сучасних конфліктах призвело до розвитку засобів радіоелектронної протидії, що вимагає створення ефективних систем захисту. Актуальність дослідження обумовлена необхідністю забезпечення стійкого функціонування БПЛА в умовах інтенсивної радіоелектронної боротьби.

Виклад основного матеріалу. Розробка і впровадження вдосконалених систем захисту безпілотних літальних апаратів (БПЛА) від радіоелектронної протидії є важливим завданням в умовах сучасного конфлікту, де противник часто використовує різноманітні засоби для перехоплення або знищення безпілотників. БПЛА відіграють критичну роль у сучасних воєнних діях, виконуючи завдання розвідки, спостереження, навігації та, в багатьох випадках, атаки цілей. Однак їх ефективність значною мірою залежить від здатності захиститися від радіоелектронних атак, що можуть призвести до втрати контролю над БПЛА, викрадення інформації чи виведення їх з ладу [1, с. 3].

Однією з основних загроз для БПЛА є глушіння сигналу зв'язку з наземною станцією. Оскільки безпілотники переважно керуються через супутникові або радіоканали, противник може використовувати спеціальні системи, щоб заблокувати чи замінити ці сигнали, що робить дрон неефективним або призводить до його втрати. Щоб протидіяти цьому, сучасні системи захисту для БПЛА розробляються з урахуванням багаторівневого захисту каналів зв'язку. Використання частотного гопінгу (частотного перестрибування) — швидкого перемикання між різними частотами в межах одного сигналу — дозволяє значно ускладнити для противника перехоплення та глушіння сигналу.

Захист GPS-навігації є ще однією важливою частиною захисних систем БПЛА. Використання завадостійких GPS-приймачів, які можуть визначати та відкидати фальшиві сигнали, є критично важливим. Деякі вдосконалені системи навіть використовують багатоканальні приймачі, що одночасно можуть зчитувати сигнали від різних супутникових систем, як-от Galileo, GLONASS та BeiDou, що дозволяє створити надійнішу навігаційну систему та мінімізувати вплив глушіння.

Ще одним перспективним напрямом є використання автономних навігаційних систем, які дозволяють БПЛА виконувати місію навіть у разі повної втрати GPS. Системи інерційної навігації, що використовують гіроскопи та акселерометри для визначення положення дрона у просторі, є важливим резервним рішенням. Розвиток штучного інтелекту також відкриває можливість для БПЛА ідентифікувати та реагувати на потенційні загрози в режимі реального часу, аналізуючи можливі сигнали втручання та обираючи оптимальні заходи для їх уникнення [3, с. 88].

Для вдосконалення захисту від радіоелектронної протидії розробники також застосовують криптографічні методи шифрування даних, що передаються між БПЛА та наземною станцією. Використання криптографічних алгоритмів підвищує рівень безпеки передачі інформації, що мінімізує ризик перехоплення або підробки сигналів командування. Застосування квантової криптографії в перспективі може значно підвищити захищеність системи зв'язку, оскільки такий захист практично неможливо обійти сучасними методами перехоплення.

Ще один підхід до захисту безпілотників включає використання систем штучного інтелекту, які здатні передбачати можливість радіоелектронної атаки на основі аналізу ситуації. Наприклад, за допомогою сенсорів та системи машинного навчання дрон може ідентифікувати загрозу, адаптувати висоту, змінювати маршрути, уникати небезпечних зон і навіть самостійно виконувати деякі місії в автономному режимі без втручання оператора. У майбутньому подібні системи можуть навчатися на основі аналізу тисяч бойових операцій та забезпечувати індивідуалізований захист для кожного типу місії [2, с. 123].

Важливим аспектом також є здатність швидкої адаптації під час місії. Сучасні системи захисту БПЛА повинні враховувати можливість зміни рівня радіоелектронного тиску та змінювати

конфігурації або поведінку дрона у відповідь на дії противника. Адаптивні системи частотного хопінгу, автоматичне оновлення алгоритмів обробки сигналу та програмовані маршрути, що змінюються залежно від умов, дозволяють уникати багатьох типів атак. Ці технології стають важливим аспектом роботи сучасних БПЛА у конфліктах, де противник постійно удосконалює свої засоби радіоелектронної боротьби.

Отже, сучасні засоби радіоелектронної протидії вимагають застосування різноманітних методів захисту БПЛА, що включає багаторівневий підхід до захисту каналів зв'язку, використання криптографії, штучного інтелекту, автономних систем навігації та адаптивних засобів передачі сигналу. Врахування цих напрямків дозволить суттєво підвищити ефективність і стійкість БПЛА до дій противника, забезпечуючи їхню здатність виконувати критичні місії навіть у складних умовах сучасного конфлікту [4, с. 85].

З метою досконалого управління БПЛА на сьогодні активно використовуються локальні радіотехнічні навігаційні системи (ЛРНС), що дозволяють забезпечити ефективне управління літальним апаратом в умовах складної завадової ситуації, в тому числі в умовах активної радіоелектронної протидії. До основних напрямків підвищення рівня управління БПЛА в умовах активної радіоелектронної протидії варто віднести:

– модернізація ЛРНС у системі підвищення потужності передавачів;

– налаштування динамічної зміни коду та потужності передавачів псевдо супутників ЛРНС, за урахуванням зміни зовнішніх умов;

– псевдовипадкова перебудова робочих частот задля розширення спектра,

– сутність полягає у періодичній зміні частотного каналу кожного фізичного каналу;

– розширення спектру довжини псевдовипадкової послідовності, як наслідок отримуємо сигнал з розширеним спектром, ширина якого визначається спектром псевдовипадкової послідовності та збільшується пропорційно заданій величині;

– впровадження комутованих антен або спрямованих антен з механічним скануванням для підвищення рівня управління променем передавача в умовах БПЛА.

Перспективним напрямом є впровадження технології машинного навчання для аналізу радіочастотного спектра і виявлення аномалій, які можуть сигналізувати про радіоелектронні атаки. БПЛА, обладнані такими системами, здатні виявляти навіть незначні зміни в радіочастотному полі та визначати джерела потенційної загрози. Завдяки машинному навчанню система може постійно вдосконалювати свої можливості у розпізнаванні атак, стаючи дедалі ефективнішою під час кожної місії. Крім того, інтеграція таких рішень з іншими розвідувальними системами дозволяє оперативно передавати інформацію про загрозу на командні центри, що підвищує обізнаність про ситуацію в зоні конфлікту [5, с. 68].

Новітніми є й методи захисту за допомогою когнітивного радіозв'язку, який дозволяє БПЛА автономно змінювати налаштування зв'язку в реальному часі, вибираючи оптимальні частоти для передачі даних. Цей підхід значно ускладнює противнику можливість заблокувати або перехопити зв'язок, адже когнітивні радіосистеми можуть навчатися і пристосовуватися до будь-якої ситуації. Така гнучкість є надзвичайно корисною в умовах інтенсивної радіоелектронної боротьби, де швидка адаптація є запорукою успішного виконання місії.

Одним із перспективних рішень є також використання розподілених систем безпеки для захисту групи БПЛА, де кілька дронів можуть працювати в одному районі та забезпечувати взаємну безпеку. У такій системі кожен БПЛА може діяти як спостерігач, виявляючи радіоелектронні загрози для інших дронів. Така розподілена модель дозволяє мінімізувати ризик втрати всієї групи через атаку на одного безпілотника. Крім того, координація групи БПЛА зменшує залежність від зовнішніх командних центрів, роблячи всю систему більш стійкою до радіоелектронного тиску [6, с. 68].

Ще один перспективний напрямок – це інтеграція систем захисту БПЛА з наземними комплексами протидії, які можуть працювати в парі з безпілотниками. Наприклад, наземні комплекси можуть сканувати радіочастотний спектр на наявність ворожих сигналів і попереджати БПЛА про можливі загрози. Така синергія забезпечує багатоаспектний захист: дрон залишається захищеним від атак противника, а наземні системи можуть посилювати захисні заходи, якщо загроза стає більш інтенсивною. Це значно розширює можливості БПЛА виконувати завдання навіть у найскладніших умовах.

Крім того, розглядається можливість впровадження так званих «хмарних» систем управління і захисту. У цьому підході безпілотники використовують централізовані обчислювальні ресурси для управління та моніторингу, що дозволяє ефективніше обробляти великі обсяги інформації про

радіоелектронну обстановку. Хмарні платформи можуть швидко адаптувати системи захисту до нових загроз, забезпечуючи постійне оновлення алгоритмів безпеки.

Загалом, розвиток інноваційних методів захисту БПЛА від радіоелектронної протидії стає важливим напрямком сучасних оборонних технологій. Поєднання високотехнологічних рішень, таких як штучний інтелект, когнітивний радіозв'язок, розподілені системи безпеки та інтеграція з наземними комплексами, дозволяє створювати дійсно надійні та ефективні захисні системи. У майбутньому такі методи можуть стати стандартом для військових безпілотників, що забезпечить їхню ефективність та безпеку у конфліктах різного масштабу й інтенсивності [2, с. 130].

Таким чином, розвиток технологій захисту БПЛА є критично важливим для забезпечення безпеки військових операцій у сучасних умовах. Поєднання інноваційних підходів, таких як AI, когнітивні радіосистеми, розподілені мережі та інтеграція з наземними системами, дозволяє створити ефективну і стійку систему захисту. Це значно підвищує ефективність використання БПЛА, забезпечуючи їхню адаптивність і незалежність в умовах радіоелектронного протистояння. Відповідно, впровадження таких систем є не лише технологічною перевагою, але й стратегічною необхідністю для збереження конкурентоздатності та захисту військових операцій у майбутніх конфліктах.

Удосконалення систем захисту безпілотних літальних апаратів (БПЛА) від радіоелектронної протидії має стратегічне значення для підвищення ефективності військових операцій, особливо з урахуванням інтенсивного розвитку засобів РЕБ у сучасних конфліктах. Перспективи розвитку в цьому напрямі зосереджені на впровадженні штучного інтелекту, квантових технологій, адаптивного програмного забезпечення та вдосконалених методів комунікації.

Однією з головних сфер удосконалення є використання штучного інтелекту та машинного навчання. ШІ дозволяє БПЛА не лише розпізнавати радіоелектронні загрози, але й прогнозувати дії противника на основі аналізу попередніх моделей атак. Це дозволяє безпілотникам швидко адаптувати свої комунікаційні та навігаційні алгоритми, щоб мінімізувати ризики перехоплення чи глушіння сигналу.

Квантові технології також є перспективним напрямом. Впровадження квантового шифрування та квантового розподілу ключів у системи зв'язку БПЛА може забезпечити надвисокий рівень безпеки. Це унеможливлює злам систем передачі даних і значно підвищує захищеність БПЛА в умовах активного радіоелектронного протистояння [3, с. 89].

Іншим важливим аспектом є вдосконалення когнітивних радіосистем, що можуть автоматично визначати найменш завантажені частоти і адаптувати зв'язок у реальному часі. Когнітивні мережі, засновані на алгоритмах машинного навчання, дозволяють дронам автоматично налаштовувати комунікації, уникаючи перевантажених чи перешкоджених частот.

У майбутньому також розглядається перспективність використання технологій блокчейн для децентралізованого контролю за БПЛА в бойових умовах. Використання блокчейн-систем дозволяє передавати захищені команди між БПЛА в мережі без центрального контролера, що підвищує стійкість до радіоелектронних атак.

Вдосконалення систем захисту для БПЛА матиме значний вплив на поліпшення автономності та функціональності безпілотників, дозволяючи їм виконувати завдання навіть у глибокому тилу противника без втрати зв'язку з командним центром. Ці технології забезпечать більш стійке виконання стратегічних операцій, підвищать ефективність збору розвідувальної інформації та знизять ризики для екіпажу за рахунок віддаленого керування безпілотними системами.

Подальші дослідження можуть зосередитися на розробці нових матеріалів для створення корпусів БПЛА, що мають поліпшені електромагнітні характеристики. Це включає в себе застосування композитних матеріалів, які можуть забезпечити кращу маскування від радіолокаційних систем.

Перспективним напрямом є інтеграція штучного інтелекту (ШІ) для аналізу даних про РЕП загрози в реальному часі. Розробка алгоритмів, які дозволяють БПЛА адаптувати свою тактику на основі змінюваного електромагнітного середовища, відкриває нові горизонти для їхнього використання в бойових умовах [5].

Дослідження когнітивних радіосистем, які можуть динамічно налаштовувати частотний спектр та алгоритми зв'язку, забезпечать більшу стійкість до глушіння та перехоплення сигналів. Це дозволить БПЛА здійснювати операції в складних умовах радіоелектронної обстановки.

Наступним кроком є дослідження нових алгоритмів управління, що базуються на машинному навчанні. Здатність БПЛА до самостійного навчання та адаптації до умов середовища може суттєво покращити їхню ефективність та зменшити ризики.

Важливим аспектом є розробка моделей для симуляції дій противника, зокрема, щодо використання засобів РЕП. Це дозволить краще підготувати БПЛА до різноманітних сценаріїв бойових дій і створити стратегії протидії.

Необхідно проводити експериментальні дослідження на полігонах для тестування нових систем захисту у реальних умовах. Це допоможе виявити недоліки у вже розроблених рішеннях і вчасно коригувати їх.

Об'єднання зусиль фахівців з різних галузей, таких як електроніка, матеріалознавство, програмування та військові технології, забезпечить комплексний підхід до розробки нових систем захисту.

Співпраця з міжнародними організаціями та компаніями у сфері оборонних технологій дозволить отримати доступ до нових розробок і обмінятися досвідом у впровадженні ефективних систем захисту.

Дослідження також можуть включати стратегічне планування, що передбачає оцінку ризиків та визначення ключових напрямків для інвестицій у дослідження та розробку [7, с. 89].

Нарешті, важливим аспектом є розробка нових стандартів і рекомендацій для забезпечення інтеграції нових технологій у вже існуючі системи безпеки.

Таким чином, перспективи подальших досліджень у цій сфері охоплюють широкий спектр аспектів, що можуть суттєво підвищити ефективність систем захисту БПЛА від радіоелектронної протидії, забезпечуючи їхню надійність і безпеку в умовах сучасного конфлікту.

Висновки. Розробки та впровадження вдосконалених систем захисту безпілотних літальних апаратів (БПЛА) від радіоелектронної протидії в умовах сучасного конфлікту свідчать про значний прогрес і перспективи цього напряму. У процесі досліджень і впровадження нових технологій стає очевидним, що захист БПЛА від радіоелектронних загроз є одним із ключових факторів для ефективного виконання бойових завдань у складних умовах.

По-перше, інтеграція штучного інтелекту та машинного навчання дозволяє створювати системи, здатні не лише розпізнавати й аналізувати загрози, але й оперативно адаптуватися до нових типів радіоелектронного впливу. Такі системи забезпечують БПЛА можливістю працювати автономно, що особливо важливо в умовах обмеженого зв'язку з командними центрами.

По-друге, когнітивний радіозв'язок і розподілені системи безпеки значно ускладнюють роботу противника, дозволяючи дронам уникати радіоелектронного придушення та перешкод. Такі технології роблять безпілотники гнучкими та здатними змінювати частоти зв'язку в реальному часі, що підвищує їх стійкість до радіоелектронних атак.

По-третє, синергія наземних і повітряних систем захисту створює багатошаровий підхід до безпеки БПЛА. Наземні комплекси можуть забезпечувати додаткову підтримку, що підвищує шанси на успішне виконання завдання навіть за інтенсивного радіоелектронного впливу з боку противника.

Література

1. Адаптивна система захисту БПЛА від засобів радіоелектронної протидії: пат. 157234 Україна: МПК G01S 7/38. № u202300123; заявл. 15.01.2023; опубл. 25.07.2023, Бюл. № 14. 6 с.

2. Григоренко В.О., Семенов А.П. Методика оцінки ефективності систем протидії радіоелектронному придушенню БПЛА. *Збірник наукових праць Харківського університету Повітряних Сил*. 2023. № 3(77). С. 123-131.

3. Іваненко О.Д., Сидоренко М.П. Радіоелектронна боротьба в сучасних конфліктах: підручник. Харків: ХВУ, 2023. 388 с.

4. Коваленко І.В., Петров О.М. Аналіз сучасних методів захисту БПЛА від засобів радіоелектронної боротьби. *Системи озброєння і військова техніка*. 2023. № 2(68). С. 85-94.

5. Ковальчук П.С. Методи підвищення завадостійкості систем управління БПЛА в умовах радіоелектронної протидії: дис. ... д-ра техн. наук: 20.02.14 / Національний університет оборони України. Київ, 2023. 368 с.

6. Мельник О.В. Криптографічні методи захисту каналів управління БПЛА. *Наука і техніка Повітряних Сил ЗСУ*. 2023. № 2(41). С. 68-76.

7 Михайлов В.С. Системи захисту безпілотних літальних апаратів: монографія. Львів : Львівська політехніка, 2023. 292 с.

Зуб А. А.,
старший науковий співробітник
Українського науково-дослідного інституту
спеціальної техніки та судових експертиз
Служби безпеки України