УДК 623.746.-519

С. О. Гладкий

РОЗВИТОК РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ В УМОВАХ ВІЙНИ ІЗ ЗАСТОСУВАННЯМ ДРОНІВ

Вінницький національний технічний університет
Кафедра військової підготовки

Анотація
Запропоновано заходи захисту каналу управління дроном, враховуючи можливі загрози радіоелектронної боротьби при плануванні маршруту польоту дрона та виборі зони польоту дрону.
Ключові слова: безпілотні літальні апарати, радіоелектронна боротьба, дрон, канал зв'язку, маршрут.

Abstract
Proposed measures to protect the drone control channel, taking into account the possible threats of radio-electronic warfare when planning the drone flight route and choosing the drone flight zone.
Keywords: unmanned aerial vehicles, electronic warfare, drone, communication channel, route.

Вступ

У військових конфліктах та війнах останнім часом стає все більше популярним використання безпілотних літальних апаратів (дронів). Їх застосування дозволяє отримати розвідувальну інформацію, а також здійснювати удари по ворогу та бойової техніки без втрат особового складу. Проте, з поширенням використання дронів з'являється нове завдання для військових – боротьба з ними за допомогою радіоелектронної боротьби.

Радіоелектронна боротьба – це комплекс заходів, спрямованих на забезпечення безпеки власних військових об'єктів, а також на порушення роботи електронних засобів противника. Застосування радіоелектронної боротьби дозволяє знизити ефективність дій ворога, завдяки перешкоджанню його зв'язку і використанню електронно-технічних засобів (далі – РЕБ). [1]

Застосування дронів у війні може бути порівняне з розвитком літаків у Першу світову війну. Наприклад, можуть виникати проблеми з навігацією та керуванням дронами, а також забезпечення безпеки даних, зібраних за допомогою дронів. Крім того, використання дронів може призвести до цивільних жертв, особливо в разі неправильного визначення цілей для атак.

Отже, використання дронів у війні має як свої переваги, так і недоліки, і вимагає уважного аналізу та розробки відповідних стратегій та правил використання.

Основна частина

Одним з найважливіших елементів дронів є система керування, які забезпечують їхню навігацію та керування. Військові можуть використовувати радіоелектронну боротьбу для перешкоджання роботі цих систем. Наприклад, за допомогою системи підриву сигналів (jamming) можна змінювати або перешкоджати передачі сигналів між дроном та його пультом керування. Таким чином, дрон може стати неспроможним до виконання команд пілота або втратити зв'язок з ним повністю.

Розробники БПЛА постійно працюють над покращенням систем керування та навігації, щоб зменшити їх вразливість до радіоелектронної боротьби. Вони можуть використовувати складніші алгоритми передачі сигналів або застосовувати системи автоматичного повторення сигналів для забезпечення стабільного зв'язку. Крім того, можуть застосовувати системи інтегрованої навігації, які використовують багато датчиків для визначення точного положення дрона у просторі. Такі системи дозволяють забезпечити точну навігацію навіть у разі втрати зв'язку з контролером дрона.

Крім того, військові можуть використовувати різноманітні засоби захисту від радіоелектронної боротьби, такі як системи антиджемінгу (antijamming), які дозволяють здійснити перехід на інший

канал зв’язку в разі перешкоджання на поточному каналі. Також можуть використовувати захисні системи, такі як шифрування зв’язку та системи захисту від перешкод. Використовують дрони з автономним керуванням, які не потребують зв’язку з оператором та можуть самостійно приймати рішення в умовах радіоелектронної боротьби.

Загалом, хоча радіоелектронна боротьба може вплинути на роботу БПЛА, розробники постійно працюють над покращенням системи керування та навігації, а військові застосовують різні засоби захисту.

Розглянемо заходи для збереження управління БПЛА під час дії РЕБ.

Захист каналу управління дроном від РЕБ може бути забезпечений за допомогою різноманітних заходів технічного та організаційного характеру. Одним з можливих заходів- це використання шифрування сигналу управління, що дозволить забезпечити безпеки передачі даних та унеможливить їх перехоплення. Крім того, можливо застосування технічних засобів захисту, таких як фільтр та інші засоби підвищення захисту від електромагнітного впливу.

Для запобігання блокування сигналу управління можна застосувати резервні канали зв’язку, які дозволяють керувати дроном навіть у разі блокування основного керування.

Важливим заходом є організація періодичної перевірки роботи радіоелектронного обладнання та вчасне виявлення та локалізація РЕБ. Необхідно враховувати можливу загрозу РЕБ при плануванні маршруту та виборі зони польоту дрону, уникаючи потенційно небезпечних зон.

Принцип використання резервних каналів зв’язку для управління дроном полягає в тому, щоб мати можливість забезпечити безперебійний зв’язок з дроном у випадку, коли основний канал зв’язку втратить зв’язок. Зазвичай, безпілотні літальні апарати оснащені двома каналами: основним і резервним. Основний канал зазвичай є бездротовий, наприклад, радіо- або GSM-зв’язок, а резервний канал може бути дротовим, наприклад, Internet або USB-зв’язок. Коли з’єднання з основним каналом втрачається, здійснюється автоматичне перемикання на резервний канал, щоб забезпечити безперебійну роботу. Такі системи автоматичного перемикання на резервний канал зв’язку можуть бути програмовані з використанням алгоритмів вирішення проблем, таким як частотні перешкоди або переви в зв’язку. Крім того, додатковий захист може бути забезпечений шляхом використання шифрування для збереження приватності і недоступності противникам, які можуть намагатися здійснити зв’язок з дроном.

Для врахування можливих загроз РЕБ при плануванні маршруту польоту дрона та вибору зони його польоту необхідно виконати наступні кроки:

- Дослідити регіон, де планується виконувати політ. Дізнатися про наявність потенційних загроз РЕБ в цьому районі, наприклад, про можливість наявності супутникової та радіоелектронної забороненої зони.
- Використовувати технології, які дозволяють визначити геолокацію БПЛА в режимі реального часу та забезпечення можливості віддаленого керування. Це дозволить вам контролювати політ дрона та уникнути небезпечних зон.
- Потрібно дбати про безпеку даних та забезпечувати захист передачі даних між дроном та пультом керування. Для цього використовуйте шифрування та інші технології захисту даних.
- Користуватися спеціальними додатками для планування маршруту дрона, що дозволяють враховувати можливі загрози РЕБ.

Розглянемо додатки.

Існують різноманітні додатки для планування маршруту, які дозволяють враховувати можливі загрози РЕБ. Деякі з цих додатків мають вбудовані системи автоматичного виявлення радіосигналів, які можуть розпізнавати заборонені радіочастоти та інші радіозакриття і враховувати їх у процесі планування маршруту.

Одним із таких є “Ardupilot”, який є відкритим програмним забезпеченням для автопілотів дронів. Він має вбудовані функції планування маршруту, які дозволяють враховувати можливі загрози РЕБ.

Іншим зразком є “Drone Harmony”, який також дозволяє планувати маршрути для дронів з урахуванням загроз РЕБ. Цей додаток використовує вбудовані системи виявлення радіосигналів, щоб ідентифікувати заборонені радіочастоти та інші загрози.

Крім того, існують додатку, які дозволяють користувачам відстежувати інтерференцію радіосигналів та робити прогнози щодо можливих загроз. Один із таких застосунків – “RF Explorer for Windows”, що дозволяє відстежувати радіосигнали та заборонені радіочастоти в режимі реального часу.

У будь-якому випадку, перед використанням будь-якого додатку для планування маршруту дрона, необхідно докладно ознайомитись з інструкціями та забезпечити відповідну підготовку для забезпечення безпеки польоту дрону.

Висновок

Застосування засобів захисту та використання додатків для планування маршрутів можуть забезпечити безпечну експлуатацію дронів та ефективну протидію РЕБ під час ведення бойових дій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бакуменко Б.В. Тактика радіотехнічних військ. Х.: ХУПС, 2007.
2. Основи РЕБ в радіотехнічних військах. Конспект лекцій за ред. І.С. Добриніна- Харків: Стиль-Іздат, 2006

Гладкий Станіслав Олександрович – студент групи 01-21 кафедри військової підготовки, Вінницький національний технічний університет, м. Вінниця, e-mail:hladkiys@gmail.com

Hladkyi Stanislav O. – student of group 01-21, Department of Military Training, Vinnitsa National Technical University, Vinnitsa, e-mail: hladkiys@gmail.com