УДК 621.396.96:004.056]:623.746-519
DOI: https://doi.org/10.30837/IYF.IRTTPI.2024.460

МЕТОДИ ЗАБЕЗПЕЧЕННЯ СКРИТНОСТІ КАНАЛІВ УПРАВЛІННЯ БПЛА

Компанієць С.О.
Науковий керівник – к.т.н., доц. Іванова О.О.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
e-mail:stanislav.kompaniiets@nure.ua

Considered topical issues related to ensuring the secrecy of UAV control channels from radio-technical intelligence. The general characteristics of the technical means of UAV detection are given. The problem of ensuring energy stealth of UAV ground control points is considered. Practical recommendations are given to ensure the secrecy of UAV control channels by methods and means of passive and active radio masking.

Безпілотні літальні апарати (БПЛА) набули широкої популярності завдяки можливості одержувати видову інформацію з місцевості, на якій важко розмістити спостерігача. З використанням БПЛА виникають загрози незаконного вторгнення в канал зв’язку для отримання конфіденційної інформації, яка передається від БПЛА, та несанкціоноване втручання в командну телеметрію, тобто в керування БПЛА, з метою виведення його з ладу або заволодіння їм [1, 2]. Отже, завдання захисту командно-телеметричної інформації БПЛА від несанкціонованого доступу є актуальним в забезпеченні її конфіденційності. В даній роботі розглянуті шляхи маскування каналів управління БПЛА.

У роботі розглядалася протидія радіотехнічній розвідці (РТР). Засоби РТР виявляють радіовипромінювання наземного пункту управління (НПУ) та БПЛА, пеленгують місце їх знаходження і визначають вид обладнання з точністю аж до кожного конкретного пристрою індивідуально завдяки неповторній сигнатурі передавача. Тому потрібно знати правила безпеки, тобто методи протидії РТР та намагатися максимально їх дотримуватись.

Основним оперативно-тактичним показником скритності РЕЗ від засобів РТР є ймовірність добування необхідних для поразки чи придушення РЕЗ відомостей:

$$P_{\text{РР РЕЗ}} = P_{\text{в РЕЗ}} P_{\text{ан РЕЗ}}, \quad (1)$$

де $P_{\text{в РЕЗ}}$ – ймовірність виявлення джерела радіовипромінювання; $P_{\text{ан РЕЗ}}$– ймовірність отримання необхідних характеристик випромінювання для організації навмисного впливу на РЕЗ.

Однак показник (1) пов'язаний із конкретними умовами застосування РЕЗ. Його визначення, крім цього, потребує статистичних даних про процес виявлення сигналу. Тому у ряді випадків на практиці для порівняльної

характеристики скритності різних РЕЗ вводять такі технічні показники:

- дальність виявлення РЕЗ, або відносну величину зменшення цієї дальності за рахунок застосування заходів підвищення скритності РЕЗ;
- коефіцієнт зниження помітності РЕЗ;
- ширину основної пелюстки діаграми спрямованості (ДС) антени РЕЗ;
- середній рівень бічних пелюстків ДС антени РЕЗ;
- ширину спектра сигналу РЕЗ.

Методи підвищення скритності НПУ пасивними методами зведені до табл.1.

Табл. 1. Методи підвищення скритності пасивними методами

Найменування методу	*Чинники підвищення скритності випромінювання РЕЗ*
Енергетичний	Зменшення потужності сигналу РЕЗ загалом, зменшення спектральної густини потужності сигналу РЕЗ застосуванням складних (широкосмугових) сигналів
Структурний	Зміна структури сигналу
Просторовий	Зменшення потужності сигналу РЕЗ, що випромінюється в напрямку (секторі напрямків) на розвідприймач
Територіальний	Зменшення потужності сигналів РЕЗ, розміщених поблизу місця дислокації розвідприймача або збільшення дальності до розвідприймача
Часовий	Скорочення часу роботи РЕЗ на випромінювання
Частотний	Зміна робочої частоти РЕЗ
Поляризаційний	Зміна поляризації сигналу
Комбіновані методи	

На підставі вище сказаного можна дати низку рекомендацій екіпажу БПЛА.

1. Чим менше екіпаж використовує джерела радіовипромінювання, то складніше противнику запеленгувати місце, звідки він працює. Тобто не варто без нагальної необхідності вести радіопереговори, не варто без необхідності тримати увімкненим пульт управління. Якщо є необхідність увімкнення цих радіопристроїв для налаштування роботи комплексу БПЛА, то розміщувати їх треба так, щоб вони не випромінювали у бік супротивника, а за перепонами, що надійно екранують радіосигнал.

2. Група джерел сигналу мобільного зв'язку в невластивому місці, де зазвичай нікого немає, викликає підозру.

3. Спрямовану антену не потрібно орієнтувати в різні напрямки без потреби, а тільки супроводжувати сам БПЛА.

4. Не варто постійно літати з одного і того ж майданчика. Треба використовувати кілька різних майданчиків для польотів в той самий сектор і використовувати їх несистематично.

5. З погляду безпеки не варто задовго до початку роботи попереджати інші підрозділи біля площадок про намір використовувати БПЛА в цьому районі. Достатньо попередити їх про це безпосередньо перед самим виходом на майданчик, для мінімізації наслідків від витоку інформації про місце роботи, можливо навіть ненавмисного витоку.

6. Під час виконання вильоту на коригування рекомендується дотримуватись додаткових заходів радіобезпеки. Є сенс летіти до цілі, не використовуючи відеоканал, включати його безпосередньо над ціллю, на по-

чатку коригування. Це забезпечить додаткову скритність.

7. Використовуючи природні укриття та рельєф, можна відвести БПЛА за радіогоризонт системи РТР супротивника. Тому будь-яке перевищення майданчика установки станції управління дає більший радіогоризонт, тобто трохи більші можливості відходу БПЛА вниз при спробі сховатися від радіорозвідки за рельєф (рис.1).

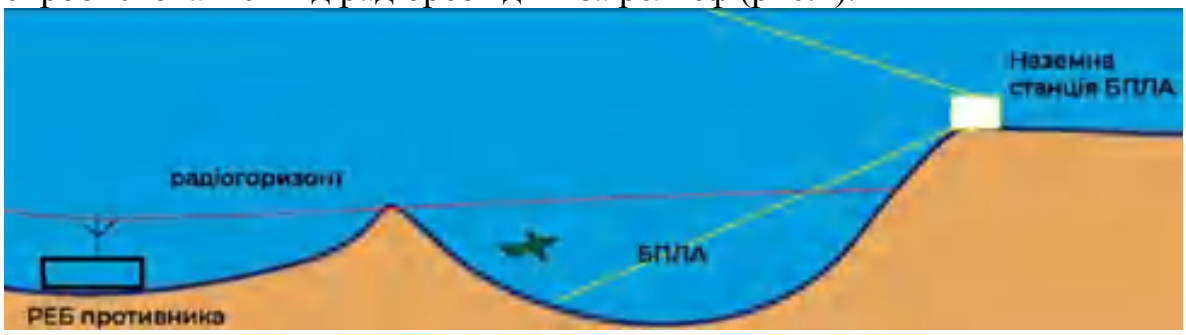

Рис.1. Використання природного укриття та рельєфу місцевості для забезпечення скритності каналів керування БПЛА

8. Для невеликих коптерів, які мають невеликий радіус дії, варто виконувати набір висоти на тлі якихось високих будов, ліній електропередачі, териконів. Екіпажу бажано підняти коптер на невелику висоту, відігнати убік, а потім виходити на робочу висоту.

У випадках, коли пасивними методами важко забезпечити скритність функціонування НПУ, протистояти розвідці можна шляхом технічної дезінформації (створення хибних сигналів). Методи технічної дезінформації або методи активного радіомаскування спрямовані на те, щоб разом зі сигналом від НПУ на вході приймача розвідки були присутні помилкові сигнали, що заважають розпізнаванню та виміру дійсних параметрів сигналу НПУ. В результаті передавач завад створює завади на частотах хибних сигналів або завади, оптимізовані під параметри хибних сигналів. Активне радіомаскування підвищує радіобезпеку і утруднює визначення місця розташування працюючої наземної станції (НПУ) БПЛА. Завдяки використанню засобів активного радіомаскування можна суттєво ускладнити ви-значення супротивником місця, звідки дійсно працює екіпаж БПЛА. В якості засобу активного радіомаскування,наприклад, можна використовувати звичайний пульт від несправного або втраченого БПЛА. Рекомендується встановлювати такий засіб на місці, звідки вона працюватиме досить ефективно (високе самотнє дерево, дах будинку тощо).

Список використаних джерел: 1. Michel A. H. Counter-drone systems // Center for the Study of the Drone at Bard College. 2018. – 23 с. 2. Вишневський С.Д., Бейліс В.Й., Климченко Л.В. Потенційні можливості РЛС РТВ з виявлення оперативно-тактичних та тактичних безпілотних літальних апаратів // Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2. С. 92–98.