УДК 004.056
DOI: 10.31673/2409-7292.2019.044044

А.В. Науменко, Г.В. Шуклін, О.В. Барабаш

ПРОБЛЕМА ІНФОРМАЦІЙНОГО ЗАХИСТУ КОМАНДНОЇ ТЕЛЕМЕТРІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

В даній роботі розглянуті основні способи, спрямовані на несанкціонований доступ до каналу зв'язку передачі даних безпілотних летальних апаратів. Розглянуті реальні події, пов'язані з успішною реалізацією несанкціонованого отримання інформації з безпілотних літальних апаратів і наслідки, які при цьому були зафіксовані. Виявлено протиріччя в технічних системах захисту інформації командної телеметрії. Розглянуті шляхи маскування безпілотних летальних апаратів. Сформульовані основні завдання захисту конфіденційної інформації командної телеметрії безпілотних летальних апаратів.

Ключові слова: малогабаритний безпілотний авіаційний комплекс, системи зв'язку, канал передавання даних, криптографічний захист, кореляційні атаки, направлене шифрування.

Вступ і постановка завдання

За останні роки активно здійснюється розвиток авіабудування в області безпілотних літальних апаратів (БПЛА) структури Drone. Це зумовлено, в першу чергу, низькою вартістю технології створення різноманітних БПЛА, та практичним застосуванням їх як в цивільному житті так і в військовій справі. На теперішній час БПЛА застосовуються в огляді та поливі пестицидами полів в сільському господарстві, огляду на справність вітрових турбін у відновлювальній енергетиці, моніторингу лісових пожеж та надзвичайних ситуацій. Окремою областю застосування БПЛА є військова справа: по-перше - це розвідка місцевості, що дає можливість здійснювати точність виявлення цілей та корегування вогню; по-друге - це можливість оперативного реагування на основі відеоінформації, яка надходить від БПЛА. Отже, наявність в військових підрозділах необхідної кількості одиниць спеціально розроблених для відповідних цілей БПЛА, дає можливість отримувати та аналізувати тактичну та стратегічну інформацію для розробки і впровадженню відповідних військових заходів для підвищення боєздатності відповідних підрозділів.

Однак, з використанням безпілотних комплексів 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.

Вперше несанкціоноване втручання противника в командну телеметрію та захоплення літального апарату було зафіксовано 4 грудня 2011 року. Іранські джерела ЗМІ повідомили з посиланням на військових Ірану, що на сході країни засобами радіоелектронної боротьби (РЕБ), було здійснено примусову посадку БПЛА « RQ 170 Sentinel». Згодом Іран оприлюднив фото та відеодокази захопленого БПЛА [6-7]. Цей випадок стався завдяки можливості втручання в незахищений канал БПЛА. Відомо багато інших випадків перехоплення цивільних БПЛА таких, як DJI Phantom та Parrot AR QuadCopter 2.0 [8-10].

Отже, завдання захисту командно-телеметричної інформації БПЛА від несанкціонованого доступу є актуальним в забезпеченні її конфіденційності.

Метою статті є виявлення протиріччя між можливостями перехоплення відеосигналів, які надходять від БПЛА і можливістю інформаційного захисту командної телеметрії.

Аналіз останніх досліджень і публікацій показав, що існують публікації, присвячені задачам побудови каналів керування та телеметрії БПЛА [1,4-5]. В них показано, що завдяки вимогам скритності і завадозахищеності передачі даних, надійними є технічні засоби цифрової передачі даних .

Однак, проблема інформаційної безпеки для забезпечення захисту каналів передавання командних та телеметричних даних між БПЛА та оператором постійно існує, так як зацікавлена сторона в перехваті інформації, може успішно сканувати дані, що має реальні підтвердження на практиці. Ці завдання розв'язуються завдяки методам шифрування каналів передачі даних, таких як метод асиметричного шифрування [3], метод генерації

псевдовипадкової послідовності з відкритим текстом [2]. Однак, проблема в перехоплені відеосигналу і шифруванні командної телеметрії залишається не розв'язаною.

Виклад основного матеріалу. Час показав, що БПЛА є досить ефективним засобом в боротьбі з тероризмом та розвідування місцевості, але існує досить велика загроза в заглушенні або подолані сигналу GPS, а також в підміні координат GPS засобами радіоелектронної боротьби (РЕБ), втручання в телеметрію БПЛА, та перехоплення відосигналу в реальному часі. Проблемою залишається саме вразливість потоку відеосигналів (телеметрія відеосигналу в реальному часі) так як можливо його дуже легко перехопити за допомогою простого ноутбуку супутникової антени та відеограбера, на відміну від командної телеметрії. Це зумовлено тим, що відеосигнал передається в незахищеному вигляді на відміну командної телеметрії, та досить легко піддається зламу та перехопленню потоку відеосигналів. Такі технологічні гіганти, як DARPA та Lockheed Martin зараз намагаються вирішити цю проблему, але поки, що лише на рівні імітаційних моделей. Суть проблеми в тому, що командна телеметрія підлягає шифруванню досить надійно завдяки малим об'ємам даних, на відміну від телеметрії в якій є візуальні дані потоку відеосигналів в реальному часі. Це зумовлено тим, що така інформація має великий об'єм, і її шифрування призводить до затримки сигналу, яка може призвести до невірної оцінки інформації та помилкового розуміння подій на полі бою. Ці негативні явища породжують недостовірність отриманої інформації, що призводить до тактичних помилок.

З іншого боку, перехоплення відеосигналу не є критичним. Це зумовлено тим, що при перехопленні відеоконтенту, зацікавлена сторона, з боку якої здійснюється злом, не має доступу до командної телеметрії, а це означає, що відсутня можливість перехоплювати керування БПЛА. При цьому лише є можливість спостерігання разом з оператором БПЛА, але відсутня можливість впливати на сам процес керування та прийняття рішень.

Управління БПЛА здійснюється дистанційно. Оператори, які здійснюють керування ними, можуть знаходитись за тисячі кілометрів і при цьому знаходитись в наземних пунктах управління. Керування здійснюється через супутниковий канал передачі даних. Однак, на теперішній час існують шляхи несанкціонованого втручання в керування БПЛА.

На рисунку 1 представлено основні шляхи несанкціонованого доступу до інформації БПЛА.

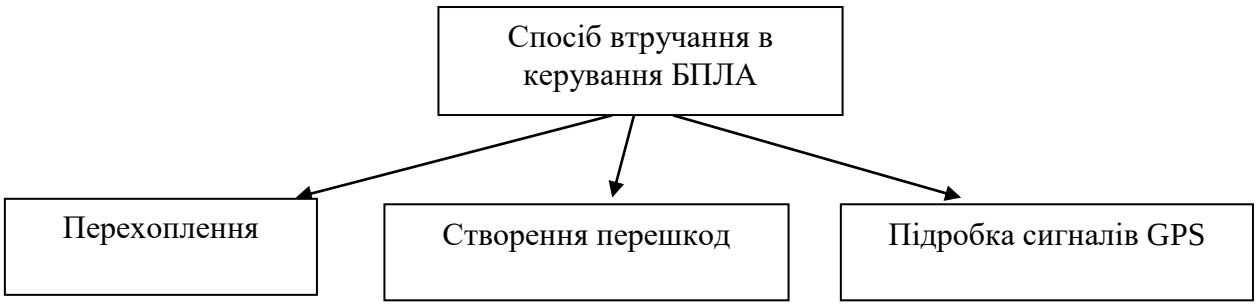

Рис. 1. Шляхи несанкціонованого доступу до інформації БПЛА

Перехоплення – це складний шлях, яки полягає в використанні супутникової тарілки, ТБ-тюнера та програми skygrabber для перехоплення частот БПЛА. Можуть бути перехоплені як дані, які відправляються від супутника на БПЛА, так і ті, які передаються від БПЛА на супутник.

Створення перешкод – мовлення на частотах, які використовує БПЛА, може бути обірване з оператором, який керує БПЛА.

Підробка сигналів GPS – портативні GPS передавачі можуть відправляти хибні GPS сигнали і при цьому порушувати систему навігації БПЛА. Це можна використовувати для руху БПЛА по траєкторії, яка призведе його до руйнування або перехоплення його для здійснення посадки на злітно – посадкової смуги противника.

Кожен з вказаних способів мав місце в реальних подіях і при цьому були негативні наслідки.

В таблиці 1 представлені інциденти і шляхи несанкціонованого втручання, а також наслідки, які при цьому мали місце.

Таблиця 1.

Інциденти [14-19]

Зона розвідки бпла	**Тип бпла**	**Спосіб несанкціонованого доступу**	**Наслідки несанкціонованого втручання**
Луганщина	БПЛА RQ 11B	РЕБ (дублювання сигналу командної станції оператора БПЛА,та підміна пакетів командної телеметрії з метою його посадки та вивчення зразка).	БПЛА був посаджений на непідконтрольній Україні території, НЗФ ЛНР його забрали та передали Російській Федерації.
Іран	Ударний БПЛА	Перехоплення відеосигналу з БПЛА його відстеження.	Супротивник міг в реальному часі спостерігати за американським БПЛА та отримувати розвід інформацію від нього.
Іран	Ударний БПЛА	Перехоплення відеосигналу та командної телеметрії БПЛА.	Знищення дрону шляхом жорсткої посадки, з метою його критичного пошкодження
Донеччина	Малий розвідувальний БПЛА	Заглушення GPS, дезорієнтація БПЛА, втрата оператором командної телеметрії.	ЗСУ отримали не пошкоджений зразок ворожої техніки(БПЛА) доказ присутності на Донеччині російських БПЛА, а також резонанс та доказ присутності Російської Федерації.
Приазов'я	Малий розвідувальний БПЛА	Заглушення GPS БПЛА, втрата командної телеметрії оператором.	ЗСУ отримало не пошкоджений зразок ворожої техніки(БПЛА) доказ присутності на Донеччині російських БПЛА, а також резонанс та доказ присутності. Російської Федерації.
Ірак	Ударний БПЛА	Апаратно програмні методи, використання грабера з спеціальним програмним забезпеченням.	Іракські повстанці отримали доступ до відеосигналу в реальному часі та паралельно із США отримували розвід інформацію.
Сирія,Ірак	Середній розвідувальний БПЛА	Апаратно програмні методи, використання грабера з спеціальним програмним забезпеченням.	Палестинські бойовики отримали доступ до відеосигналу в реальному часі та паралельно із США отримували розвід інформацію.
США	Малий аграрний БПЛА	РЕБ, дублювання сигналу командної станції(оператора БПЛА) та підміна пакетів командної телеметрії з метою експерименту можливості вивчення.	Було виявлено на конкретному прикладі небезпеку незахищених каналів БПЛА та перехоплення керування з можливістю керувати БПЛА
Великобританія	Малий цивільний БПЛА	Пошук дрона та оператора спеціальними системами, визначення координат, заглушення командної телеметрії з метою безпечної посадки дрону.	В крнкретно цьоми випадку скоріш за все дрон був апаратно та програмно модифікований, і спецзасоби не могли його засікти та знешкодити

Виходячи з аналізу інцидентів, які мали місце, можна зробити висновок, що завдання захисту каналу командної телеметрії на теперішній час є актуальною і вимагає ретельного аналізу для створення надійних заходів його захисту.

З іншого боку, БПЛА мають потужну камеру, яка спроможна розпізнавати людей та інші габаритні засоби з висоти декількох кілометрів. Великий тип БПЛА мають інфрачервоні камери нічного бачення, або ІК – системи переднього огляду. Вони спроможні з достатньо великої відстані як в ночі так і з ранку сканувати тепло людини. Отже, виникає необхідність не тільки захищати інформацію БПЛА, але і створювати заходи щодо укриття від них. Це пов'язано з тим, що протилежна сторона також використовує їх для отримання інформації, яку інша сторона захищає.

На рис. 2 представлено основні способи укриття від БПЛА.

Рис. 2. Способи укриття від БПЛА

Світлове маскування – використання тіней від будівель або дерев, використання маскуючих засобів в густому лісі.

Нічне маскування – використання внутрішніх стін будівель або дерев, та не використання засобів світла.

Теплове маскування – використання матеріалу, який не пропускає інфрачервоне світло. При температурі повітря 36 -40 градусів цельсія, інфрачервона камера не розпізнає людину.

Врахування погодних умов – БПЛА не можуть працювати при сильному вітрі, димі або грозі.

Не використання бездротового зв'язку – використання мобільного зв'язку або GPS пристроїв може сканувати безпілотним літальним апаратом місце розташування джерела.

Використання скла – шматки скла або інших дзеркальних матеріалів на дахах домів і автомобілей створюють перешкоди для камер БПЛА.

Використання хибних цілей – для виявлення повітряної розвідки варто використовувати манекени, яки мають середній зріст людини.

Висновок. Не дорогий БПЛА може паралізувати аеропорт та нанести величезні збитки. З іншого боку втрата військового БПЛА шляхом його злому або знищення коштує теж чи малих коштів. Отже, при використанні БПЛА в розвідувальних цілях, потрібна надійна система шифрування, як потоку відеосигналів, так і командної телеметрії, адже збитки від втрати БПЛА такого класу є досить відчутні. З іншого боку, при захисті від присутності БПЛА теж треба вкладати гроші з одного боку на маскування від нього, а з іншого боку, для його перехоплення. Тому, завдання захисту інформації БПЛА та своєчасного виконання їм команд від оператора залишається на теперішній час до кінця не розв'язаною.

Перелік посилань

1. Рассомахін С.Г. Обгрунтування принципів побудови каналу управління і телеметрії та інформаційного каналу малогабаритних безпілотних авіаційних комплексів / С.Г. Рассомахін, А.Г. Снісаренко, В.В. Романенко, В.Б. Бзот // Збірник наукових праць Харківського університету Повітряних Сил. - № 4 (22), 2009. – с. 53-59.
2. Навроцький Д.О. Криптографічна система захисту радіоканалів БПЛА від несанкціонованого втручання /Д.О. Навроцький // Ukrainian Scientific Journal of Information Security vol.20, issue 3, 2014.- p. 248-252.
3. Петренко О.С. Пропозиції щодо застосування асиметричного шифрування для забезпечення криптографічного захисту в каналах передавання командних та телеметричних даних між БПЛА та оператором / О.С. Петренко, О.Є. Петренко // Наука і техніка Повітряних Сил Збройних Сил України , №2(19), 2015, с.97-100.
4. Васюта К.С. Аналіз можливості застосування хаотичних процесів для організації командно – телеметричної радіомережі управління безпілотними літальними апаратами / К.С. Васюта, С.В. Озеров, А.В. Литвин, А.В. Северилов // Збірник наукових праць Харківського університету Повітряних Сил. - № 3 (52), 2017. – с. 35-38.
5. Vladimir V. Mitrashchuk. Hardware – Software Complex Protection of Telemetry and Telecontrol of Specialized Unmanned Aeridl Vechicles / Vladimir V. Mitrashchuk, Marina P. Baranova // Journal of Siberian Federal University. Engineering & Technologies,№12(5), 2019.- p. 585-598.
6. Електронний ресурс: https://www.bbc.com/russian/international/2011/12/111208_us_drone_iran
7. Електронний ресурс: https://habr.com/ru/post/135150/
8. https://pikabu.ru/story/kak_vzlomat_politseyskikh_dronov_imeya_apparaturu_za_40_4113871
9. Електронний ресурс: https://www.popmech.ru/technologies/238507-kak-vzlomat-bespilotnik-s-pomoshchyu-deshyevogo-kompyutera/
10. Електронний ресурс: https://www.popmech.ru/technologies/238507-kak-vzlomat-bespilotnik-s-pomoshchyu-deshyevogo-kompyutera/
11. Електронний ресурс: https://www.bbc.com/russian/news-46633933
12. Електронний ресурс: https://www.bbc.com/russian/news-46643202
13. Електронний ресурс: https://avianews.info/v-gatvike-armiya-ispolzovala-izrailskuyu-sistemu-drone-dome-dlya-podavleniya-bpla/
14. Електронний ресурс: https://topwar.ru/106252-uyazvimost-kanalov-upravleniya-shtatovskimi-takticheskimi-bpla-tehnologicheskie-momenty.html
15. Електронний ресурс: https://www.rbc.ru/society/22/02/2019/5c702e6d9a794732c8fadd49
16. Електронний ресурс: https://zautra.by/news/news-30482
17. Електронний ресурс: https://www.pravda.com.ua/news/2019/01/25/7204819/
18. Електронний ресурс: https://lenta.ru/news/2009/12/17/hack/
19. Електронний ресурс: https://www.bbc.com/russian/science/2012/06/120629_drone_spoof_hack

Надійшла: 09.10.2019 Рецензент: д.т.н., доцент Гайдур Г.І.