Секція 1

КІБЕРАТАКИ НА БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ: КЛАСИФІКАЦІЯ ТА УРАЗЛИВОСТІ

Логачов М. Г.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Фесенко Г. В.

Актуальність. Використання БПЛА для розмінування стає важливою стратегією для зменшення ризиків, пов'язаних із мінно-вибуховими об'єктами в Україні. БПЛА дозволяють проводити швидку та безпечну розвідку та розмінування, що дозволяє знизити ризики для життя людей, оптимізувати час і ресурси, а також забезпечити більш точні та ефективні результати при розмінуванні [1].

Метою роботи є дослідження та аналіз методів збору та передачі даних з безпілотних літальних апаратів (БПЛА) з метою виявлення потенційних уразливих точок у процесі передачі цих даних.

Основні положення. БПЛА, також відомі як дрони, використовуються для різноманітних застосувань і поділяються на дві основні категорії: цивільні та військові.

Під час управління дронами оператор постійно обмінюється різноманітними пакетами даних через бездротовий зв'язок. Ці дані включають відео, аудіо, інформацію від датчиків та оброблені дані. Керуючі пакети містять команди, інструкції, інформацію про стан системи, позицію та інші дані для ефективного управління дронами та їхніми мережами [2]. Як високооптимізована кібер-фізична система, дрони піддаються широкому спектру можливих кібератак.

Кібератака – це агресивна дія з злочинними намірами, що впливає на функції обчислення та комунікації. Хоча атаки можуть призвести до деяких поступових збоїв у вимогах кібербезпеки, такі збої можуть не бути кінцевою метою зловмисника. Таким чином, кібератака може бути складним багатоетапним процесом. Наприклад, кібератака може складатися з трьох етапів. На першому етапі до БПЛА надсилають фальшиві навігаційні повідомлення, що призводить до неправильного розрахунку його координат. На другому етапі супротивник глушить канал управління, щоб БПЛА не отримував команди від наземної станції управління. І, нарешті, на третьому етапі за допомогою підроблених навігаційних повідомлень і без команди управління БПЛА може бути дезорієнтованим і зрештою впасти на землю [3].

Розглядаючи кібератаку як атомарну на кожному етапі, та классифікуючи ці атаки на основі їх точок входу, можна виділити три основні типи входу в атаку, а саме: радіоканал, повідомлення та бортова система, де на кожному з кількох етапів атомарна атака спричиняє

додатковий збій у системі кібербезпеки та приводить БПЛА до більш скомпрометованого стану, що ближче до кінцевої мети зловмисника [4].

На основі цих точок входу, можна розподілити кібератаки на БПЛА на такі шість категорій: блокування каналу (Channel Jamming), перехоплення повідомлень (Message Interception), видалення повідомлень (Message Deletion), впровадження повідомлень (Message Injection), фальсифікація повідомлень (Message Spoofing), атака на бортову систему (On-Board System Attack)

Висновки. У контексті кібербезпеки нам потрібно забезпечити конфіденційність, цілісність та автентичність інформації, якою керуються БПЛА. Крім того, ми повинні забезпечити доступність послуг, які використовуються або пропонуються БПЛА. Ця доступність послуг, в поєднанні з конфіденційністю, цілісністю та автентичністю інформації, узагальнюється вимогами кібербезпеки БПЛА.

Список літератури

1. Федоренко Г. Л., Фесенко Г. В., Харченко В. С. «Аналіз методів і розроблення концепції гарантованого виявлення та розпізнавання вибухонебезпечних предметів.» Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 4 (22). С. 20–31. DOI: https://doi.org/10.30837/ITSSI.2022.22.020
2. Erdelj, M.; Saif, O.; Natalizio, E.; Fantoni, I. «UAVs that fly forever: Uninterrupted structural inspection through automatic UAV replacement.» Ad Hoc Netw. 2019, 94, 101612.
3. Kong, P.-Y. «A Survey of Cyberattack Countermeasures for UAV». November 2021.
4. Mohsen Riahi Manesh and Naima Kaabouch, «Cyber attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions,» Computers & Security, vol. 85, pp. 386-401, August 2019.

Відомості про авторів

Логачов Михайло Геннадійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.h.lohachov@student.csn.khai.edu

Фесенко Герман Вікторович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, h.fesenko@csn.khai.edu