УДК 629.3.025.2

Шевченко А.А. студент (*Національний авіаційний університет*)

Романовський Е.Р. студент (*Національний авіаційний університет*)

Система захисту БПЛА від перехвату управління

Перехоплення управління безпілотних літальних апаратів (БПЛА) шляхом відправлення помилкових даних системи GPS - один із найпоширеніших і найскладніших одночасно видів електронної атак на БПЛА. Підсумком такої атаки, проведеної з використанням сучасного обладнання, може бути як мінімум відхилення від курсу і виліт за потрібний квадрат, а в гіршому випадку - відмова всіх необхідних датчиків. Безпілотні літальні апарати знаходять широке застосування в різних областях, у будь-якій з яких перехоплення є небажаним або неприпустимим. Але найчастіше це пов'язано зі стандартними протоколами обміну даними між оператором та БПЛА, а також БПЛА та супутником GPS.

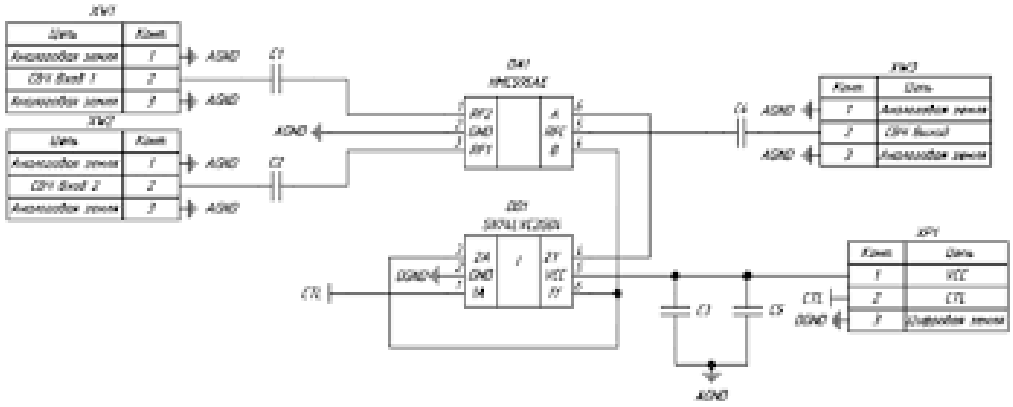

Рис 1. Комплекс перехвата управления БПЛА

Існуючі на сьогоднішній день методи протидії подібним атакам не можна вважати високоефективними. Як методи боротьби з GPS-Spoofing розглядають системи криптографії, а також застосування засобів перешкодостійкості кодування з використанням керованих перестановок, що дозволяють на короткому відрізку часу здійснювати маскування істинної структури сигналу [1]. Пропонується новий альтернативний підхід до проблеми захисту БПЛА від GPS Spoofing і подібного роду активних атак перехоплення управлінням апаратом, який полягає в реалізації так званої Системи Альтернативного Орієнтування (САО). Принцип роботи даної системи базується на математичному обчисленні положення БПЛА щодо останніх даних, отриманих від GPS-супутника до початку розриву з'єднання при спробі реалізації атаки типу GPS Spoofing і зміні його курсу за записаним раніше маршрутом. Система завдяки наявності специфічних датчиків визначає значення швидкості, напряму, висоти та інших критичних параметрів управління БПЛА і виходячи з цього виробляє математичний розрахунок пройденого шляху, записуючи це внутрішню карту місцевості. Представлений метод може забезпечити захист БПЛА від атаки типу GPS Spoofing, безпечно перенаправити апарат у найближчу задану раніше точку пройденого маршруту до моменту відновлення з'єднання з оператором. На відміну від відомих методів, запропонована система трохи підвищує вартість БПЛА, його масу і не ускладнює його конструкцію.

Список літератури

1. Spoofed' GPS signals can be countered, researchers show [Електронний ресурс]. - Режим доступу: https://news.cornell.edu/stories/2012/07/researchers-counter-gps-spoof- attack. - Дата доступа: 20.11.2023.