СИСТЕМА ЗАЩИТЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ОТ АКТИВНЫХ АТАК ПЕРЕХВАТА УПРАВЛЕНИЯ ПОСРЕДСТВОМ GPS-НАВИГАЦИИ

А.В. Казак

Перехват управления беспилотных летательных аппаратов (БПЛА) путем отправки ложных данных системы GPS – один из самых распространенных и сложных одновременно видов электронной атак на БПЛА. Итогом такой атаки, проведенной с использованием современного оборудования, может быть, как минимум, отклонение от курса и вылет за нужный квадрат, а в худшем случае – отказ всех необходимых датчиков. Беспилотные летательные аппараты находят широкое применение в различных областях, в любой из которых, перехват является нежелательным или недопустимым. Зачастую, возможность реализации подобного рода атак определяется уязвимостями каналов управления. Но чаще всего это связано со стандартными протоколами обмена данными между оператором и БПЛА, а также БПЛА и спутником GPS.

Существующие на сегодняшний день методы противодействия подобного рода атакам нельзя считать высокоэффективными. В качестве методов борьбы с «GPS-Spoofing» рассматривают системы криптографии, а также применение средств помехоустойчивости кодирования с использованием управляемых перестановок,

позволяющих на коротком отрезке времени осуществлять маскировку истинной структуры сигнала [1]. Также существуют методы с использованием коротких сегментов дынных GPS-приемника и методы, которые позволяют изменять положение антенны с определенной частотой [2].

Предлагается новый альтернативный подход к проблеме защиты БПЛА от «GPS Spoofing» и подобного рода активных атак перехвата управлением аппаратом, который заключается в реализации, так называемой, Системы Альтернативного Ориентирования (САО). Принцип работы данной системы базируется на математическом вычислении положения БПЛА относительного последних данных, полученных от GPS-спутника до начала разрыва соединения при попытке реализации атаки типа «GPS Spoofing» и изменении его курса по записанному ранее маршруту. Система благодаря наличию специфических датчиков определяет значения скорости, направления, высоты и других критичных параметров управления БПЛА и на основании этого производит математический расчет пройденного пути, записывая это на внутреннюю карту местности. Представленный метод может обеспечить защиту БПЛА от атаки типа «GPS Spoofing», безопасно перенаправить аппарат в ближайшую заданную ранее точку пройденного маршрута до момента восстановления соединения с оператором. В отличие от известных методов, предложенная система незначительно повышает стоимость БПЛА, его массу и не усложняет его конструкцию.

Литература

1. Навроцкий Д.А. Система защиты радиоканалов БПЛА от несанкционированного вмешательства // Национальная ассоциация ученых. Технические науки. 2015. № III (8). С. 95–99.

2. Spoofed' GPS signals can be countered, researchers show [Электронный ресурс]. – Режим доступа: https://news.cornell.edu/stories/2012/07/researchers-counter-gps-spoof-attack. – Дата доступа: 2.05.2022.