АНАЛИЗ АКТИВНЫХ АТАК НА БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ

А.В. Казак, Г.А. Пухир

Современный этап развития беспилотных летательных аппаратов (БПЛА), которые применяются в различных сферах не только в гражданской области, но и для военного назначения, порождает проблемы безопасности БПЛА, как связанные с возможностью перехвата самих устройств злоумышленниками, так и с обеспечением безопасного воздушного пространства в условиях применения БПЛА. Беспилотные летательные аппараты – это летательные аппараты без экипажа, которые управляются дистанционно (например, с земли или с другого воздушного судна) или при помощи другого автономного программного обеспечения, установленного на борту [1]. Принцип управления БПЛА строится на связи между оператором и самим БПЛА.

Существующие методы противодействия БПЛА делятся на два типа: контактные и бесконтактные. Контактными методами являются методы, которые влияют кинетически на сам БПЛА. Примерами контактного противодействия являются противодроны, сети, кинетическое оружие и обученные животные. В связи с разнообразием задач, выполняемых БПЛА в различных климатических условиях и местах базирования, во время боевого дежурства и на траектории полета по условиям эксплуатации БПЛА могут подвергаться прямому электромагнитному воздействию [2]. Кроме этого необходимо учесть, что сегодня в мире существует реальная угроза воздействия на БПЛА различных преднамеренных деструктивных электромагнитных

воздействий, например, посредством сверхкороткоимпульсного электромагнитного излучения, что можно отнести к бесконтактным методам противодействия БПЛА.

Также существует возможность перехвата управления беспилотным летательным аппаратом третьими лицами. Одним из существующих методов перехвата является GPS Spoofing [3]. Данный принцип строиться на замещении сигнала GPS, который передается от спутника до БПЛА, за счет более мощного сигнала от ретранслятора третьего лица. Реализация этого способа перехвата довольно проста, что делает данную угрозу весьма вероятной.

Литература

1. Павлов А.М. Принципы организации бортовых вычислительных систем перспективных летательных аппаратов // Мир компьютерной автоматизации. 2001. № 4.

2. Комягин С.И., Соколов А.Б. Требование по стойкости радиоэлектронной аппаратуры летательных аппаратов в условиях воздействия электростатических разрядов // Технологии электромагнитной совместимости. 2008. № 2. С. 3–8.

3. Можно ли защититься от атак на GPS? [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/gps-spoofing-protection/22674/. – Дата доступа: 2.05.2022.