И.А. Бледных, С.А. Попов, Филиппов Д.С.
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
г. Воронеж, ул. Старых Большевиков 54а
e-mail: popsa230@rambler.ru

Возможности информационно-технологического воздействия на БПЛА

В настоящее время строительство беспилотных летательных аппаратов (БПЛА) переживает большой подъем. Создается широкая номенклатура машин – от стратегических аппаратов до мини-БПЛА. Неуклонно увеличивается численность их парка, расширяется круг решаемых ими задач. В результате, многие компании, имеющие разработки в области БПЛА, склонны обращать внимание на перспективы применения БПЛА в гражданской и коммерческой сферах. В свою очередь, заинтересованные государственные ведомства и спецслужбы, функции которых связаны с охраной, контролем и мониторингом объектов, ликвидацией чрезвычайных ситуаций; предприятия топливно-энергетического комплекса, а также фирмы, бизнес которых связан с получением пространственных данных, также проявляют встречный интерес к БПЛА. Так, с марта 2014 по февраль 2015 года было поставлено в вооруженные силы различных стран более 20000 экземпляров БПЛА [1].

Ведущие мировые державы осуществляют долгосрочные программы создания БПЛА, развивают промышленные технологии получения ключевых компонентов, таких как: платформа, многоцелевые датчики, системы связи и обработки их информации, необходимые для выполнения поставленных задач. Многие функции пилота воздушного судна в БПЛА заменяются аппаратными и программными модулями, входящими в состав бортового радиоэлектронного оборудования (БРЭО), позволяющими решать следующие задачи: подготовка к вылету, навигация, управление БПЛА на всех этапах полета, обеспечение радиосвязи, обеспечение групповых действий БПЛА и взаимодействия, при необходимости, с пилотируемыми воздушными судами, управление целевой нагрузкой, обеспечение применения по предназначению, контроль и диагностика БРЭО.

Развитие функциональной совместимости, надежности, эффективности и живучести компонентов БПЛА является необходимым условием для радиоэлектронных систем, размещаемых на борту в ограниченном пространстве. Перспективные комплексы БРЭО БПЛА, как и комплексы БРЭО перспективных пилотируемых воздушных судов, должны состоять из следующих взаимосвязанных систем: информационно-управляющая система, навигационное оборудование, бортовые средства радиосвязи, системы целевой нагрузки, система радиолокационного опознавания [1, 2]. Современные комплексы БРЭО БПЛА, объединяя огромное количество радиоэлектронных компонентов, позволяют значительно повысить уровень автономности и гарантировать выполнение задач, снижая вероятность ошибок, обусловленных человеком в системе управления БПЛА «земля-воздух» [3]. Перспективные комплексы БРЭО должны сводить ущерб человеческих ошибок к нулю.

Параллельно развитию БПЛА развиваются методы и средства целенаправленного нарушения их нормального функционирования. Современные технические средства позволяют обнаруживать и пеленговать каналы управления и сброса информации БПЛА, вмешиваться в работу БРЭО и наземных комплексов управления. К основным факторам риска в отношении БРЭО БПЛА следует отнести: 1) разрушающие радиоэлектронные воздействия на информационно-управляющую систему; 2) несанкционированный доступ к основным узлам на программном уровне и, как следствие, нарушение технологических циклов работы; 3) нарушение (срыв) управления из-за деструктивного воздействия вредоносного программного обеспечения (ПО); 4) человеческий фактор (свободный доступ к элементам БРЭО, ошибки программистов); 5) использование штатных операционных систем и аппаратных средств с имеющимися недекларированными возможностями.

БПЛА управляется дистанционно через спутниковый или иной беспроводной канал передачи команд и данных. Операторы БПЛА могут находиться за тысячи километров в наземных пунктах управления. В связи с этим наиболее часто применяются следующие виды нарушения (срыва) управления БПЛА:

1. Создание помех, внедрение вредоносного ПО. Вещанием на частотах, используемых БПЛА, может быть нарушена связь с его оператором. Заглушив или перехватив канал связи, можно вмешаться в управление БПЛА, в том числе внедрив и вредоносное ПО.

2. Перехват трафика. Заключается в использовании спутниковой антенны, ТВ-тюнера и программы типа skygrabber, чтобы перехватить частоты БПЛА. Могут быть перехвачены как

команды и данные, отправляемые с пункта управления на БПЛА, так и команды и данные, идущие в обратном направлении.

3. Имитация и подмена сигналов GPS. Портативные GPS передатчики могут посылать более мощные ложные сигналы и нарушить систему навигации БПЛА. Используется для направления БПЛА по траектории, на которой он разобьется, для его перехвата и посадки.

Информационно-технологические воздействия на БПЛА могут быть и гораздо сложнее, иметь более широкий спектр применения и различаться по характеру и природе возникновения, использованию различных средств, например, в виде нарушения работы датчиков бортового и наземного оборудования. Неординарный подход к разработке средств информационно-технологических воздействий на БПЛА в настоящее время выражается в тенденции создания специальных дронов-охотников, разрабатываемых в целях перехвата других БПЛА. Особое место в нарушении (срыве) управления БПЛА играет информационно-технологическое воздействие с использованием технологии программно-определяемого радио (software defined radio или SDR), поскольку оно дает возможность получить доступные для широкого круга лиц средства, позволяющие проводить следующие преднамеренные воздействия:

1. Считывание и передача сигнала на любой частоте от 100 МГц до 6 ГГц, благодаря доступности универсальных радиопередатчиков (уязвимость практически всех частотных диапазонов, которые используются для передачи данных: 3G, WiFi, FM, GPS). Использование универсального передатчика для перехвата и расшифровки радиосигналов приведет к компрометации любого незащищенного протокола радиосвязи;

2. Извлечение секретных ключей шифрования аппаратно-программного средства при проведении экономичной электромагнитной атаки с замером побочных электромагнитных излучений в течение нескольких секунд (использование доступного оборудования: потребительского радиоприемника или USB-модуля с SDR).

Все это определяет необходимость разработки мер информационной защиты в отношении информационно-управляющей системы БРЭО БПЛА, которые заключаются в проведении комплекса работ, включающих: анализ и тестирование информационно-управляющих компонентов БРЭО с целью выявления уязвимостей и последующей их классификации по степени возможных угроз; разработку защищенной доверенной инфокоммуникационной инфраструктуры для специализированных систем управления; разработку методик поиска уязвимостей в программном обеспечении информационно управляющих систем и устройств БРЭО; создание системы сертификации и типовых стендов специального функционального и нагрузочного тестирования программного обеспечения; совершенствование нормативной базы по обеспечению безопасности информации в информационно-управляющих системах; разработку индивидуальных для каждой модели БПЛА средств, использующих шаблоны блокировки для защиты от атак через шину передачи данных и установки скрытой аппаратной закладки на шину, либо перепрограммирования штатного блока управления.

Данные меры позволят снизить риск реализации информационно-технологического воздействия, повысить уровень безопасности полетов БПЛА и эффективность выполнения возложенных на них задач.

Литература

1. Беспилотные летательные аппараты: справочное пособие / под общ. ред. С.А. Попова. – Воронеж: ИПЦ «Научная книга», 2015. – 619 с.

2. Жуков И. Актуальные вопросы обеспечения кибербезопасности беспилотных летательных аппаратов // Радиоэлектронные технологии. – 2016. – № 1. – С. 56-60.

3. Управление и наведение беспилотных маневренных летательных аппаратов на основе современных информационных технологий / Под ред. М.Н. Красильщикова и Г.Г. Себрякова. — М.: ФИЗМАТЛИТ, 2003. – 280 с.