УДК 004.056.5

Власов Андрей Игоревич, Салуев Евгений Алексеевич, Махмудов Тимур Назимович, Федотов Айсен Андреевич.

Московский Государственный Технический Университет им. Н. Э. Баумана
Кафедра ИУ4 "Проектирование и технология производства электронной аппаратуры"
105005 Россия, Москва, 2–я Бауманская 5, стр.1, тел. 84992636553

ИССЛЕДОВАНИЕ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ.

В настоящей работе проведено исследование методов обеспечения информационной безопасности беспилотных летательных аппаратов, рассмотрены основные методы различных атак на них, способы противодействия несанкционированному проникновению. Основное внимание уделено введению в проблематику, описанию основных принципов и понятий в информационной безопасности беспилотных летательных аппаратов.

Ключевые слова: беспилотные летательные аппараты, беспроводные самоорганизующиеся сети, информационная безопасность, уязвимости безопасности, угрозы информационной безопасности, атака, защита информации.

Vlasov A.I., Saluev E.A., Makhmudov T.N., Fedotov A.A..
Bauman Moscow State Technical University
Department of IU4 "Design and technology of electronic equipment production"
105005 Russia, Moscow, 2nd Baumanskaya 5, p.1, 8 (495) 2636553

A STUDY OF INFORMATION SECURITY TECHNIQUES FOR UNMANNED AERIAL VEHICLES.

In this paper a study of methods of ensuring information security of unmanned aerial vehicles is conducted, the main methods of various attacks on them, and ways to counteract unauthorized intrusion are considered. The main attention is paid to introduction to the problems, description of basic principles and concepts in information security of unmanned aerial vehicles.

Keywords: drones, wireless self-organising networks, information security, security vulnerabilities, information security threats, attack, information security.

Введение

В современном мире беспилотные летательные аппараты (БПЛА) становятся все более популярными и широко используются в различных отраслях, начиная от транспортировки грузов и заканчивая военными операциями. Однако, увеличение числа БПЛА также повышает риски связанные с информационной безопасностью.

Хакеры могут использовать уязвимости БПЛА для доступа к конфиденциальной информации или даже для реверс-инжиниринга самого устройства. В связи с этим, исследование методов обеспечения информационной безопасности БПЛА является важной задачей.

Для обеспечения безопасности БПЛА, необходимо учитывать многие факторы, такие как защита от несанкционированного доступа, защита от вредоносного программного обеспечения и защита от атак на сетевые протоколы. Для этого, важно использовать комплексный подход, который включает в себя как технические, так и организационные меры.

Кроме того, важно учитывать требования к информационной безопасности БПЛА в зависимости от конкретной отрасли. Например, в военных операциях, требования к безопасности будут более жесткими, чем в гражданской авиации или в сельском хозяйстве.

Некоторые из существующих методов обеспечения информационной безопасности БПЛА включают в себя криптографические протоколы, фильтрацию трафика, системы обнаружения вторжений, а также использование физических мер защиты, таких как шифрование данных и аутентификация.

Новые методы, которые могут быть использованы в будущем, включают в себя использование искусственного интеллекта и машинного обучения для обнаружения и предотвращения кибератак, а также использование блокчейн технологий для обеспечения безопасности данных.

В целом, обеспечение безопасности БПЛА является важной задачей, которая требует постоянного исследования и развития новых методов и технологий для обеспечения защиты от кибератак и защиты конфиденциальной информации.

В данной работе будут рассмотрены существующие методы защиты БПЛА от кибератак, а также будут предложены новые подходы к обеспечению информационной безопасности БПЛА.

1. Беспилотные летательные аппараты и способы их применения

Беспилотные летательные аппараты (БПЛА) – это автономные летательные устройства, которые могут выполнять различные задачи без участия пилота (рис. 1). Они используются во многих областях, в том числе:

- военное дело: для разведки, мониторинга, поиска и уничтожения целей,
- гражданская авиация: для мониторинга и аэрофотосъемки, дистанционного зондирования Земли, доставки товаров и медицинской помощи,
- недвижимость: для аэрофотографии и создания трехмерных моделей зданий или территорий. Сельское хозяйство: для мониторинга состояния посевов, управления урожаем и контроля за заболеваниями растений,
- энергетика: для мониторинга линий электропередач и газопроводов, обнаружения утечек и контроля за оборудованием,
- лесное хозяйство: для мониторинга состояния лесных массивов, обнаружения лесных пожаров и контроля за лесными ресурсами,
- геодезия и картография: для создания цифровых карт и трехмерных моделей территорий,
- метеорология: для мониторинга погодных условий и сбора метеоданных.
- спасательные операции: для поиска и спасения людей в затруднительных условиях,
- развлечения: для создания аттракционов и развлекательных мероприятий, таких как гонки дронов или фестивали световых шоу.

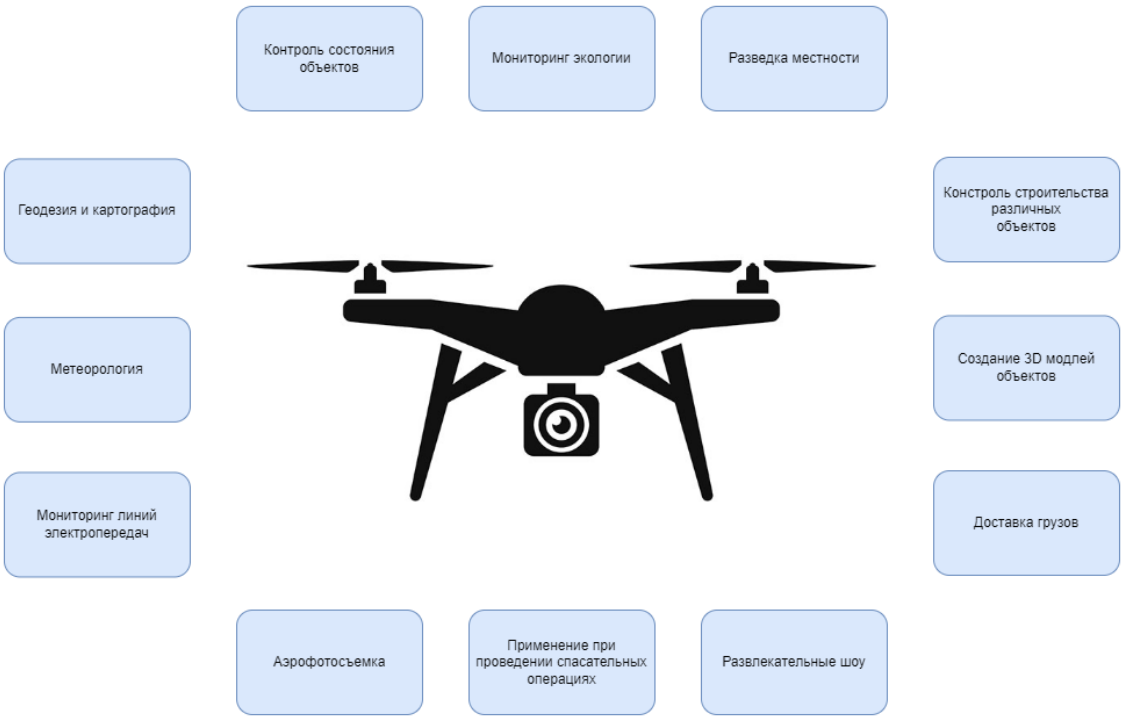

Рисунок 1. Задачи, которые можно выполнять с помощью БПЛА.

Одним из главных преимуществ БПЛА является безопасность. Они могут выполнять задачи, которые могут быть опасны для человека, такие как наблюдение за вулканами или выполнение заданий в зоне военных действий. БПЛА могут использоваться для сбора данных и мониторинга в реальном времени, что позволяет быстро реагировать на изменения в окружающей среде.

В целом, БПЛА имеют огромный потенциал в различных областях и могут быть использованы для повышения эффективности и безопасности в различных сферах деятельности [1].

2. Виды атак на беспилотные летательные аппараты

Ввиду того, что наиболее распространенные дроны изначально разрабатывались/разрабатываются для гражданского сектора и появились на рынке относительно недавно. На многих из них либо отсутствует полностью, либо имеются лишь низкоэффективные протоколы защиты передачи данных, не обеспечивающие достаточный уровень безопасности беспроводных каналов управления и передачи данных. Таким образом, злоумышленник имеет возможность почти беспрепятственно взять БПЛА под полный контроль, либо перехватить управление над отдельными модулями [2].

На сегодняшний день, существуют несколько общепринятых способов атак на беспилотные летательные аппараты. Первый из них, подменить сигнал GPS передаваемый на приемно передающий модуль (ППМ) беспилотника. Получив ложный координаты, БПЛА начнет перестраивать первоначальный маршрут. Данный метод удаленного реверс-инжиниринга открывает перед злоумышленником большое количество возможностей: разбить дрон о землю, направить его в человека, машину или любой другой объект, посадить его на землю, после чего похитить, выкрав все файлы, находящиеся на его карте памяти (видео, фотоматериалы, маршруты передвижения, точки запусков и посадок и т.д.) [3].

Второй способ - наведение на частотный канал передачи данных активных шумовых помех, тем самым “ослепляя” дрон, что приводит к потере контроля оператора над БПЛА или же полного выведению его из строя. Это вид атаки на БПЛА наиболее прост и распространен среди всех известных.

Также злоумышленники могут осуществить реверс-инжиниринг при помощи анализатора трафика, более известный как сниффер. Так как радиоканал управления как правило на гражданских БПЛА не обладает системами шифрования, для стороннего пользователя не составляет труда расшифровать его при помощи сниффера, после чего перехватить управление беспилотным летательным аппаратом.

Атака на БПЛА производится как при помощи специализированных устройств, вроде станций РЭБ, так и при помощи других дронов, “подчиняющие” свою оператору другие дроны в воздухе при помощи вредоносного ПО и др.

Исследователь Сэми Камкар (Samy Kamkar) провел эксперимент под названием Skyjack: он угнал дрон с Raspberry Pi и с его помощью подчинил себе другие беспилотники, таким образом завладев целым роем дронов. Захват одного беспилотника с помощью другого существенно расширяет потенциал угрозы. Точно

так же ботнеты – армии личных устройств, захваченных злоумышленниками, – совершают DDOS-атаки.

Злоумышленники могут перехватывать данные, которые дрон передает на базовую станцию, – например, видеозапись, транслируемую на контроллер системой First Person View (FPV). Часто производители обычных дронов, которые продаются в магазинах, не защищают их шифрованием, а незашифрованные данные – легкая добыча для злоумышленников. Это как раз и доказал эксперимент.

3. Основные методы защиты беспилотных летательных аппаратов от реверс-инжиниринга

Безопасность дронов вызывает опасения у некоторых людей, и это не удивительно. Однако, существует множество способов защитить любой беспилотный летательный аппарат от возможных кибератак.

Вот некоторые из них:

- рекомендуется регулярно обновлять прошивку вашего дрона, чтобы избежать проблем, так поступила компания DJI, добавив исправление после атаки хакеров, но некоторые пользователи не установили его, оставив свои данные уязвимыми для атаки,
- рекомендуется установить надежный пароль для приложения базовой станции, чтобы уменьшить вероятность реверс-инжиниринга и защитить дрон от перехвата сигнала,
- чтобы обезопасить дрон от вредоносного ПО, необходимо защитить устройство которым он управляется, используя антивирусное ПО и не загружая программы и приложения сомнительного происхождения [4],
- рекомендуется использовать виртуальную частную сеть (VPN), которая создает защищенное соединение между вашим устройством и сервером, что не позволит злоумышленникам перехватить ваши данные,
- рекомендуется частая проверка подключенных к базовой станции устройств, для того, чтобы хакеры не смогли перехватить сигнал для управления дроном через другие устройства,
- перед использованием дрона необходимо убедиться, что функция "Возврат на базу" (RTH) включена и указано местоположение базы, чтобы дрон мог вернуться к вам в случае потери сигнала, глушения или низкого заряда батареи, а также обеспечить защиту от перехвата управления, но следует помнить, что функция RTH работает только при наличии включенного GPS и дрон может быть уязвим для подмены GPS-координат [5],
- для защиты БПЛА от наводок и помех используются ферритовые сборки (фербиды) в электронных схемах устройств, которые пропускают на плату “чистый” сигнал и делают дрон менее чувствительным к внешним помехам, что выражается в таких характеристиках, как: добротность колебательного контура, резонансной частоте и т.д. [6].

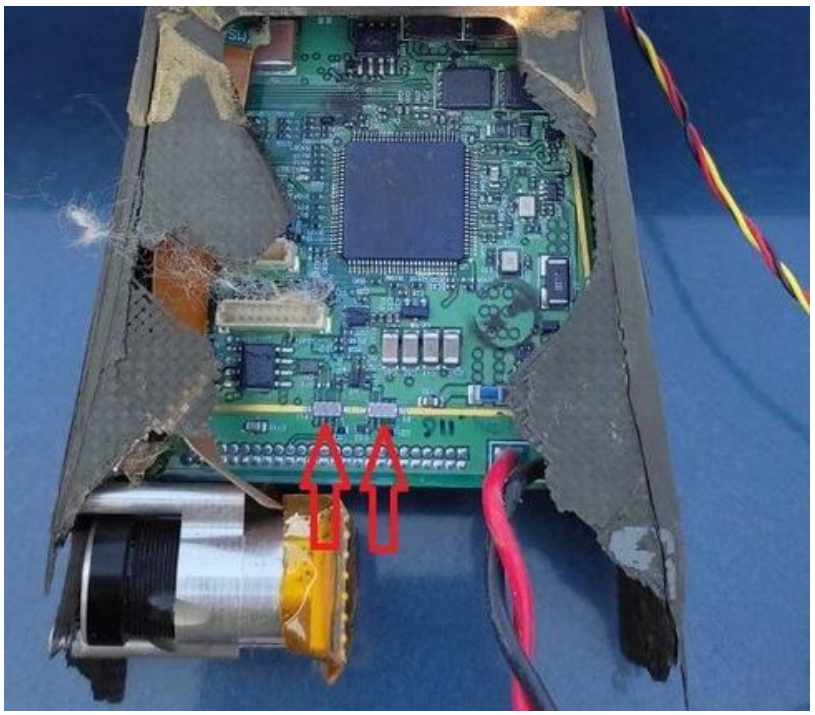

Рисунок 2. Использование ферритовых сборок в БПЛА [7].

Некоторые рекомендации по использованию ферритовых сборок (фербидов) в БПЛА:

- необходим правильный выбор типа и размера фербидов с учетом рабочих характеристик сигнала и частоты устройства,
- необходимо размещать фербиды на плате БПЛА таким образом, чтобы они не затрудняли прохождение сигнала, но одновременно были защищены от механических повреждений,
- использование ферритовых сборок в соответствии со стандартами и рекомендациями производителя,
- проведение регулярных технических работ по обслуживанию и замене феритовых сборок,
- необходим правильный выбор типа феритовой сборки, исходя из понимания, что фербид может оказывать влияние на некоторые параметры электронных схем, такие как добротность колебательного контура и резонансная частота, поэтому следите за соответствующими характеристиками.

4. Анализ методов и средств обеспечения безопасности самоорганизующихся сетей БПЛА

В современной практике дроны используют не только для одиночных вылетов, но и для работы в группах, основанных по принципу роя, которые объединены в самоорганизующуюся сеть [8]. Такие сети характеризуются разнообразными моделями мобильности и высокой степенью мобильностью узлов, динамичной и изменяемой топологией сети и низкой плотностью узлов [9].

Главным образом реализация функций безопасности осложняется для беспроводных самоорганизующихся сетей на основе БПЛА. Характерные особенности

функционирования таких сетей заключается в формировании новых условий для возникновения уязвимостей, что делает возможным реализацию угроз их безопасности.

Наиболее частыми причинами и источниками возникновения уязвимостей безопасности являются [10]:

- общая доступность среды передачи данных,
- низкая живучесть и защищенность узлов сети,
- отсутствие инфраструктуры, фиксированной топологии и центральных узлов,
- более динамичный и частый характер изменения топологии сети.

Основное требование к безопасности беспроводных самоорганизующихся сетей на основе БПЛА – обеспечить сбалансированную защиту конфиденциальности, целостности и доступности информации, которая находится в этой сети, с учетом целесообразности применения и без ущерба производительности системы [11]. Для выполнения этого требования необходимо предпринять следующие действия:

- использовать криптографические протоколы аутентификации, а также инфраструктуру открытых ключей и шифрование каналов связи,
- внедрять доверительные отношения между узлами сети БПЛА, а также использовать аппаратно-программные средства, которые усложняют компрометацию конкретного узла сети при физическом доступе к нему,
- использовать соответствующие сетевые протоколы и протоколы маршрутизации.

Анализ угроз безопасности информации, которые находятся в самоорганизующихся сетях на основе БПЛА, и требований к защите ее конфиденциальности, доступности и целостности, показывает, что наиболее важными с точки зрения информационной безопасности являются сетевой и канальный уровни, мероприятия в отношении защищенности которых целесообразно осуществлять как за счет разработки методов построения устойчивой к угрозам архитектуры сети, так и за счет исследования различных подходов и механизмов обеспечения безопасности сетей подобного типа и их дальнейшей реализации [12].

Исходя из выше сказанного предлагается несколько методик и алгоритмов, направленных на обеспечение безопасности таких сетей:

1. Алгоритм мониторинга и обнаружения атак на сеть: автоматическая система мониторинга сети обнаруживает подозрительную активность, перенаправляет трафик на сервер для анализа и блокирует доступ к сети для атакующего узла, отправляя уведомление администратору.
2. Методика шифрования сигналов передачи данных: для защиты от перехвата и манипуляций с данными в сети, каждый узел использует уникальный ключ шифрования, который регулярно меняется, а также применяется алгоритм проверки цифровой подписи передаваемых данных.
3. Методика защиты от физического доступа к устройству: для обеспечения защиты от неправомерного доступа БПЛА оснащаются датчиками движения и устройствами защиты от вскрытия, которые при обнаружении движения или попытки вскрытия автоматически отключают питание и отправляют уведомление администратору.

4. Алгоритм защиты от внедрения вредоносного ПО: для обеспечения безопасности сети каждый узел оснащается актуальным антивирусным ПО, которое при обнаружении вредоносного ПО автоматически блокирует доступ зараженного узла к сети и отправляет уведомление администратору.

Конкретные методики и алгоритмы зависят от вида самоорганизующейся сети БПЛА и требований к ее протоколам безопасности. Приведенные выше примеры могут служить отправной точкой при разработке таких сетей с повышенной защитой от внешних несанкционированных источников управляющих сигналов.

Заключение

Таким образом, исследование методов обеспечения информационной безопасности беспилотных летательных аппаратов является актуальной и важной задачей современной индустрии и технологий. Безопасность БПЛА является одним из критических факторов для их успешного применения в различных сферах деятельности. На сегодняшний день существует множество методов и технологий, которые могут быть использованы для обеспечения безопасности БПЛА, таких как шифрование данных, защита от реверс-инжиниринга и вирусов, контроль доступа и т.д. Однако, в связи с постоянным развитием технологий и возникновением новых угроз, необходимо постоянно совершенствовать методы обеспечения безопасности беспилотных летательных аппаратов. Важно учитывать, что безопасность БПЛА не только защищает их от внешних угроз, но и способствует сохранению жизней и предотвращению катастроф в воздухе. Поэтому, исследование методов обеспечения информационной безопасности беспилотных летательных аппаратов является неотъемлемой частью их успешного применения в различных областях деятельности.

Для того чтобы обеспечить безопасность БПЛА, необходимо принимать комплексные меры по защите информации, а также использовать современные технологии и методы обнаружения и предотвращения атак. Важно учитывать, что безопасность БПЛА должна быть рассмотрена на всех этапах их жизненного цикла - от проектирования и разработки до эксплуатации и вывода из эксплуатации. Также необходимо учитывать, что в различных сферах деятельности требуются разные требования к безопасности БПЛА и методы их обеспечения, поэтому следует разрабатывать индивидуальные подходы и решения для каждого конкретного случая. В целом, исследование методов обеспечения информационной безопасности беспилотных летательных аппаратов является актуальной и важной задачей, которая поможет повысить эффективность и безопасность использования БПЛА в различных сферах деятельности.

Список литературы

1. Швецова С.В., Швецов А.В. Анализ безопасности при перевозке грузов беспилотными летательными аппаратами // журнал “Мир транспорта”, том 17, №5, 2019, с. 286-297.

2. Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 1. Беспилотный летательный аппарат как объект обнаружения и поражения // журнал “Системы управления, связи и безопасности”, 2020, №1.

3. Дудко А. Л. Определение актуальных угроз беспилотного летательного аппарата // EUROPEAN SCIENCE FORUM, 2020, с. 58-65

4. Мартыненко А. А. Противодействие угрозам нарушения безопасности информации беспилотных летательных аппаратов с помощью протокола BB84 с поляризационным кодированием состояний фотонов // МИРОВАЯ НАУКА: НОВЫЕ ВЕКТОРЫ и ОРИЕНТИРЫ : Материалы VII Международной научно-практической конференции, Ростов-на-Дону, 2022 года, Том Часть 2, с. 11-15.

5. Теодорович Н. Н., Строгонова С.М, Абрамов П.С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // интернет журнал “Науковедение”, 2017.

6. Гулевич С. П., Веселов Ю. Г., Прядкин С. П., Тырнов С. Д. Анализ факторов, влияющих на безопасность полета беспилотных летательных аппаратов. Причины авиационных происшествий беспилотных летательных аппаратов и способы их предотвращения // Электронный научно-технический журнал “Наука и образование”, 2012.

7. Использование ферритовых сборок в БПЛА [Электронный ресурс] URL: https://t.me/UAVDEV/1369 (дата обращения: 24.03.23)

8. Hentati A.I., Fourati L.C. Comprehensive survey of UAVs communication networks. Comput. // Stand. Interfaces, 2020, vol. 72, art. 103451.

9. Кулагин Г.И. Анализ проблем обеспечения безопасности беспроводных самоорганизующихся сетей на основе беспилотных летательных аппаратов // Политехнический молодежный журнал МГТУ им. Н.Э. Баумана, 2022, № 03

10. Демидов Р.А., Зегжда П.Д. Унифицированная модель многоуровневых угроз нарушения информационной безопасности в сетях с динамической топологией // Интеллектуальные технологии на транспорте, 2019, № 2, с. 10-14.

11. Dahiya S., Garg M. Unmanned aerial vehicles: vulnerability to cyber attacks. // Proc. UASG, 2019, с. 201–211.

12. Sampigethaya K., Poovendran R., Bushnell L. Security of future eEnabled aircraft ad hoc networks // AIAA Meeting Paper, 2008, № 2008-8894.

Информация об авторах

Власов Андрей Игоревич, канд. техн. наук, доцент кафедры «Проектирование и технология производства ЭА» МГТУ им. Н.Э. Баумана (НИУ), e-mail: vlasovai@bmstu.ru.

Салуев Евгений Алексеевич, студент кафедры «Проектирование и технология производства ЭА» МГТУ им. Н.Э. Баумана (НИУ), e-mail: saluev.evgeniy@gmail.com

Махмудов Тимур Назимович, студент кафедры «Проектирование и технология производства ЭА» МГТУ им. Н.Э. Баумана (НИУ), e-mail: mahmudov.timur701@gmail.com

Федотов Айсен Андреевич, студент кафедры «Проектирование и технология производства ЭА» МГТУ им. Н.Э. Баумана (НИУ), e-mail: kirball261@gmail.com