ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОМУ ДОБЫВАНИЮ ИНФОРМАЦИИ ДРОНАМИ

Кривенков Дмитрий Вадимович

студент, Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет», РФ, г. Уфа

Миронов Константин Валерьевич

научный руководитель, канд. техн. наук, старший преподаватель, Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет», РФ, г. Уфа

ВВЕДЕНИЕ

Появление в XXI веке беспилотных летательных аппаратов, и их массовое распространение создало массу новых проблем различного характера такие как несанкционированное получение информации.

В современном мире все тяжелее скрыть информацию и объекты от посторонних глаз. Если раньше можно было запретить спутникам фотографировать определенную территорию и/или делать спутниковые снимки замазанными, или скрывать объекты при пролете спутника над объектом, то с развитием беспилотных летательных и наземных аппаратов скрыть объекты становится тяжелее.

На 2017 год развитие БПЛА и его массовость развивается, как и в позитивном ключе (поиск пропавших людей, протечек газа, доставка посылок и т.д.) так и в отрицательном ключе над различными режимными объектами (аэропортами, портами, верфях, заводов и т.д.) в местах плотной застройки или над частными территориями. Также не стоит забывать и о военной сфере, где беспилотники начинают представлять существенную угрозу чем с 1990 по 2001 год, когда в небе могло находится максимум три летательных аппарата с некоторыми ограничениями.

В связи с этими остро встал вопрос как защитить объекты инфраструктуры и организаций от несанкционированного доступа и защититься свои беспилотники от взлома.

1 Общесистемная часть

1.1 Анализ предметной области

1.1.1 Проблематика предметной области

Тема Противодействие несанкционированному добыванию информации дронами становится все более и более актуальной. Растет опасность от того что дроны начинают летать там, где пролет должен быть либо санкционирован или вовсе запрещен (территория аэропорта, тюрьмы, промышленного предприятия и других зон.).

Система по борьбе с нарушителями должна быть эффективна и иметь несколько различных способов для взлома бпла так и быть не дорогой.

На данный момент тревогу бьют аэропорты где дроны стали появляется в большом количестве и уже создают проблемы. Зафиксирован случай столкновения дрона с самолетом [1], залет в ангары где производятся ремонтные работы воздушных судов. При этом методы борьбы с пернатыми (от пугал до дрессированных хищных птиц) против коптеров неэффективны. В некоторых странах (например, в Голландии и Франции) орлов и соколов учат «перехватывать» дроны, но широкого распространения такая практика не получила [2]. Уже сейчас самолеты чаще сталкиваются с беспилотниками, чем с птицами.

Сейчас начинают появляются различные способы для борьбы с дронами, от беспилотников с сетками и электромагнитных ружей до систем радио электронной разведки и лазеров военного образца. Также как различные стартапы начинают получать финансирование как от правительственных структур, так и частных предприятий, и организаций.

Недавно Пентагон выделил солидную сумму на стартап SkySafe — систему обнаружения и поимки БПЛА, представляющих угрозу. Помимо США такие же работы ведут в России, концерн Калашникова предлагает свою электромагнитное ружье для силовых структур и различных частных предприятий для борьбы с дронами. Вооружённые силы России разрабатывают свои мобильные системы по взлому и перехвату дронов.

На прошлой неделе исследовательская группа из Альянса за безопасность системы UAS через Research Excellence (ASSURE) опубликовала отчет о том, что столкновения беспилотных самолетов с крупными пилотируемыми самолетами могут нанести больше структурных повреждений, чем птицы того же веса для данной скорости удара [3].

1.1.2 Общая технико-экономическая характеристика объекта

На данный момент во главу угла ставится эффективность и мобильность. На данный момент на рынке большой спрос на данные системы, но отсутствуют предложения. Так Концерн “Калашников” находится на стадии тестирование прототипа Rex-1, ружьё подавляет каналы навигации и передачи дронов, а также их фото- и видеокамеры в оптико-электронном диапазоне, ГНИИЦ РТ МО РФ в рамках форума «Армия-2017» представил образец ружья «Ступор», при выстреле «Ступор» излучает мощный электромагнитный импульс, который направлен на подавление канала управления беспилотным летательным аппаратом.
Под воздействием излучения дрон теряет связь с оператором, что теоретически приводит к его неконтролируемому падению. Американский стартап показал ружье “Скайнет” который блокирует сигналы GPS которые идут к дрону и отключает камеру, но дальше чем рекламного ролика дело не идет, стартап SkySafe из Сан-Диего сосредоточен вокруг технологии создания системы принудительной посадки вражеских дронов. Система также будет обладать способностью в некоторых случаях возвращать коммерческие модели ботов на исходную позицию, что позволит выяснить местонахождение командного центра противника. Данный стартап уже подписал договор с DIUx, который по сути является офисом Пентагона на базе Кремниевой долины.

1.1.3 Анализ текущего методов взлома управления дронов

Основная уязвимость беспилотников остаются каналы связи. Перехват видеопотоков, а также GPS-Spoofing, последня на данный момент является самой сложной и вдобавок самым надежным способом перехвата управления беспилотником. Ниже приведены примеры взломов:

1. Место: Ирак, Афганистан

Модель: Predator MQ-1 Predator (US$4.03 million, 2010)

Взломщик: «иракские хакеры»

Уязвимость: канал передачи данных с БПЛА в наземный центр управления

В 2008 году, когда был взят в плен повстанец, на ноутбуке которого хранились изображения, полученные с американских беспилотников. Летом 2009 года также были обнаружены компьютеры с несколькими часами видеозаписей с БПЛА. Повстанцы использовали для видеоперехвата незащищенные каналы связи с БПЛА. При этом они использовали программное обеспечение, такое как, например, SkyGrabber, которое можно купить через интернет всего за 25,95 доллара.

SkyGrabber, согласно описанию российской компании-производителя SkySoftware, «принимает и обрабатывает трафик, передаваемый со спутника, извлекает из него файлы и сохраняет их на ваш жесткий диск в соответствии с настроенными фильтрами».[4]

2. Место: Иран

Модель: RQ-170 Sentinel

Взломщик: Персидские специалисты

Уязвимость: GPS-спуфинг

Иран представил средствам массовой информации пресс-релиз, в котором говорилось об успешном перехвате американского беспилотного летательного аппарата типа RQ-170 Sentinel. Среди прочих версий о перехвате аппарата фигурировала и та, что касалась использования специальной электроники, заглушивший сигнал спутников системы GPS и подменившей его своим. В результате этих действий беспилотник в автоматическом режиме, ориентируясь по глобальной системе навигации, начал возвращение домой. Поскольку истинный сигнал спутников был заглушен ложным, то RQ-170 сел на иранский аэродром, приняв его за свой «родной». Однако это только версия, хотя и достаточно правдоподобная. Первые сообщения о таком способе перехвата поступили вскоре после публикации пресс-релиза и делались они со ссылкой на некоего иранского инженера, якобы имеющего самое прямое отношение к операции по перехвату.[5]

2. Место: Техас

Модель: Вертолет для полива

Взломщик: Todd Humphreys

Уязвимость: GPS-спуфинг

В 2012 году американскими учёными из Техасского университета в Остине была доказана практическая возможность взлома и перехвата управления БПЛА путём GPS-спуфинга.

GPS-спуфинг можно провести только для тех аппаратов, которые используют незашифрованный гражданский сигнал GPS.[6]

Spoofing атака на GPS — атака, которая пытается обмануть GPS-приемник, широковещательно передавая немного более мощный сигнал, чем полученный от спутников GPS, такой, чтобы быть похожим на ряд нормальных сигналов GPS. Эти имитирующие сигналы изменены таким способом, чтобы заставить получателя неверно определять своё местоположение, считая его таким, какое отправит атакующий. Поскольку системы GPS работают измеряя время, которое требуется для сигнала, чтобы дойти от спутника до получателя, успешный спуфинг требует, чтобы атакующий точно знал, где его цель — так, чтобы имитирующий сигнал мог быть структурирован с надлежащими задержками сигнала.

Атака спуфинга GPS начинается, широковещательно передавая немного более мощный сигнал, который указывает корректную позицию, и затем медленно отклоняется далеко к позиции, заданной атакующим, потому что слишком быстрое перемещение повлечет за собой потерю сигнальной блокировки, и в этой точке spoofer станет работать только как передатчик

помех. Spoofing GPS был предсказан и обсужден в сообществе GPS ранее, но никакой известный пример такой вредоносной атаки спуфинга ещё не был подтвержден.[6]

29 июля 2013 студентам из университета Остина, Техас, удалось отклонить от курса 213-футовую яхту с помощью метода GPS-спуффинга.[7]

В ноябре 2016 появилась информация о том, что служба безопасности Кремля использует оборудование, имитирующее сигналы спутника GPS на частоте L1. Действительная локация подменяется координатами аэропорта «Внуково», что, вероятно, связано с опасениями использования гражданских дронов вблизи правительственных зданий.[8]

1.1.4 Обоснование выбора данного направления в качестве объекта исследований

С практически молниеносного развития беспилотных летательных так и наземных аппаратов, практически не уделялось внимание защите каналов связи, которые являются основными для беспилотников. При этом нет и защиты от беспилотников которые используются от обычной сьемки с высоту до поражения живой силы и зданий. Так на различных ресурсах есть видео записи с беспилотников которые сбрасывают бомбы на бронетехнику и солдат, сьемки частной жизни людей, случаи аварий беспилотников с самолетами, доставка наркотиков, шпионаж за объектами и т.д. Основная проблема и кроется в том, что практически нет способом защититься от атак или поймать беспилотник.

Последний инцидент, когда для того чтобы уничтожить гражданский беспилотник стоимостью в 1500$ был сбит ракетой стоимостью в 40000$. В связи с этим целью моей работы является анализ систем и научных работ в области взлома каналов связи для того чтобы предложить эффективную и как можно дешевую систему по перехвату различных дронов.

1.2 Информационное обследование использование дронов

1.2.1 Описание существующего положения

На данный момент особое внимание уделяется беспилотникам в военной области, перехватчики, истребители, бомбардировщики в перспективе перевести на наземные части на автономное управление. Уже сейчас Пентагон предлагает передавать боевые задания по каналам связи напрямую пилотам истребителей, а в будущем координировать таким образом уже беспилотники.

И актуальной темой становится не уничтожение сил противника, а перехват, подмена боевых задач. Опираясь на фразу “Война – двигатель прогресса” ожидается развитие гражданских систем перехвата беспилотников. Ведь как пример можно взять пример Японию где мафия переправляет наркотики с помощью дронов, а полиция на данный момент перехватывает такие дроны, дронами с сетями. Некоторые люди ради забавы ставят на дроны бензопилы.

Рисунок 1. Квадрокоптер “KillerDrone”

И против такой напасти есть только старые способы борьбы, сети и дробовики.

Для защиты от напасти военные разрабатывают целые комплексы такие как “1Л222 Автобаза” которая предназначена для перехвата дронов, но для защиты тюрем, территорий заводов и для поимки доставщиков наркотиков и других нарушителей нет надежных и простых способов, и для перехвата требуются знания в области защиты информации, программирование и работы с данными GPS. Так ружье от концерна Калашникова хоть и вписывается в систему унифицированной системы, но минус данной системы в дальности.

1.2.2 Выбор базы для системы по перехвату

Как уже стало ясно самая слабая сторона систем, чем больше система, тем лучше и надежнее она работает, при уменьшении размеров система становится более узко направленной. Как способ спасения оснащение либо автомобилей системой, состоящей из нескольких компонентов которая будет питаться от аккумулятора автомобиля, с учетом что полицейский автомобиль в основном находится в движении, второй способ больше подойдёт для защитных каких либо зон (промышленных или муниципальных) например разместить систему на уже существующих вышках сотовой связи или как более простой способ использовать другой дрон.

Больший интерес вызывает сам перехват дронов, сейчас основным способом полета дрона на большие расстояния в дрон закладывается маршрут, и если управление берет оператор но совсем на короткий промежуток. В этом и есть главная проблема, неважно дрон или крылатая ракета, проблема в определении своего положения по общей карте GPS меняется только точность позиционирования в зависимости от начинки беспилотника. Так обычной дрон используя обычный сигнал GPS или Glonass не имея доступа к наземным точкам позиционирования имеет минимальную погрешность в 6 метров, если количество спутников которые “видит” дрон падает то погрешность увеличивается. У крылатых ракет также используются общедоступные сигналы GPS.

Основная проблема заключается в том, что для управления дронами используются небезопасные методы. Применяются протоколы общего назначения, отсутствуют средства

надёжной аутентификации, сигнал GPS легко глушится, а загрузчик даже не проверяет цифровую подпись прошивки. В результате типовое программное обеспечение базовой станции позволяет вмешаться в полёт чужих дронов и угнать их.

Мощность сигнала – один из ключевых факторов. По мере удаления дрона от контроллера она падает, и в какой-то момент атакующая сторона оказывается в выигрыше за счёт более близкого расположения. Чтобы сбить с толку пролетающий мимо дрон достаточно сравнительно маломощного оборудования.

Одним из первых на это обратил внимание Сами Камкар (Samy Kamkar). Пару лет назад для демонстрации уязвимости он даже превратил игрушечный дрон Parrot AR в радиоперехватчик. Летая среди других беспилотников, он сканировал диапазон 2,4 ГГц при помощи модуля Wi-Fi. Размещённый на борту одноплатный компьютер Raspberry Pi обрабатывал собранные пакеты программой SkyJack. Обнаружив управляющие команды для других дронов, он подменял их и заставлял следовать обманутые беспилотники за собой, заглушая сигналы настоящих контроллеров.

Более сложные БПЛА вместо Wi-Fi используют другие технологии беспроводной связи, но во время полёта они также интенсивно обмениваются данными с наземной станцией и запрашивают корректировки маршрута. Пакеты телеметрии всегда можно расшифровать, модифицировать и использовать для перехвата управления. При атаке по типу MitM дрону отправляются ложные корректировки маршрута, а от диспетчера скрывается истинное местоположение беспилотника. Однако проблема кроется не столько в конкретных ошибках, сколько в недостатке общего подхода к проектированию.

1.2.3 Защита сигналов, получаемых дроном

Недавно обновленные технические решения для электронной защиты и автоматизированные системы управления Uavos обеспечивают эффективные контрмеры против последнего спуфинга GPS, не позволяя угрозам перенаправлять беспилотный летательный аппарат или дестабилизировать работу его бортовой навигационной системы.

По словам Вадима Тарасова, инвестора и члена правления Uavos в условиях радиоэлектронного влияния, система противодействия UAVOS против GPS и других атак с использованием спутников GNSS отключает навигацию GPS и переключается на автономный полет с встроенной интегрированной инерциальной навигационной системой. Эта система была специально разработана с целью определения с высокой точностью местоположения ее носителя и обладает сложной обработкой и навигационной информацией, полученной в отсутствие наземных, морских или космических сигналов.

Система контрмер обеспечивает защиту беспилотных летательных аппаратов и повышает живучесть и эффективность беспилотного летательного аппарата. БПЛА, оснащенный такими контрмерами против систем электронной войны, позволяет воздушному судну вернуться на базу и выполнить свою миссию с навигационной ошибкой в 1,2-2,5 мили (2-4 км) за час полета.

«Система противодействия атакам спутников GPS является результатом многолетней систематической работы Uavos в области контрмер EW», - продолжил Вадим Тарасов. «Испытательные рейсы наших беспилотных летательных аппаратов показали эффективность выполнения миссии в условиях сложных помех и неуязвимость беспилотных транспортных средств к системам EW последнего поколения».[9]

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы был проанализирована ситуация с беспилотными аппаратами, и угроза, которая от них иногда исходит. Также были описаны два основных способа воздействия на дроны для его отключения или перехвата. К сожалению скорость развития беспилотной техники идет быстрее чем развитие способов защиты самих дронов от перехвата.

На данный момент в гражданской сфере квадрокоптеры это всего лишь “игрушка”, которая при неправильном использовании превращается в оружие. Используются для достижения преступных целей. Остро также стоит вопрос защиты от этих “игрушек” ведь это идеальные шпионы, они практически невидимы и их практически невозможно засечь.

В военной же сфере страшна не потеря дрона, а его перехват или переписывание боевой задачи, чем могут воспользоваться противники.

Список литературы:

1. Drones more damaging than bird strikes to planes, study finds [Электрон, ресурс]. - 2017. Режим доступа: https://news.osu.edu/news/2017/12/06/study-finds-drones-more-damaging-than-bird-strikes-to-planes/.

2. Uavos Improves GPS Spoofing Protection for UAVs [Электрон, ресурс]. – 2017. Режим доступа: http://www.unmannedsystemstechnology.com/2017/10/uavos-improves-gps-spoofing-protection-uavs/.

3. UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea [Электрон, ресурс]. – 2013. Режим доступа: https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea.

4. Взлом дронов [Электрон, ресурс]. - 2017. Режим доступа: https://habrahabr.ru/company/neuronspace/blog/254685/.

5. «Вы во Внуково, здравствуйте» [Электрон, ресурс]. – 2016. Режим доступа: https://lenta.ru/articles/2016/11/07/gpsoff/.

6. Дрон врезался в самолёт: зачем нужна регистрация? [Электрон, ресурс]. - 2017. Режим доступа: https://www.popmech.ru/technologies/237765-dron-vrezalsya-v-samolyet-zachem-nuzhna-registratsiya/.

7. Сапсаны научат людей перехватывать дроны [Электрон, ресурс]. - 2017. Режим доступа: http://www.nat-geo.ru/nature/1174271-sapsany-nauchat-lyudey-perekhvatyvat-drony/.

8. Спуфинг [Электрон, ресурс]. – 2013. Режим доступа: https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D1%83%D1%84%D0%B8%D0%BD%D0%B3.