DOI: 10.18137/RNU.V9187.23.03.P.157 УДК 004.056

А.Р. Кузьмин, М.Ф. Савельев

# АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И КАНАЛОВ СВЯЗИ КОММЕРЧЕСКИХ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

**Аннотация.** Статья продолжает цикл публикаций, посвященных информационной безопасности беспилотных авиационных систем. Целью настоящей статьи является анализ векторов атак на программное обеспечение и каналы связи беспилотных авиационных систем. Кроме того, проводится обзор методов защиты от подобных атак. При проведении исследований применялись методы контент-анализа и эксперименты с коммерческими беспилотными авиационными система доступных для гражданских пользователей. В результате был разработан систематизированный перечень атак на программное обеспечение и каналы связи.

*Ключевые слова:* БПЛА, БАС, целостность, киберфизические системы, безопасность программного обеспечения, информационная безопасность.

A.R. Kuzmin, M.F. Saveliev

# ACTUAL CIVILIAN UAS SOFTWARE AND COMMUNICATIONS INFORMATION SECURITY PROBLEMS

**Abstract.** With this article, the authors continue the series devoted to the information security of UAS. The purpose of this article is to analyze attack vectors on UAS software and communication channels. In addition, the authors reviewed methods of protection against such attacks. In their work, the authors applied content analysis methods and experiments with real commercial unmanned aerial systems available to civilian users. As a result, the authors have developed a systematic list of attacks on software and communication channels, presented in the form of tables in this article.

*Keywords:* UAS, UAV, Integrity, cyber-physical systems, software security, information security.

## *Введение*

От фото- и видеосъемки, доставки небольших грузов – до геологоразведки и контроля состояния газопроводов беспилотные летательные аппараты (далее – БПЛА) находят всё больше применений в деятельности человека. Беспилотная авиационная система является совокупностью БПЛА и наземной станции управления, которая может быть представлена как сложной стационарной кабиной со спутниковой связью и несколькими постами управления, так и смартфоном или планшетом с установленным программным обеспечением дистанционного управления. Так или иначе, беспилотная авиационная система (далее – БАС) является объектом интереса с целью осуществления атак на ее компоненты со стороны как энтузиастов-одиночек, криминальных группировок, так и поддерживаемых на государственном уровне профессионалов – представителей противоборствующих сторон.

На Рисунке 1 представлена общая архитектура БАС.

**Кузьмин Александр Ростиславович**
аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Санкт-Петербург. Сфера научных интересов: информационная безопасность киберфизических систем, распределенные реестры, разведка по открытым источникам. Автор пяти опубликованных научных работ.
Электронный адрес: alexander.kouzmin@gmail.com

**Савельев Максим Феликсович**
кандидат технических наук, доцент кафедры информационной безопасности, Санкт-петербургский электротехнический университет «ЛЭТИ», Санкт-Петербург. Сфера научных интересов: искусственный интеллект, информационная безопасность, беспилотный транспорт. Автор более 10 опубликованных научных работ.
Электронный адрес: mfsavelev@etu.ru

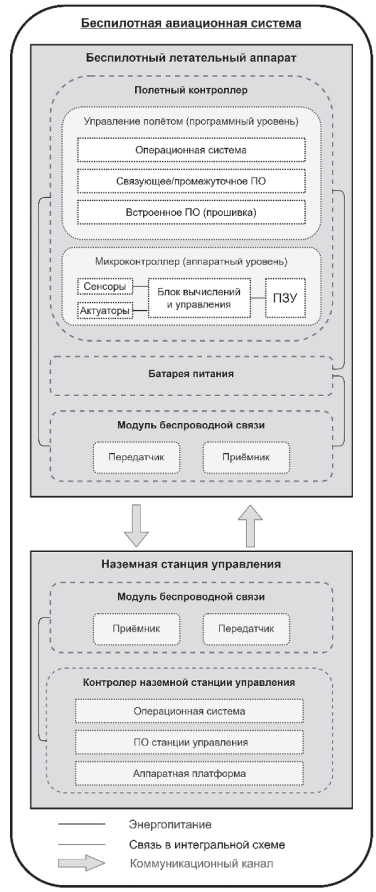


**Рисунок 1.** Архитектура БАС
*Здесь и далее рисунки и таблицы составлены авторами

*Архитектура программного обеспечения*

Архитектура программного обеспечения БПЛА имеет многоуровневую структуру. Интеграция между этими уровнями составляет полетный стек или полетный контроллер, состоящий из трех основных уровней:

• микропрограмма (прошивка) является нижним уровнем полетного стека, который предоставляет инструкции из машинного кода процессору полётного контроллера;

• промежуточное программное обеспечение представляет собой уровень, отвечающий за надлежащее управление полетом путем управления связью между службами, такими как управление, навигация и телекоммуникации;

• операционная система реального времени обрабатывает данные в режиме реального времени и позволяет программному обеспечению БПЛА управлять различными процессами, такими как полет, видеозапись и планирование маршрута. Программное обеспечение наземной станции управления включает в себя человеко-машинный интерфейс, который отображает параметры полета и обычно работает на ноутбуках, планшетных компьютерах или других устройствах в полевых условиях.

Программное обеспечение наземной станции управления также известно как планировщик миссий. Оно включает в себя человеко-машинный интерфейс, который отображает параметры полета и обычно работает на ноутбуках, планшетах или любых устройствах в полевых условиях.

*Каналы связи*

Канал связи в общем случае представляет собой беспроводную связь между наземной станцией управления и БПЛА. Он обеспечивает передачу данных во время выполнения полетного задания. Однако из-за погодных условий и ограниченного энергоснабжения частоты передачи и дальность полета могут иметь ряд ограничений. Выделяются два типа коммуникационных потоков: передача данных и передача сигналов управления. При передаче информации БПЛА отправляет данные, такие как телеметрия и статус состояния, на наземную станцию управления. Находясь в режиме управляющей связи, наземная станция управления отправляет команды и сигналы управления на БПЛА. Связь с БПЛА может осуществляться через точки-ретрансляторы, такую связь обозначают как БПЛА-2-Х. Но более популярной для гражданских БПЛА является тип связи непосредственно с наземной станцией управления (далее – НСУ), минуя промежуточные точки.

БПЛА-2-Х – во время полета БПЛА связывается с несколькими объектами.

БПЛА-2-НСУ – основной тип связи для БПЛА. НСУ обменивается данными с БПЛА по восходящей и нисходящей линиям связи, что позволяет отслеживать трафик и управлять полетным заданием. Рассмотрим три класса передаваемого трафика в связи БПЛА-2-НСУ: контрольный, координационный и зондирующий. Управляющий трафик включает в себя команды управления и контроля, в частности команды для конкретных полетных миссий и запрос статуса БПЛА в реальном времени (например, данные телеметрии, уровень заряда батареи и др.). Координационный трафик обеспечивает взаимодействие между несколькими БПЛА во время полетного задания и выполняемых задач. Может проходить, минуя наземную станцию управления, например, в рамках процесса предотвращения столкновений. Зондирующий трафик – это трафик, проходящий на борту БПЛА между сенсорами, контроллером полета, иными бортовыми подсистемами. Отметим, что все типы трафика в коммуникациях БПЛА-2-НСУ основаны на беспроводных технологиях с ограниченным радиусом действия, таких как Bluetooth или Wi-Fi

802.11, и в большинстве случаев не защищены, что делает их уязвимыми для пассивных и активных атак.

**Связь БПЛА со спутником.** В миссиях за пределами прямой видимости оператору необходимо определить местоположение БПЛА для безопасной навигации. Таким образом, БПЛА могут установить канал спутниковой связи, чтобы определить свое местоположение в режиме реального времени, а затем передать его обратно на НСУ через спутник. Кроме того, спутниковая связь необходима на больших расстояниях без наличия инфраструктуры и обеспечивает надежное взаимодействие с высокой пропускной способностью. Также коммерческая спутниковая связь может быть использована для управления БПЛА. К недостаткам спутниковой связи можно отнести высокое энергопотребление и дорогое с точки зрения затрат обслуживание, а также вероятность задержек при передаче сигнала.

**Сотовая связь с БПЛА.** На большой высоте, будь то в городской или сельской местности, сотовая связь с БПЛА гарантирует широкую зону покрытия и включает сотовые сети с наземными пользователями смартфонов и других устройств. В этой интеграции БПЛА работают либо как воздушное пользовательское оборудование (UE), либо как воздушные базовые станции (BS). Когда они действуют как пользовательское оборудование, также известное как БПЛА с сотовой связью, они устанавливают связь «БПЛА – сотовая связь» с наземной базовой станцией, при которой оператор БПЛА может напрямую управлять БПЛА через сотовые сети. БПЛА в качестве воздушных базовых станций дополняют наземные базовые станции. Они обеспечивают надежные и экономичные беспроводные сотовые сети для покрытия областей, где наземные базовые станции недоступны. Несмотря на преимущества использования БПЛА в сотовых сетях в обоих сценариях, их реальное развертывание сталкивается с рядом проблем, таких как ограниченная производительность и низкая энергоэффективность.

Связь между несколькими БПЛА называется «воздух – воздух» или «БПЛА-2 – БПЛА» и осуществляется во время полетов, требующих использования нескольких БПЛА. В таких сценариях беспилотные летательные аппараты сотрудничают и координируют свои действия с помощью беспроводных технологий с низким энергопотреблением (например, Bluetooth, Zigbee и др.) для обмена информацией напрямую или через беспроводные каналы с несколькими переходами-ретрансляторами. В этом случае один БПЛА работает в сети для обмена данными и выполнения полетной задачи. К недостаткам связи «БПЛА-2 – БПЛА» можно отнести низкую пропускную способность и узкую полосу пропускания.

В общем случае связь БПЛА функционирует в рамках многоуровневой архитектуры и включает физический уровень, MAC-уровень, сетевой и транспортный уровни. К сожалению, внедрение решений безопасности для этих уровней затруднено из-за таких характеристик БПЛА, как время автономной работы, нехватка бортовых ресурсов, необходимость вычислений в реальном времени и наличие автономного управления. Эта проблема вызывает различные уязвимости на сетевом уровне, которые будут описаны в настоящей статье.

*Уровень программного обеспечения (далее – ПО)*

После обсуждения общей архитектуры программного обеспечения БАС можно перейти к описанию уязвимостей, угроз и атак, нацеленных на программный уровень БПЛА, а также существующих механизмов для защиты от подобных атак.

**Уязвимости программного обеспечения.** Уязвимости и угрозы на уровне ПО для БПЛА состоят из вредоносного программного обеспечения и уязвимостей нулевого дня. Наземная станция управления и контроллер полета подвержены влиянию вредоносного программного обеспечения. Угрозы, исходящие от вредоносного ПО для БПЛА, могут привести к потере конфиденциальных данных, целостности и контроля над управляемой системой БПЛА. Доступ злоумышленника к полетному стеку БПЛА потенциально может привести к отключению системы БПЛА, что приведет к отказу в обслуживании и, следовательно, к срыву полетной задачи. Внедрение такого вредоносного ПО в БПЛА может поставить под угрозу их безопасность. Например, вредоносное ПО Maldrone заражает полетный контроллер вирусом, позволяя злоумышленнику перехватить управление БПЛА [2]. Он воздействует как прокси-сервер контроллера полета БПЛА и связи с датчиками, что позволяет скомпрометированному БПЛА приземляться в любом выбранном месте. SkyJack – это вредоносное ПО для угона БПЛА, которое может быть развернуто злоумышленниками [3]. Данное ПО с помощью беспроводной связи может захватить контроль над другими «легитимными» БПЛА с помощью атаки де-аутентификации Wi-Fi и поставить под угрозу всю систему.

**Уязвимости нулевого дня.** В полетном стеке БПЛА или программном обеспечении наземной станции управления могут существовать неизвестные уязвимости (например, переполнение буфера, отказ в обслуживании и др.). Эти уязвимости неизвестны производителям БПЛА и могут представлять серьезную угрозу для операторов. Злоумышленники могут постоянно эксплуатировать уязвимости нулевого дня, пока производители БПЛА не выпустят соответствующие исправления. Однако операторам необходимо обновлять свои системы БПЛА для каждого выпущенного исправления.

**Атаки на программное обеспечение.** Программные атаки на БПЛА включают в себя атаки на операционную систему ПО управления видеопотоком и подмены системных идентификаторов. Потенциальные атаки могут происходить через системное программное обеспечение контроллера полета. В результате скомпрометированное системное ПО приведет к потере БПЛА и их полезной нагрузки. Посылочные коптеры сервиса Prime Air, разработанные Amazon, являются примером гражданских приложений, которые могут подвергаться атакам на уровне операционной системы. Атака на систему доставки потенциально может быть использована для кражи посылки адресата, перевеса груза для потери БПЛА. Атака на операционные системы БПЛА состоит из удаленного внедрения вредоносного программного обеспечения, такого как Maldrone, а затем захвата дрона путем получения контроля над системой. С этой целью злоумышленник может извлечь криптографический ключ и украсть или скомпрометировать сохраненные незашифрованные данные.

**Фальсификация видеопотока.** Чтобы гарантировать безопасную навигацию и избежать столкновений во время полета, операционной системой используются системные вызовы, которые позволяют захватывать видео с бортовой камеры. Однако хорошо осведомленный с параметрами системы злоумышленник может перехватить системные вызовы для захвата БПЛА. Злоумышленник также может комбинировать фальсификацию с атакой подмены GPS-сигнала для управления БПЛА. В отличие от атак на операционную систему основная цель злоумышленника – поставить под угрозу безопасность навигации и вызвать столкновение БПЛА с другим объектом.

**Подмена системного идентификатора.** В соответствии с правилами безопасности полета в некоторых странах БПЛА должны предоставлять свой системный идентифика-

тор и местоположение третьим сторонам, таким как федеральные агентства и правоохранительные органы, когда это необходимо. Однако большинство существующих БПЛА не реализуют механизмы шифрования и, следовательно, злоумышленник может выдать себя за третье лицо и выполнить атаку с подменой личности, чтобы скомпрометировать канал связи и получить системный идентификатор БПЛА. Производители БПЛА всё чаще вводят ряд ограничений на программном уровне в свои изделия, например, для запрета их использования противоборствующими сторонами в зоне конфликта. Поэтому становятся популярны альтернативные (неофициальные) обновления прошивок (firmware) гражданских БПЛА. Злоумышленник может распространять микропрограммы обновлений прошивок с логическими ошибками (бэкдор) [4].

**Противодействие атакам на программное обеспечение.** Регулярное обновление операционной системы может предотвратить компрометацию БПЛА и их полезной нагрузки. Кроме того, функционирующий межсетевой экран на наземной станции управления может блокировать отправку вредоносного трафика на БПЛА. Программные решения, такие как антивирус и IDS, могут отслеживать сетевой трафик и защищать БПЛА от вредоносных действий. Однако внедрение бортовых IDS является сложной задачей из-за ограничений по вычислениям и энергопотреблению. Также включение механизмов авторизации для системных ресурсов БПЛА может помочь защитить системы БПЛА от выполнения вредоносного кода. Перспективным решением против программных атак является использование программных подходов к аттестации ПО. Они обеспечивают целостность программного обеспечения, работающего в полетном стеке [1]. Решения для удаленной аттестации недороги и обеспечивают надежную легитимность программного стека. Кроме того, оператор должен постоянно обновлять свою операционную систему и внедрять программные решения для аттестации, чтобы проверять легитимность кода, работающего в операционной системе. Однако стоит отметить, что представленные механизмы защиты от программных атак не могут полностью защитить полетный стек от вредоносных действий. Процесс исправления обнаруженных уязвимостей нулевого дня может занять несколько недель, делая БПЛА уязвимыми для злоумышленников.

В Таблице 1 обобщены проблемы безопасности программного обеспечения БПЛА и существующие меры противодействия.

*Таблица 1*

**Атаки на уровне программного обеспечения***

| № п/п | Тип атаки | Контрмеры | Ограничения |
|---|---|---|---|
| 1 | Вредоносное ПО | Использование межсетевого экрана. Использование антивирусных и IDS-решений | Обнаружение вредоносного ПО в режиме реального времени увеличивает вычислительные расходы |
| 2 | Уязвимости нулевого дня | Периодическое обновление системы | Некоторые производители могут выпускать патчи неделями после обнаружения уязвимостей нулевого дня |
| 3 | Атаки на операционные системы | Принятие механизмов авторизации ресурсов системы БПЛА. Аттестация ПО [1] | В сети с несколькими БПЛА управление авторизацией для роя БПЛА является сложной задачей |

*Окончание Таблицы 1*

| № п/п | Тип атаки | Контрмеры | Ограничения |
|---|---|---|---|
| 4 | Фальсификация видеопотока | Использование межсетевого экрана. Аттестация ПО [1] | Даже при надлежащих мерах безопасности легитимный пользователь, присоединившийся к сети БПЛА может подделать видеопоток |
| 5 | Подмена системного идентификатора | Периодическое обновление системы. Использование межсетевого экрана | Использование методов социальной инженерии может выявить системный идентификатор БПЛА еще во время их изготовления |
| 6 | Атака через альтернативное обновление прошивки (firmware) | Установка альтернативных обновлений только из доверенных источников. Тестирование обновления прошивки на стенде или анализ микропрограммы обновления прошивки на логические ошибки и бэкдор | Тестирование требует наличия специального стенда или дополнительного времени на работу с БПЛА вне основной миссии. Анализ кода микропрограммы требует особых навыков и времени |

*Уровень каналов связи*

Связь является важнейшим компонентом системы БПЛА для управления полетом и передачи данных. Большинство БПЛА используют беспроводную связь для обмена данными и командами с наземной станцией управления. В связи с этим необходимо описать уязвимости, угрозы и атаки на БПЛА на уровне каналов связи, которые ставят под угрозу конфиденциальность, целостность, подлинность и доступность.

**Уязвимости каналов связи.** Уязвимости и угрозы на уровне связи можно классифицировать следующим образом. Уязвимости и угрозы физического и MAC-уровня. Сложность сети беспроводной связи БПЛА – наземная станция управления открывает потенциальные уязвимости. Например, в [5] авторы продемонстрировали три различные атаки, затрагивающие коммерческие беспилотные летательные аппараты на базе Wi-Fi: атака переполнения буфера, атака DoS и атака отравления кэша ARP. Результаты их экспериментов выявили серьезные проблемы с безопасностью беспроводной связи БПЛА – наземная станция управления. Выбор правильного типа технологии беспроводной связи зависит от специфики требований полетной миссии (например, дальности передачи, рабочей частоты, категории и др.). Однако этот выбор не гарантирует успеха, поскольку должны учитываться вопросы безопасности каждого типа технологии беспроводной связи. Таким образом, фундаментальный вопрос, который остается без ответа, заключается в том, какой тип технологии беспроводной связи обеспечивает высокий уровень безопасности БПЛА для каждой области применения. Сеть БПЛА работает в режиме ad hoc, обычно называемом FANET. Эти сети имеют динамическую топологию и представляют собой критически уязвимую структуру. Увеличение сложности сети управления БПЛА приводит к увеличению уязвимостей. Атаки нацелены в основном на входы данных сенсоров и коммуникационные модули. Угрозы связи с БПЛА, такие как перехват или блокировка канала связи между контроллером полета и наземной станцией управления, могут вызвать потенциальную DoS-атаку. Кроме того, учитывая уникальные характеристики FANET, в том числе задержку и вычислительную мощность для маршрутизации данных, необходимо создавать криптографические алгоритмы для FANET, учитывающие эти характеристики. Злоумышленник мо-

жет нарушить работу сети БПЛА, отправив вредоносный трафик напрямую через наземную станцию управления или опосредованно через БПЛА. Будь то централизованная или децентрализованная архитектура, наземная станция управления постоянно находится под угрозой со стороны злоумышленника. В обеих архитектурах наземная станция управления представляет собой единую точку отказа всей сети БПЛА. Однако, несмотря на то, что механизмы безопасности реализованы для наземной станции управления, злоумышленник всё равно может прервать полетное задание, скомпрометировав летающие БПЛА. Следует подчеркнуть, что в некоторых сценариях полетное задание можно считать успешным, даже если один или несколько БПЛА будут скомпрометированы. В этом случае оператору будет достаточно минимального количества корректно работающих БПЛА.

**Атаки на каналы связи.** Атаки на сетевой уровень связи БПЛА включают подслушивание, отказ в обслуживании (DoS), «человек посередине», подделку, атаку повторного воспроизведения и др.

***Атака «подслушивание»***

Злоумышленник может выполнить атаку с прослушиванием через канал связи БПЛА – наземная станция управления, собирая данные, такие как прямые видеопотоки, показания датчиков и данные GPS, отправленные БПЛА. Поскольку большинство БПЛА избегают шифрования беспроводной связи ради повышения производительности связи, злоумышленник может прослушивать обмениваемую информацию, включая каналы телеметрии и команды наземной станции управления.

***DoS-атаки***

Злоумышленник может забить канал связи БПЛА случайным трафиком, отправив несколько запросов, что приведет к перегрузке его ресурсов и нарушению его доступности. Воздействие выполнения таких атак на БПЛА может привести к существенному увеличению задержки в сети и снижению качества приложений потокового видео. Другой способ выполнения DoS-атаки – отправка больших пакетов на наземную станцию управления в пределах определенного диапазона для отключения управляющего сигнала. Как только сигнал отключается, БПЛА переходит в состояние потери связи, что приводит к сбоям в работе канала передачи данных. В [6] авторы моделировали распределенную DoS-атаку (DDoS) на БПЛА с использованием ботнетов. Атака DDoS была смоделирована путем переполнения сетевого трафика с использованием пакетов протокола пользовательских дейтаграмм (UDP). Этот тип моделирования демонстрирует возможность проведения реальных DDoS-атак на БПЛА. Кроме того, выполнение атак деаутентификации также может лишить оператора возможности управлять БПЛА. Атака деаутентификации – это DoS-атака, состоящая в отправке пакетов деаутентификации на БПЛА для нарушения связи. Пример таких атак демонстрирует Skyjack [3].

***Атаки «человек посередине»***

В этой одной из самых известных атак злоумышленник контролирует беспроводной канал БПЛА – наземная станция управления и изменяет безопасные пакеты вредоносным содержимым. Атака с воспроизведением видео является примером атаки «человек посередине», когда злоумышленник обманывает оператора, передавая вредоносные данные в реальном времени. VideoJak является примером таких атак.

***Атака «подделка»***

Злоумышленник может поставить под угрозу целостность связи БПЛА, передав поддельный запрос на БПЛА, не прошедший проверку подлинности. В этой атаке злоумышленник генерирует вредоносный запрос, выдавая его за законный запрос.

***Атака повторного воспроизведения***

В сетях БПЛА злоумышленник может выполнить атаку с прослушиванием, чтобы перехватить несколько запросов, а затем воспроизвести достоверные данные на БПЛА. В этом случае БПЛА могут получать повторяющиеся данные, и если не будет реализована защита от повторного воспроизведения, БПЛА не смогут отличить законные запросы от вредоносных.

***Атаки на маршрутизацию***

В протоколах маршрутизации мобильных одноранговых сетей (MANET) могут возникать различные пассивные и активные атаки, которые состоят из внедрения вредоносных узлов, управления сетевым трафиком или нарушения функций маршрутизации. Большинство существующих атак, нацеленных на протоколы маршрутизации в сетях MANET, можно перенести на протоколы маршрутизации в сетях FANET, поскольку сети FANET являются подкатегорией сетей MANET.

***Противодействие атакам на каналы связи***

В литературе предложены различные подходы к обеспечению безопасности при обмене данными с БПЛА. Защита физических свойств канала связи (например, среды передачи, физической топологии и др.) является одним из способов нивелирования атак БПЛА на физическом и MAC-уровне. Учитывая широкое использование БПЛА в различных технологиях беспроводной связи, важно учитывать, что обеспечение безопасности беспроводной связи на физическом и MAC-уровне является сложной задачей из-за характеристик каждой технологии связи (например, категории, частоты, диапазона и др.). Кроме того, алгоритмы шифрования, такие как AES, могут использоваться при обмене данными на физическом уровне и на уровне MAC. Также могут использоваться нелегитимные пользователи [17]. В дополнение к этому одним из лучших способов безопасного обмена данными является обновление микропрограммы устройства и соответствующего программного обеспечения с помощью выпущенных исправлений безопасности. Использование криптографических примитивов, таких как криптография с открытым ключом, гарантирует целостность и конфиденциальность связи БПЛА. В [12] авторы предложили схему безопасной связи для сети БПЛА с использованием метода широковещательного шифрования на основе иерархической идентификации (HIBBE). Предлагаемый подход гарантирует конфиденциальность сообщения и аутентификацию посредством шифрования на основе идентификации. Результаты их анализа производительности показали, что предложенная схема устойчива к DoS-атакам. В другой работе был представлен безопасный протокол связи, основанный на эффективном безсертификационном механизме инкапсуляции ключей подписи (eCLSCTKEM) [18]. Кроме того, протокол является энергоэффективным и соответствует требованиям безопасности и эффективности для связи с БПЛА. Для защиты коммерческих беспилотных летательных аппаратов на основе Wi-Fi в [5] представлена комплексная многоуровневая структура безопасности, которая эффективна против основных атак безопасности, таких как атаки с «отравлением» кэша ARP и атаки DoS. В [10] представлено легковесное аппаратное решение FPGA для защиты связи БПЛА – наземная станция управления коммерческими БПЛА на основе Wi-Fi. Решение содержит криптографический механизм, отвечающий за шифрование данных управления связью. Однако включение подходов на основе криптографии потребует дополнительных вычислений, как в наземной станции управления, так и в БПЛА, и увеличения потребления энергии. Сле-

довательно, эти решения могут снизить производительность связи БПЛА – наземная станция управления. Другие решения для обнаружения вторжений на сетевом уровне основаны на использовании методов анализа пакетов для обеспечения целостности данных и доступности сети БПЛА. В литературе были предложены различные решения безопасности для защиты протоколов маршрутизации MANET от злоумышленников [19; 14]. Эти подходы также могут использоваться в сетях FANET и включают в себя криптографические схемы, такие как аутентификация сообщений, цифровые подписи и хеширование. Существуют также протоколы безопасной маршрутизации для FANET, чтобы гарантировать процесс маршрутизации и надежность при наличии вредоносных узлов. В эту категорию входит использование механизмов безопасности в протоколах маршрутизации. Примеры безопасных протоколов маршрутизации на основе сетей БПЛА: SUANET (безопасная специальная сеть БПЛА), PASER (позиционно зависимая, безопасная и эффективная ячеистая маршрутизация), SUAP (протокол безопасной маршрутизации БПЛА), AODVSEC (Ad hoc On-demand Distance Vector-Secure) и SRPU (протокол безопасной маршрутизации для БПЛА). Каждый из этих протоколов использует определенную стратегию для обеспечения безопасности и конфиденциальности путей маршрутизации. Например, в протоколе SUANET используется стратегия управления ключами между БПЛА для обеспечения конфиденциальности и аутентификации. Напротив, протокол PASER использует криптографические функции для защиты пакетов маршрутизации в сети БПЛА. Протокол маршрутизации SUAP предотвращает лавинную атаку. Протокол маршрутизации AODV-SEC обеспечивает безопасный процесс обнаружения маршрута. Однако реализация безопасных протоколов маршрутизации в реальных сценариях затруднена из-за их сложности и высокой плотности.

***Противодействие атакам на транспортном уровне***

Чтобы предотвратить раскрытие злоумышленником конфиденциальной информации на транспортном уровне, важно реализовать механизмы безопасности, обеспечивающие конфиденциальность и целостность передаваемых данных (например, криптографические протоколы, безопасный обмен ключами и др.). Для нивелирования атак MAVLink один из подходов предлагает архитектуру, которая состоит из восстановления и завершения миссии в полете, несмотря на кибератаку. Существуют и другие подходы для защиты протокола связи MAVLink. В [20] исследователи разделили существующие решения безопасности MAVLink на аппаратные и программные решения. В литературе были разработаны конкретные контрмеры, гарантирующие конфиденциальность, целостность и доступность обмениваемых данных. Эти контрмеры состоят из создания решений IDS, внедрения шифрования с проверкой подлинности для предотвращения атак с целью перехвата, обеспечения многоуровневой структуры безопасности и использования безопасных протоколов маршрутизации. Однако стоит отметить, что упомянутые выше меры противодействия коммуникационным атакам БПЛА имеют некоторые ограничения и недостатки. Например, создание решений IDS для предотвращения DoS-атак влияет на производительность каналов связи. Кроме того, проблемы с задержкой возникают при шифровании данных.

В Таблице 2 обобщены атаки и меры противодействия на телекоммуникационном уровне БПЛА.

*Таблица 2*

**Атаки на каналы связи***

| № п/п | Уровень | Тип атаки | Контрмеры | Ограничения |
|---|---|---|---|---|
| 1 | Сетевой уровень | Подслушивающие атаки | Использование антиподслушивающего алгоритма связи БПЛА [7].<br>Применение аутентифицированного шифрования [8] | Подходы, основанные на криптографии, требуют дополнительных вычисления и могут увеличить потребление энергии |
| 2 | Сетевой уровень | DoS-атаки | Использование решений класса IDS [9] | Влияние на производительность связи БПЛА.<br>IDS на основе сигнатур не справляется со всеми типами атак.<br>IDS на основе аномалий могут страдать от ложных срабатываний |
| 3 | Сетевой уровень | Атаки «человек посередине» | Шифрование данных при их передаче [10].<br>Внедрение методов отпечатков для аутентификации БПЛА [11] | Проблемы с задержкой для критичных ко времени приложений БПЛА |
| 4 | Сетевой уровень | Атаки «подделка» | Включение многоуровневой структуры безопасности [5] | Сложность сети увеличивается в сценарии с несколькими БПЛА |
| 5 | Сетевой уровень | Атаки повторов | Создание безопасной схемы связи (например, шифрование на основе идентификации) [12]<br>Использование механизмов аутентификации [13] | Повторяющиеся запросы могут загрузить сеть<br>и вызвать возможную DoS-атаку |
| 6 | Сетевой уровень | «Черная дыра»<br>«Затопление»<br>атака «Сибил»<br>«Червоточина»<br>«Лишение сна»<br>«Византийская атака»<br>Переадресация | Использование безопасных протоколов маршрутизации [14] | Высокие вычислительные расходы и задержки.<br>Функции безопасности поддерживают не все протоколы маршрутизации |
| 7 | Транспортный уровень | Атаки на протоколы связи | Построение высокоуровневой архитектуры отказоустойчивости и надежности, способной восстановить полетное задание, несмотря на атаку [15].<br>Встраивание сервисов безопасности в аппаратные модули.<br>Использование классических подходов к обеспечению безопасности, таких как методы шифрования и подходы IDS.<br>Использование особенностей новых технологий, таких как блокчейн [16] | Поиск компромиссов между производительностью и безопасностью |

*Заключение*

Анализ угроз программного обеспечения и каналов связи БАС показал необходимость разработки и апробации новых подходов к обеспечению их информационной безопасности. Следует обратить внимание исследователей и специалистов по информационной безопасности на моделирование угроз с учетом их влияния на физические характеристики беспилотного летательного аппарата, быстродействие бортовых подсистем и полетную миссию в целом. По мнению авторов, актуальной также является задача описания цепочки деструктивных действий (Cyber Kill Chain) как одного из самых эффективных подходов к моделированию поведения злоумышленника, именно, для беспилотных авиационных систем.

## Литература / Literature

1. Bansal G., & Sikdar B. (2022, May). Secure and Trusted Attestation Protocol for UAV Fleets. IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Pp. 1–6. IEEE.

2. Paganini P. (2015). A hacker developed Maldrone, the first malware for drones. Securityaffairs (cit. 2020-11-1). URL: https://securityaffairs. co/wordpress/32767/hacking/maldrone-malware-for-drones html (accessed 28.03.2023)

3. Crook J. (2013). Infamous Hacker Creates SkyJack To Hunt, Hack, And Control Other Drones. Tech Crunch.

4. Taylor M., Boubin, J., Chen H., Stewart C., & Qin F. (2021, June). A study on software bugs in unmanned aircraft systems. 2021 International Conference on Unmanned Aircraft Systems (ICUAS), Pp. 1439–1448. IEEE.

5. Hooper M., Tian Y., Zhou R., Cao B., Lauf A. P., Watkins L., ... & Alexis W. (2016, November). Securing commercial WiFi-based UAVs from common security attacks. MILCOM 2016-2016 IEEE Military Communications Conference, Pp. 1213–1218. IEEE.

6. Muzzi F.A.G., de Mello Cardoso P.R., Pigatto D.F., & Branco K.R.L.J.C. (2015, August). Using Botnets to provide security for safety critical embedded systems-a case study focused on UAVs. Journal of Physics: Conference Series, 2015, Vol. 633, No. 1, P. 012053. IOP Publishing.

7. Zhang G., Wu Q., Cui M., & Zhang R. (2017, December). Securing UAV communications via trajectory optimization. In GLOBECOM 2017-2017 IEEE Global Communications Conference, Pp. 1–6. IEEE.

8. Bellare M., & Namprempre C. (2000). Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In Advances in Cryptology - ASIACRYPT 2000: 6th International Conference on the Theory and Application of Cryptology and Information Security Kyoto, Japan, December 3–7, 2000 Proceedings 6, Pp. 531–545. Springer Berlin Heidelberg.

9. Choudhary, G., Sharma, V., You, I., Yim, K., Chen, R., & Cho, J. H. (2018, June). Intrusion detection systems for networked unmanned aerial vehicles: a survey. In 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Pp. 560–565. IEEE.

10. Shoufan, A., AlNoon, H., & Baek, J. (2015). Secure communication in civil drones. In Information Systems Security and Privacy: First International Conference, ICISSP 2015, Angers, France, February 9-11, 2015, Revised Selected Papers 1, Pp. 177–195. Springer International Publishing.

11. Alladi, T., Bansal, G., Chamola, V., & Guizani, M. (2020). SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication. *IEEE Transactions on Vehicular Technology*, *69*(12), 15068-15077.

12. He, S., Wu, Q., Liu, J., Hu, W., Qin, B., & Li, Y. N. (2017). Secure communications in unmanned aerial vehicle network. In Information Security Practice and Experience: 13th International Conference, ISPEC 2017, Melbourne, VIC, Australia, December 13–15, 2017, Proceedings 13 (pp. 601-620). Springer International Publishing.
13. Shafique, A., Mehmood, A., & Elhadef, M. (2021). Survey of security protocols and vulnerabilities in unmanned aerial vehicles. IEEE Access, 9, Pp. 46927–46948.
14. Oubbati, O. S., Atiquzzaman, M., Lorenz, P., Tareque, M. H., & Hossain, M. S. (2019). Routing in flying ad hoc networks: Survey, constraints, and future challenge perspectives. IEEE Access, 7, Pp. 81057–81105.
15. Highnam, K., Angstadt, K., Leach, K., Weimer, W., Paulos, A., & Hurley, P. (2016, June). An uncrewed aerial vehicle attack scenario and trustworthy repair architecture. In 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), Pp. 222–225. IEEE.
16. García-Magariño, I., Lacuesta, R., Rajarajan, M., & Lloret, J. (2019). Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. Ad Hoc Networks, 86, Pp. 72–82.
17. Zhang, J., Duong, T. Q., Woods, R., & Marshall, A. (2017). Securing wireless communications of the internet of things from the physical layer, an overview. Entropy, 19(8), 420.
18. Won, J., Seo, S. H., & Bertino, E. (2015, April). A secure communication protocol for drones and smart objects. In Proceedings of the 10th ACM symposium on information, computer and communications security, Pp. 249–260.
19. Maxa, J. A., Mahmoud, M. S. B., & Larrieu, N. (2017). Survey on UAANET routing protocols and network security challenges. Ad Hoc & Sensor Wireless Networks.
20. Koubâa, A., Allouch, A., Alajlan, M., Javed, Y., Belghith, A., & Khalgui, M. (2019). Micro air vehicle link (mavlink) in a nutshell: A survey. IEEE Access, 7, Pp. 87658–87680.