DOI: 10.18137/RNU.V9187.23.02.P.121 УДК 004.056

А.Р. Кузьмин, М.Ф. Савельев

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СЕНСОРОВ И АППАРАТНОГО ОБЕСПЕЧЕНИЯ КОММЕРЧЕСКИХ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

Аннотация. Использование беспилотных транспортных средств, особенно беспилотных авиационных систем, для решения широкого спектра задач коммерческих и государственных организаций в последние годы интенсифицировалось. Преднамеренное или непреднамеренное искажение данных БАС потенциально может привести к опасным инцидентам техногенного характера с угрозой жизни и здоровью людей. Соответственно, возрастает потребность в обеспечении кибербезопасности таких систем в целом и защиты данных, необходимых для их корректного функционирования, в частности. Традиционные методы обеспечения безопасности не всегда подходят для сенсоров и аппаратного обеспечения систем беспилотного транспорта из-за целого ряда ограничений и особенностей функционирования. Настоящая статья открывает цикл публикаций, посвященных информационной безопасности БАС. Целью настоящей статьи является анализ векторов атак на сенсоры и их каналы, а также изучение аппаратного обеспечения БАС. Проведен обзор методов защиты от подобных атак. В работе применялись методы контент-анализа и эксперименты с коммерческими беспилотными авиационными системами, доступными для гражданских пользователей. В результате был разработан систематизированный перечень атак на сенсоры и аппаратное обеспечение, оформленное в виде таблиц в данной статье.

Ключевые слова: беспилотный летательный аппарат, БПЛА, беспилотные авиационные системы, БАС, киберфизические системы, безопасность аппаратного обеспечения, информационная безопасность, контент-анализ.

A.R. Kuzmin, M.F. Saveliev

ACTUAL CIVILIAN UAS HARDWARE AND SENSORS INFORMATION SECURITY PROBLEMS

Abstract. The use of unmanned vehicles, especially unmanned aerial systems (UAS) for a wide range of tasks of commercial and government organizations has intensified in recent years. Intentional or unintentional distortion of UAS data can potentially lead to dangerous man-made incidents with a threat to human life and health. Accordingly, there is an increasing need for ensuring the cybersecurity of such systems in general and protecting the data necessary for their correct functioning, in particular. Traditional security methods are not always suitable for sensors and hardware of unmanned vehicle systems due to a number of limitations and features of operation. With this article, the authors open a series of articles on UAS information security. The purpose of this article is to analyse attack vectors on sensors and their channels, as well as UAS hardware. 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 sensors and hardware, presented in the form of tables in this article.

Keywords: unmanned aerial systems, UAS, unmanned aerial vehicle, UAV, cyber-physical systems, hardware security, information security, content analysis.

Кузьмин Александр Ростиславович
аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина), Санкт-Петербург. Сфера научных интересов: информационная безопасность киберфизических систем, распределенные реестры, разведка по открытым источникам. Автор пяти опубликованных научных работ. ORCID: 0000-0002-0393-412X. Электронный адрес: alexander.kouzmin@gmail.com

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

Введение

Беспилотные авиационные системы (далее – БАС) являются неотъемлемой частью нашего технологического общества, поскольку их популярность среди гражданских пользователей возрастает с каждым днем. Кроме того, глобальное развитие различных бизнес-моделей применения беспилотных авиационных систем и преимущества, предлагаемые коммерческими БАС, множит и инциденты, связанные с их применением [1]. Таким образом, подчеркивается необходимость эффективного противодействия угрозам БАС.

С этой целью, как и для других киберфизических систем, предлагается обнаружение и идентификация угроз БАС на ранних стадиях. Такой подход предоставит пользователям БАС разумное количество времени для развертывания необходимых инструментов нейтрализации угроз. С точки зрения кибербезопасности БАС уязвимы на разных уровнях. Злоумышленники используют различные уязвимости коммерческих БАС, создавая активную угрозу безопасности людей. Кроме того, производители БАС не учитывают проблемы кибербезопасности на ранних этапах их проектирования и производства.

В своей статье мы рассматриваем БАС как сложные киберфизические системы. Беспилотный летательный аппарат (далее – БПЛА) работает под управлением набора бортовых систем и сенсоров (например, приемник глобальной навигационной спутниковой системы, акселерометр, лидар и др.), которые передают показания на контроллер полета, а он, в свою очередь, отправляет данные по каналу беспроводной связи оператору. В этом сценарии четыре основных компонента БАС: сенсоры, аппаратное обеспечение, программное обеспечение и каналы беспроводной связи, на которых исследуются проблемы безопасности, – должны работать согласованно для поддержания желаемого состояния. Потенциальный отказ одного из компонентов может привести к потере контроля или падению летательного аппарата.

Общая архитектура беспилотных авиационных систем

Развитие технологий привело к появлению БПЛА различных типов, аэродинамической формы и веса. Насколько нам известно, не существует единого стандарта для классификации БПЛА. БАС обычно состоит из беспилотного летательного аппарата, наземной станции управления и линии связи. БПЛА с функционалом автономного выполнения по-

летного задания могут контролироваться оператором через сложный комплекс наземной станции управления либо с помощью пульта дистанционного управления, иногда совмещенного со смартфоном или планшетным компьютером. Компоненты БПЛА:

• контроллер полета – служит центральным процессором БПЛА, который взаимодействует между программным обеспечением и бортовыми устройствами; представляет из себя микроконтроллер, оснащенный вычислительно-управляющим блоком и хранилищем (например, Pixhawk, NVIDIA Jetson, Raspberry Pi и др.);

• аккумуляторы – как правило, литий-полимерные или литий-ионные батареи, обеспечивающие питание бортовых систем БПЛА;

• приводы – состоят из бесщеточных двигателей, реже двигателей внутреннего сгорания, и пропеллеров; могут срабатывать автоматически, без действий оператора, когда необходимо выполнить определенный маневр полетного задания;

• сенсоры – являются важными составляющими частями БПЛА. Они обеспечивают функции обнаружения, предоставляя физические измерения окружающей среды, такие как высота, скорость и геопространственные привязки. Эти измерения преобразуются в данные, которые контроллер полета обрабатывает и передает оператору или принимает самостоятельное решение на их базе;

• модуль беспроводной связи – напрямую подключен к печатной плате контроллера полета и включает в себя передатчик и приемник. Он предназначен для отправки и получения сигналов от других устройств, таких как пульт дистанционного управления, наземная станция управления и близлежащие беспилотные летательные аппараты;

• наземная станция управления – является основным компонентом любой БАС, позволяет дистанционно управлять и контролировать БПЛА во время выполнения полетного задания с помощью беспроводной связи. Аппаратура наземной станции управления представляет собой наземный компьютерный блок обработки, используемый для управления и администрирования полетного задания. Он оснащен модулем беспроводной передачи данных, который генерирует и передает команды управления на БПЛА и получает данные в реальном времени от БПЛА.

Широкое использование БПЛА в гражданских целях порождает большое количество уязвимостей. Следовательно, важно обеспечить целостность информации и защищенный обмен данными между БПЛА и наземной станцией управления, поскольку незащищенный инфообмен может быть источником утечки или искажения информации о полете, такой как данные телеметрии и команды управления. Следовательно, любые коммуникации должны быть защищены и проверены. Это требование можно выполнить с помощью аутентифицированных алгоритмов шифрования. БПЛА должны работать без преднамеренных или непреднамеренных прерываний связи. Все ресурсы, необходимые для выполнения полетного задания, должны быть доступны авторизованным пользователям. Более того, от системы БПЛА требуется противостоять таким атакам, как отказ в обслуживании (DoS), которые ставят под угрозу ее доступность. Такие атаки можно обнаружить с помощью систем обнаружения вторжения (IDS) [2].

Процесс аутентификации является фундаментальным шагом на пути к установлению безопасной связи между различными компонентами системы БПЛА. Он позволяет проверить подлинность и идентичность БПЛА, участвующих в полетном задании. Обеспечивать надежность каждого БПЛА следует посредством аутентификации, и только аутентифицированные БПЛА могут участвовать в полете. Кроме того, аутентификация защи-

щает сеть БПЛА от злоумышленников, подменяющих легитимные узлы. Также система БПЛА должна применять соответствующие механизмы, например, цифровую подпись обмениваемых сообщений. Обмен данными в системе БПЛА должен осуществляться только авторизованными пользователями.

В дополнение к вышеперечисленным требованиям безопасности следует отметить требование по неразглашению информации для систем БПЛА. Действительно, конфиденциальная информация, которой обмениваются наземная станция управления и БПЛА, например, захваченные с помощью БПЛА изображения и видеоматериалы, не должна раскрываться третьей стороне.

Уязвимости и атаки

Опишем проблемы обеспечения целостности и безопасности БПЛА на двух из четырех уровней – уровне сенсоров и аппаратном уровне. Как показано на Рисунке 1, мы разбиваем БАС на четыре уровня. Наша задача в этой и последующих статьях – предоставить подробный обзор угроз и уязвимостей, нацеленных на безопасность и целостность систем БПЛА для каждого из уровней. Также мы опишем атаки и существующие меры противодействия им с привязкой к одному из уровней.

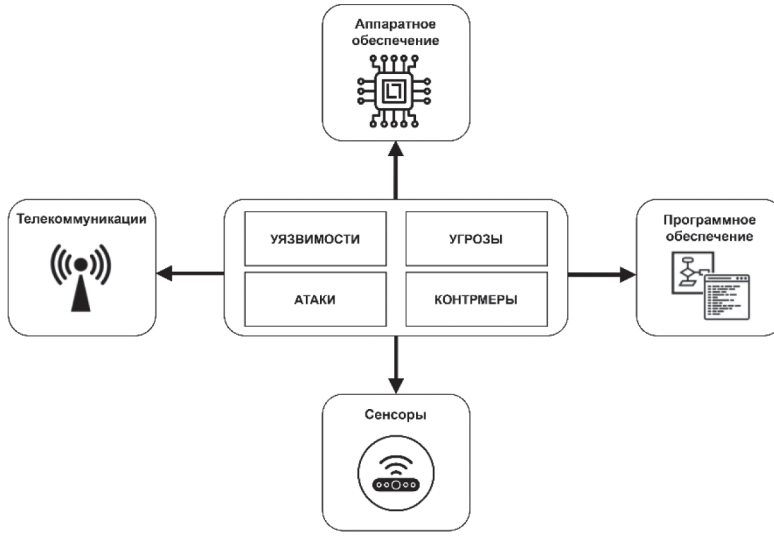

Рисунок 1. Информационная безопасность БАС
Источник: здесь и далее рисунки и таблицы составлены авторами.

Уровень сенсоров

Гражданские сигналы спутниковой навигационной системы не шифруются и не аутентифицируются. Таким образом, злоумышленник может использовать эту уязвимость, имитируя сигнал GPS/GLONASS, чтобы ввести оператора БПЛА в заблуждение. С точки зрения злоумышленника использование данных бортовых сенсоров в режиме реального времени может привести к сбоям в работе системы БПЛА; подобное может произойти из-за того, что полетный контроллер не оценивает достоверность показаний сенсоров. Внедрение уязвимостей сенсоров в систему БПЛА также может осуществляться через вредоносное программное обеспечение. Из-за практичности атак по каналам сенсоров

в реальных сценариях этот класс уязвимостей открывает новый вектор атаки для злоумышленника, позволяющий полностью контролировать коммерческие БПЛА [3; 4].

Уязвимости сенсоров

Атаки на основе сенсоров включают глушение данных геолокации, ввод ложных данных на сенсоры и атаки по сенсорным каналам. Атака с полным глушением данных GPS/GLONASS происходит, когда злоумышленник блокирует подачу навигационных сигналов, переводя БПЛА в режим дезориентации. Выполнение таких атак приводит к потере контроля над БПЛА и даже к возможному перехвату управления и угону БПЛА.

Ввод ложных данных сенсора

Введение ложных показаний сенсоров в полетный контроллер может поставить под угрозу внешние сенсоры, такие как электрооптические и инфракрасные [5]. Такая атака приводит к срыву стабилизации БПЛА. Злоумышленник может ввести ложные данные сенсоров в БПЛА, получив доступ к бортовой системе полетного контролера или изменив показания сенсоров с помощью системных вызовов. В противном случае он может напрямую передавать ложные сигналы на сенсоры, а значит, скомпрометировать БПЛА в момент полета. Известным примером атак с использованием ложных данных сенсоров является спуфинг GPS. Поскольку широковещательные сигналы GPS в большинстве случаев не зашифрованы и не аутентифицированы, злоумышленник выполняет спуфинговую атаку на GPS, подделывая сгенерированный сигнал, что в конечном счете может изменить показания GPS-приемника БПЛА. В [6; 7] авторы демонстрируют спуфинговую атаку GPS на БПЛА. Атака с подменой GPS заставляет дрон отвечать на поддельные сигналы, что влияет на его навигационную систему.

Атаки на каналы сенсоров

БПЛА используют набор сенсоров, в которых сенсорные каналы (например, инфракрасные, акустические, световые и др.) служат вектором для атак. В [8] авторы демонстрируют, что БПЛА, оснащенные гироскопами микроэлектромеханических систем (далее – МЭМС), могут вывести системы БПЛА из строя из-за преднамеренного звукового шума. Исследования показывают, что МЭМС-гироскопы резонируют на слышимых частотах, а также сенсоры камеры оптического потока, которые используются для стабилизации БПЛА, могут быть скомпрометированы воздействием окружающей среды [9].

Противодействие атакам, основанным на эксплуатации сенсоров

Чтобы нивелировать атаки, создающие помехи GPS, авторы в [10] предложили использовать дополнительные сенсоры в качестве альтернативного навигационного решения, когда сигналы GPS недоступны, например, визуальный сенсор монокулярной камеры в сочетании с сенсором блока инерциальных измерений. Существуют подходы, основанные на системах обнаружения вторжений с использованием машинного обучения для обнаружения как известных, так и неизвестных атак на основе сенсоров [11]. Эти решения собирают наборы обучающих данных с бортовых компонентов БПЛА, таких как журналы полетов и показания сенсоров. Однако реализация подобных систем в реальных условиях затруднена из-за ограниченных энергетических и вычислительных ресурсов БПЛА. Перспективными выглядят подходы для обнаружения внешних сенсорных атак, основанные на моделировании физических свойств БПЛА с помощью инвариантного подхода к управлению. Инвариантный подход к управлению проверяет соответствие физического состояния БПЛА его ожидаемому состоянию, которое идентифицируется его моделью

управления. В [12] авторы представили архитектуру для защиты показаний сенсоров при наличии физических инвариантов. Физические инварианты БПЛА – это уникальные характеристики, которые можно моделировать для прогнозирования измерений сенсоров в соответствии с их поведением. Эти функции состоят из нелинейных дифференциальных уравнений, которые моделируют скорость, углы, положение и угловую скорость БПЛА.

Предотвратить атаку спуфинга GPS возможно путем обнаружения необычных изменений мощности сигнала, что указывает на начало атаки спуфинга. В сценариях с несколькими БПЛА авторы в [13] предложили совместный подход к аттестации данных, который проверяет правильность совместно используемой информации, такой как GPS-координаты, что позволяет обнаруживать атаки с подменой GPS. Еще одна мера противодействия атакам спуфинга GPS заключается в применении схем аутентификации сигналов GPS с классическими криптографическими подходами. Необходимо отметить, что реализация таких решений требует дополнительных изменений в инфраструктуре спутника. Существуют методы защиты от спуфинга GPS с реализацией в полетном контроллере БПЛА, обеспечивающие эффективное противодействие попыткам угона БПЛА [14]. В литературе был предложен набор контрмер для нивелирования каждого типа сенсорных атак. Акустические сенсорные каналы могут быть защищены физической изоляцией, которая экранирует звуковой шум [8]. Создание надежных алгоритмов оптического потока, таких как алгоритм RANSAC [15], представляет собой механизм глубокоэшелонированной защиты от спуфинга оптического потока сенсоров. Возможности злоумышленника по компрометации сенсоров БПЛА представлены в Таблице 1.

Таблица 1

Атаки на уровне сенсоров*

№ п/п	Тип атаки	Контрмеры	Ограничения
1	Атаки на сенсорные каналы	Физическая изоляция акустических сенсорных каналов для защиты от звукового шума [16]. Создание надежных алгоритмов оптического потока для оптических сенсоров потока [17]	Большое количество сенсорных каналов для рассмотрения
2	Подмена данных GPS	Использование подхода совместной аттестации данных, который проверяет правильность GPS-координат [13]. Принятие аутентифицированных схем для GPS сигналов. Обнаружение необычных изменений мощности сигнала, которые указывают на начало атаки спуфинга. Внедрение методов защиты от спуфинга GPS [18]	Аутентифицированные сигналы GPS требуют дополнительных изменений в инфраструктуре спутника
3	Глушение GPS-сигнала	Включение автономной навигации без сигнала GPS. Использование дополнительных сенсоров для альтернативной навигации [10]. Внедрение IDS на основе машинного обучения для обнаружения сенсорных атак [11]	Ограниченные возможности энергии и вычислений для практической реализации
4	Ввод ложных данных сенсоров	Моделирование физических свойств БПЛА [19]. Защита показаний сенсоров при наличии физических инвариантов [12]. Перекрестная проверка данных путем сбора показаний сенсоров с альтернативного набора сенсоров [10]	Адаптация существующих решений к многим типам бортовых сенсоров пока невозможно

Окончание Таблицы 1

5	Атаки на МЭМС-гироскопы	Физическая изоляция акустических сенсорных каналов для защиты от звукового шума [16]	Физическая изоляция может повысить температуру и вызвать неисправность БПЛА
6	Атака на сенсоры камеры оптического потока	Создание надежных алгоритмов оптического потока для оптических сенсоров потока [2]	Практические пределы оценки оптического потока из-за шума

Исходя из анализа результатов исследований, можно сделать вывод, что предложенные методы предотвращения атак на сенсоры и их каналы существенно увеличивают вычислительные затраты бортовых систем БПЛА, а интеграция набора альтернативных сенсоров для каждого сенсорного канала неэффективна и затратна.

Аппаратный уровень

Злоумышленники рассматривают БПЛА как потенциальное средство для проведения атак на физические объекты. Аппаратные компоненты системы БПЛА в общем случае состоят из бортового контроллера полета и наземной станции управления. Оба аппаратных устройства подвержены угрозам информационной безопасности, которые потенциально могут привести к кибер- или даже физическим атакам.

Уязвимости аппаратного обеспечения

К атакам аппаратного уровня относятся аппаратные трояны, преднамеренные и непреднамеренные сбои аппаратной части БПЛА. Аппаратные трояны включают в себя модификации электронного оборудования (например, вмешательство в аппаратную схему, изменение размера логического элемента и др.). В частности, аппаратные трояны нацелены на полетный контроллер, что делает систему БПЛА уязвимой для нескольких атак. Аппаратные трояны злонамеренно внедряются ненадежной третьей стороной в цепочку поставок полупроводников полетного контроллера. Злоумышленник использует эти модификации для компрометации функциональных возможностей и функций безопасности интегральной схемы (например, снижение скорости вращения винтов, утечка криптографических ключей контроллера полета и тому подобное). Так, например, троян был обнаружен в чипе Actel ProASIC самолета Boeing 787 [20]. Бэкдор позволял злоумышленнику контролировать систему авионики и управлять самолетом, тем самым ставя под угрозу безопасность пассажиров на борту. Во время полетной миссии, которая требует взаимодействия между несколькими БПЛА, могут произойти физические столкновения, что приведет к их падению.

Для предотвращения таких столкновений в гражданском воздушном пространстве БПЛА в значительной степени полагаются на системы предотвращения столкновений. Однако эти системы не включают в себя встроенные функции безопасности и не могут устранить угрозу предотвращения столкновений, создаваемую злоумышленниками. У БПЛА могут возникнуть сбои в работе их аппаратных компонентов, такие как срок службы батареи или проблемы с двигателями. Эти технические сбои представляют угрозу для выполнения полетной задачи и могут привести к небезопасной посадке БПЛА в неожиданном месте. В этом случае, если БПЛА хранят незашифрованные данные, злоумышленник может раскрыть конфиденциальную информацию, связанную с миссией, и нарушить конфиденциальность полетного задания. Помимо прочего, к аппаратным проблемам можно отнести проблемы с летными навыками оператора.

Атаки на аппаратное обеспечение

К аппаратным атакам относятся взлом, атаки на цепочку поставок, атаки на батареи и атаки на радиочастотные модули. Из-за особенностей БПЛА они видны на малой высоте, что делает их идеальными целями для угона. Злоумышленник может совершить угон летящего БПЛА либо напрямую, либо удаленно через вредоносное программное обеспечение. Самый простой способ вывести из строя и угнать БПЛА – использовать специальные электромагнитные ружья направленного действия. Обычно они находятся в распоряжении правоохранительных органов для защиты объектов в зонах ограниченного полета. Однако злоумышленник тоже может использовать подобное ружье для посадки БПЛА и его захвата.

С ростом индустрии БПЛА у злоумышленников появляется более широкое поле для компрометации БПЛА с помощью атак на цепочку поставок. Этот тип атаки состоит в использовании уязвимостей в процессе цепочки поставок организаций путем нацеливания на менее безопасные и чувствительные компоненты, такие как пропеллеры, планеры, приводы, программное обеспечение и микросхемы. Следовательно, конечный продукт, который доставляется покупателю, может быть уже скомпрометирован.

Группа исследователей продемонстрировала практическую атаку на цепочки поставок против БПЛА [21]. Они провели физическую атаку на цепочки поставок для БПЛА с помощью аддитивного производства. Атака состояла из саботажа путем удаленного манипулирования файлами конструкции пропеллеров. Злоумышленники снизили коэффициент усталости напечатанного на 3D-принтере винта и создали отложенные повреждения винтов во время полета. Это исследование показывает, что обнаружение атак саботажа для систем аддитивного производства остается сложной исследовательской проблемой.

Большинство современных БПЛА используют в качестве элементов питания литий-ионные аккумуляторы. Эти батареи поддерживаются системой управления батареями для обеспечения надежного питания различных компонентов системы БПЛА. Однако злоумышленник может исчерпать энергию батареи, выполнив потенциальные атаки разрядки батареи [22], что приведет к сбоям в работе системы БПЛА и, следовательно, поставит под угрозу доступность и целостность батарей. Злоумышленник ставит под угрозу доступность батарей БПЛА, физически вмешиваясь или заменяя подлинные батареи неисправными, чтобы вывести из строя систему бортового питания БПЛА. Также существует тип атаки, при которой злоумышленник генерирует глубокую разрядку аккумуляторов. Этот тип атаки может произойти путем компрометации других компонентов БПЛА, таких как подмена сенсоров или внедрение вредоносного программного обеспечения, что приводит к разрядке батарей БПЛА [23].

Атаки на радиочастотные модули связи

Радиочастотные модули используются для передачи и приема радиосигналов от двух разных устройств. В контексте БПЛА оператор может использовать обычный пульт дистанционного управления или наземную станцию управления для отправки управляющих сигналов летящим БПЛА. В этом случае злоумышленник может заглушить сигналы управления и вывести из строя связь БПЛА-наземная станция управления.

Противодействие атакам на аппаратное обеспечение

Учитывая физическую уязвимость и актуальные угрозы БПЛА, следует рассмотреть и усовершенствовать подходы к физической защите для устранения атак на аппаратном

уровне БПЛА. Возможное противодействие аппаратным троянам состоит в создании системы обнаружения вторжения на основе машинного обучения для обнаружения подобных аппаратных атак. Обнаружение фальсифицированных данных или команд с помощью решений системы обнаружения вторжения достигается за счет: 1) изучения модели на основе средних данных, генерируемых сигналами широтно-импульсной модуляции (далее – ШИМ), которые обычно используются в интегральных схемах БПЛА; 2) обучения модели на вредоносных данных, которые генерируются компрометацией прошивки или внедрением аппаратных троянов через воздействия на ШИМ-сигналы.

Другой метод противодействия аппаратным троянам состоит в выполнении детального анализа схемы, позволяющего обнаруживать аппаратные нестыковки или избыточность [24]. Защита как наземной станции управления, так и БПЛА от несанкционированного доступа с использованием шифрования с проверкой подлинности и защиты от вредоносного программного обеспечения значительно снизит вероятность захвата и угона летящего БПЛА злоумышленниками. Кроме того, изменение траектории полета может помешать злоумышленнику идентифицировать схему полета, что сделает цель более сложной для физической кражи. В [25] авторы предложили метод обнаружения угона БПЛА, основанный на статистическом анализе стандартных схем полета. Моделирование различных сценариев угона показывает эффективность алгоритма их обнаружения. Однако данный алгоритм дает сбой при изменении параметров моделирования, таких как нестабильность управления, что мотивирует на дальнейшее тестирование и улучшение качества моделирования. Атаки на цепочку поставок можно нивелировать, управляя безопасностью в процессе производства, чтобы избежать использования скомпрометированных компонентов БПЛА. Кроме того, решения по защите от несанкционированного доступа (например, микропроцессоры с защитой от несанкционированного доступа, программное обеспечение для защиты от несанкционированного доступа и др.) предотвратят несанкционированные физические или логические модификации, которые могут нарушить подлинность критически важных компонентов БПЛА. Существующие меры противодействия атакам разрядки батареи включают использование цепей безосного электропитания в системе управления батареями, которые обеспечивают физическую защиту батарей БПЛА. Предполетная диагностика батарей БПЛА является вынужденной процедурой, гарантирующей безопасный полет. Необходимо использовать криптографические решения для защиты канала связи «БПЛА – наземная станция управления». Чтобы нивелировать атаки на радиочастотные модули производители, могут внедрить встроенное шифрование на уровне электронного чипа.

Как указано в Таблице 2, существующие атаки на БПЛА на аппаратном уровне включают в себя атаки на цепочку поставок, атаки с разрядкой батареи, использование методов захвата и атаки на радиочастотные модули.

Таблица 2

Атаки на аппаратном уровне*

№ п/п	Тип атаки	Контрмеры	Ограничения
1	Аппаратные трояны	Создание IDS на основе машинного обучения для обнаружения аппаратных троянов [26]. Анализ компонентной интегральной схемы [24]	Методы аппаратного запутывания могут обойти существующие методы обнаружения
2	Аппаратные сбои	Применение криптографических методов для БПЛА в целях предотвращения захвата хранимых данных в случае аппаратных сбоев и падения БПЛА [27]	Шифрование данных может помешать криминалистам восстановить доказательства аппаратных сбоев
3	Угон БПЛА	Защита наземной станции управления и БПЛА от несанкционированного доступа с помощью шифрования процесса аутентификации [28]. Последовательное изменение траектории полета, чтобы избежать трекинга схемы полета злоумышленником [25]	Использование легальных технологий противодействия БПЛА для захвата легитимных БПЛА
4	Атаки на цепочки поставок	Внедрение устройств с защитой от несанкционированного доступа [29]. Управление безопасностью цепочки поставок во время производственного процесса [21]	Возможны внутренние атаки в процессе производства
5	Атаки разряда батареи питания	Использование цепей безопасности электропитания в системе управления батареями [23] Предполетная диагностика аккумуляторов БПЛА. Мониторинг процесса разрядки аккумулятора в режиме реального времени [22]	При неаутентифицированных коммуникациях злоумышленник может отображать ложный уровень заряда батареи для оператора
6	Атаки на радиочастотные модули	Шифрование канала радиоуправления [30]. Бортовое шифрование полетного контроллера	Встроенное шифрование снижает пропускную способность и увеличивает время обработки

Стоит учитывать, что существующие меры противодействия аппаратным атакам имеют свои ограничения. Например, аппаратные методы запутывания могут затруднить детальный анализ схемы, встроенное шифрование в радиочастотных модулях уменьшает пропускную способность и влияет на быстродействие микропроцессоров [31].

Заключение

Проанализированы проблемы безопасности БАС на двух уровнях из четырех – сенсорном и аппаратном. Кроме того, обсуждены вопросы угроз и возможные решения по противодействию атакам БПЛА на данных уровнях. С увеличением числа коммерческих БПЛА в гражданском воздушном пространстве вопросы безопасности и целостности данных беспилотных транспортных систем стали весьма актуальны, поэтому промышленность, академические круги и правоохранительные органы должны сотрудничать и разрабатывать новые стандарты и правила обеспечения их безопасности. Анализ уяз-

вимостей и атак на БПЛА показал, что такие направления информационной безопасности БАС, как форензика, разработка систем обнаружения вторжений уровня сенсоров, безопасные помехоустойчивые коммуникации и защита данных, являются чрезвычайно актуальными.

Литература / References

1. AARONIA Drone Incidents World Map. *Aartos Drone Detection.* URL: https://drone-detection-system.com/drone-incidents/ (accessed 28.03.2023).

2. Choudhary G., Sharma V., You I., Yim K., Chen R., Cho J.H. (2018). Intrusion detection systems for networked unmanned aerial vehicles: A survey. In: *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. Limassol, Cyprus, 25–29 June 2018. Pp. 560–565. DOI: 10.1109/IWCMC.2018.8450305

3. Uluagac A.S., Subramanian V., Beyah R. (2014). Sensory channel threats to cyber physical systems: A wake-up call. In: *2014 IEEE Conference on Communications and Network Security*. San Francisco, CA, USA, 29–31 October 2014. Pp. 301–309. DOI: 10.1109/CNS.2014.6997498

4. Sikder A.K., Petracca G., Aksu H., Jaeger T., Uluagac A.S. (2021). A survey on sensor-based threats and attacks to smart devices and applications. In: *IEEE Communications Surveys & Tutorials*. 08 March 2021. Vol. 23. No. 2. Pp. 1125–1159. DOI: 10.1109/COMST.2021.3064507

5. Vasconcelos G., Carrijo G., Miani R., Souza J., Guizilini V. (2016). The impact of DoS attacks on the AR. Drone 2.0. In: *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR)*. Recife, Brazil, 08–12 October 2016. Pp. 127–132. DOI: 10.1109/LARS-SBR.2016.28

6. Kerns A.J., Shepard D.P., Bhatti J.A., Humphreys T.E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*. Vol. 31. No. 4. Pp. 617–636. DOI: 10.1002/rob.21513

7. Seo S.H., Lee B.H., Im S.H., Jee G.I. (2015). Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. *Journal of Positioning, Navigation, and Timing*. Vol. 4. No. 2. Pp. 57–65. DOI: 10.11003/jpnt.2015.4.2.057

8. Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, Yongdae Kim (2015). Rocking drones with intentional sound noise on gyroscopic sensors. In: *Proceedings of the 24th USENIX Security Symposium*. Washington, D.C., 12–14 August 2015. Pp. 881–896. ISBN 978-1-939133-11-3.

9. Davidson D., Wu H., Jellinek R., Singh V., Ristenpart T. (2016). Controlling UAVs with Sensor Input Spoofing Attacks. In: *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. Vol. 4. URL: https://www.usenix.org/system/files/conference/woot16/woot16-paper-davidson.pdf (accessed 22.03.2023).

10. Wu A.D., Johnson E.N., Kaess M., Dellaert F., Chowdhary G. (2013). Autonomous flight in GPS-denied environments using monocular vision and inertial sensors. *Journal of Aerospace Information Systems*. Vol. 10. No. 4. Pp. 172–186. DOI: 10.2514/1.I010023

11. Arthur M.P. (2019). Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS. In: *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*. Beijing, China, 28–31 August 2019, Pp. 1–5, DOI: 10.1109/CITS.2019.8862148

12. Quinonez R., Giraldo J., Salazar L., Bauman E., Cardenas A., Lin Z. (2020). SAVIOR: Securing autonomous vehicles with robust physical invariants. In: *Proceedings of the 29th USENIX Security Symposium*. 12–14 August 2020. Pp. 895–912. URL: https://www.usenix.org/system/files/sec20-quinonez.pdf (accessed 22.03.2023).

13. Abera T., Bahmani R., Brasser F., Ibrahim A., Sadeghi A.R., Schunter M. (2019). DIAT: Data Integrity Attestation for Resilient Collaboration of Autonomous Systems. In: *2019 Network and Distributed Systems Security (NDSS) Symposium*, San Diego, CA, USA, 24–27 February 2019. DOI: https://dx.doi.org/10.14722/ndss.2019.23420
14. Ameur A.I., Lakas A., Bachir Y.M., Oubbati O.S. (2022). Peer-to-peer overlay techniques for vehicular ad hoc networks: Survey and challenges. *Vehicular Communications*. Vol. 34. Art. no. 100455. DOI: 10.1016/j.vehcom.2022.100455
15. Guo K., Ye H., Gao X., Chen H. (2022). An Accurate and Robust Method for Absolute Pose Estimation with UAV Using RANSAC. *Sensors*. Vol. 22. No. 15. Art. no. 5925. DOI: 10.3390/s22155925
16. Roth G. (2009) *Simulation of the effects of acoustic noise on mems gyroscopes:* Doctoral dissertation. Auburn University. Auburn, Alabama August 10, 2009. URL: https://etd.auburn.edu/bitstream/handle/10415/1773/Grant_Roth_Thesis_Final.pdf?sequence=1 (accessed 22.03.2023).
17. Szeliski R. (2022) *Computer vision: Algorithms and applications*. Springer Cham. 925 p. DOI: 10.1007/978-3-030-34372-9
18. Feng Z., Guan N., Lv M., Liu W., Deng Q., Liu X., Yi W. (2018) An efficient UAV hijacking detection method using onboard inertial measurement unit. *ACM Transactions on Embedded Computing Systems (TECS)*. Vol. 17. No. 6. Pp. 1–19. DOI: 10.1145/3289390
19. Choi H., Lee W.C., Aafer Y., Fei F., Tu Z., Zhang T., Xu D., Deng X. (2018) Detecting attacks against robotic vehicles: A control invariant approach. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications* Security (CCS '18), 15–19 October 2018, Toronto, ON, Canada. ACM, New York, NY, USA. DOI: 10.1145/3243734.3243752
20. Hassan M., Große D., Drechsler R. (2022) Digital Early Security Validation. In: *Enhanced Virtual Prototyping for Heterogeneous Systems*. Cham : Springer International Publishing. Pp. 123–154. DOI: 10.1007/978-3-031-05574-4_6
21. Belikovetsky S., Yampolskiy M., Toh J., Gatlin J., Elovici Y. (2017) dr0wned-Cyber-Physical Attack with Additive Manufacturing. In: *11th USENIX Workshop on Offensive Technologies (WOOT 17),* Vancouver, BC, Canada, 14–15 August 2017. URL: https://www.usenix.org/system/files/conference/woot17/woot17-paper-belikovetsky.pdf (accessed 22.03.2023).
22. Desnitsky V., Kotenko I. (2021) Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures. *Simulation Modelling Practice and Theory*. Vol. 107. Art. no. 102244. EDN CHUKBY. DOI: 10.1016/j.simpat.2020.102244
23. Tlili F., Fourati L.C., Ayed S., Ouni B. (2022) Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures. *Ad Hoc Networks*. Vol. 129. Art. no. 102805. DOI: 10.1016/j.adhoc.2022.102805102805
24. Nigh C., Orailoglu A. (2021) AdaTrust: Combinational hardware trojan detection through adaptive test pattern construction. In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*. Vol. 29. No. 3. Pp. 544–557. DOI: 10.1109/TVLSI.2021.3053553
25. McNeely J., Hatfield M., Hasan A., Jahan N. (2016) Detection of UAV hijacking and malfunctions via variations in flight data statistics. In: *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*. Orlando, FL, USA, 24–27 October 2016. Pp. 1–8. DOI: 10.1109/CCST.2016.7815713
26. Rahman M.A., Rahman T., Kisacikoglu M., Akkaya K. (2020). Intrusion detection systems-enabled power electronics for unmanned aerial vehicles. In: *2020 IEEE CyberPELS (CyberPELS)*, Miami, FL, USA, 13–13 October 2020. Pp. 1–5. DOI: 10.1109/CyberPELS49534.2020.9311545

27. Shafique A., Mehmood A., Elhadef M. (2021). Survey of security protocols and vulnerabilities in unmanned aerial vehicles. In: *IEEE Access*. Vol. 9. Pp. 46927–46948. DOI: 10.1109/ACCESS.2021.3066778
28. Pu C., Li Y. (2020). Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system. In: *2020 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN 2020)*. Orlando, FL, USA, 13–15 July 2020, Pp. 1–6. DOI: 10.1109/LANMAN49260.2020.9153239
29. Williams Z., Lueg J.E., LeMay S.A. (2008) Supply chain security: an overview and research agenda. *The International Journal of Logistics Management*. Vol. 19. No. 2. Pp. 254–281. DOI: 10.1108/09574090810895988
30. Chen L., Qian S., Lim M., Wang S. (2018). An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems. *China communications*. Vol. 15. No. 5. Pp. 61–76. DOI: 10.1109/CC.2018.8387987
31. Yarza I., Agirre I., Mugarza I., Cerrolaza J.P. (2022) Safety and security collaborative analysis framework for high-performance embedded computing devices. *Microprocessors and Microsystems*. Vol. 93. Art. no. 104572. DOI: 10.1016/j.micpro.2022.104572