УДК 004.056: 004.73 **DOI** 10.15622/ia.21.6.8

Е.С. Басан, О.Ю. Пескова, О.И. Силин, А.С. Басан, Е.С. Абрамов

ГЕНЕРАЦИЯ ДАННЫХ ДЛЯ МОДЕЛИРОВАНИЯ АТАК НА БПЛА С ЦЕЛЬЮ ТЕСТИРОВАНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Басан Е.С., Пескова О.Ю., Силин О.И., Басан А.С., Абрамов Е.С. **Генерация данных для моделирования атак на БПЛА с целью тестирования систем обнаружения вторжений.**

Аннотация. На сегодняшний день вопросы, связанные с обеспечением безопасности БПЛА, весьма актуальны. Исследователям необходимо разрабатывать новые методы защиты для своевременного обнаружения атаки и реализации мер по смягчению ее последствий. В работе авторы предлагают новую концепцию обнаружения атак «изнутри» БПЛА. Идея состоит в анализе киберфизических параметров БПЛА, которые могут указывать на атаку и ее возможные последствия. Было определено, что для обнаружения атаки и определения последствий, к которым она может привести, необходимо контролировать не только исходные параметры, но и внутренние киберфизические параметры БПЛА. Это позволит спрогнозировать возможные последствия нападения и принять экстренные меры. Проработана схема влияния атаки на БПЛА и взаимосвязь с инцидентами безопасности, построенная с использованием онтологического подхода. Рассмотрены две основные сущности БПЛА - физические и цифровые аспекты БПЛА. Также показаны примеры цепочек атак, приводящие к различным последствиям. В обзорной части выполнен анализ методов и алгоритмов обнаружения спуфинговых атак с использованием генераторов данных, на основании которого сделаны выводы об их достоинствах и недостатках. Далее, на основании проведенных экспериментов, авторы предлагают метод оценки качества данных и метод генерации аномальных наборов данных, похожих на реальные данные об атаках, которые могут применяться для разработки и тестирования методов обнаружения и блокирования атак. Описана архитектура экспериментального стенда, который был использован в рамках натурного моделирования. На данном стенде, предназначенном для разбора атак с подменой GPS (GPS-спуфинг), проходила отработка нескольких сценариев нормального полета, а затем нескольких сценариев атаки. По результатам проведенных экспериментов был предложен метод, позволяющий имитировать данные, соответствующие атаке, с требуемой точностью. Также был предложен метод оценки качества сгенерированных данных.

Ключевые слова: анализ данных, статистика, атаки, риски, БПЛА.

1. Введение. Атаки на БПЛА и их последствия. Успешно проведенная активная атака на БПЛА может привести к негативным и даже катастрофическим последствиям. При этом важно установить связи между атакой, последствиями атаки и признаками атаки. Установление взаимосвязи между последствиями атак и непосредственно атаками может помочь получить признаки атаки, определить изменения, которые становятся предпосылками атаки, и выделить изменения, приводящие к ее успешному осуществлению [1]. Зачастую атака может быть осуществлена, но с недостаточной степенью интенсивности, благодаря чему не приведет к негативным

последствиям для кибер-физической системы, к которой можно отнести БПЛА.

Если рассматривать БПЛА как кибер-физическую систему, то последствия атак могут быть направлены как на физическую (или аппаратную) базу, так и на цифровую (кибернетическую) компоненту, то есть непосредственно на данные, информацию. Исследования по классификации типов атак и их последствий для БПЛА ведутся давно. Например, в публикациях авторов [2] выделяют пять основных типов атак: Прослушивание (Eavesdropping), Зашумление (Jamming), Внедрение сообщений (Message injection), Удаление сообщений (Message deletion), Модификация сообщений (Message modification). Эти атаки могут затрагивать как цифровые, так и физические компоненты БПЛА.

Рассмотрим рисунок 1, на котором показаны связи между атаками, физической и кибернетической частями БПЛА, а также последствиями атак. Разумеется, на этом рисунке представлены не все наборы возможных последствий атак, а только их общая структура [3]. Тем не менее, эта схема ясно показывает, что практически любая атака, реализованная должным образом, может привести к катастрофическим последствиям не только для самого БПЛА, но и для человека и окружающей среды [4].

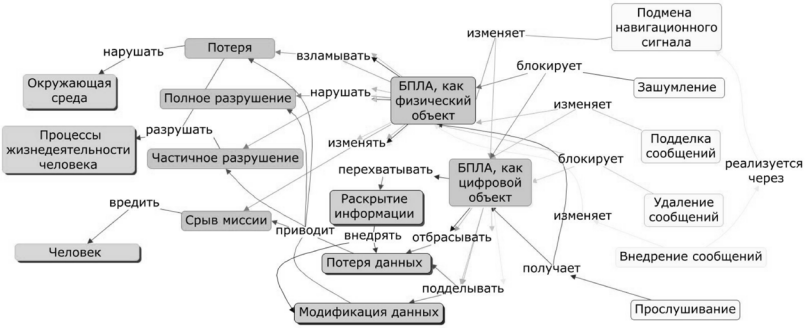


Рис. 1. Схема влияния атаки на БПЛА и взаимосвязь с инцидентами безопасности

Схема, представленная на рисунке 1, построена с применением онтологического подхода. В центре рисунка представлены две основные сущности БПЛА – физические и цифровые аспекты БПЛА. Эти две сущности представляют собой основные концепты онтологии, они представлены серым квадратом, и на них влияют различные атаки.

К цифровым аспектам БПЛА («БПЛА как цифровой объект») можно отнести информацию и данные, которые использует БПЛА в своей работе. Они могут храниться в виде файлов в памяти БПЛА, данных в оперативной памяти, а также передаваться по сети с помощью сетевых протоколов, каналов передачи данных.

К физическому аспекту БПЛА («БПЛА как физический объект») относится аппаратное обеспечение и конструкция БПЛА в целом, включая модули навигации и связи, платы управления, полетный контроллер.

Справа от основных аспектов БПЛА перечислены основные типы атак, которые могут проводиться на БПЛА (от подмены навигационного сигнала до прослушивания). Атаки обозначены светло-серыми прямоугольниками, как другие концепты онтологии. В целом, каждый концепт онтологии отличается друг от друга и представлен разным форматом. Между концептами существуют связи. Связи между концептами описываются действиями. Стрелки и действия связывают между собой концепты. Стрелки на рисунке отличаются, так как они должны позволить определить то, какая атака приводит к какому последствию, чтобы в дальнейшем оценить риски.

Последствия обозначены темно-серыми прямоугольниками, так как эти концепты отличаются от остальных. Это те последствия, которые связаны с физическим воздействием на БПЛА. Светло-серыми прямоугольниками обозначены те последствия, которые связаны с цифровым миром. При этом, как видно из схемы, последствия в самом деле пересекаются и одни последствия могут быть вызваны другими.

В целом, несмотря на то, что на рисунке приведено шесть различных типов атак, их можно объединить в два типа: атаки на нарушение доступности и атаки на получение доступа. К атакам на нарушение доступности относятся Зашумление, Удаление сообщений. Они напрямую могут заблокировать канал связи для БПЛА. При этом косвенно и другие атаки могут с физической точки зрения влиять на БПЛА. К примеру, атаки «Подделка сообщений», «Внедрение сообщений», относящиеся к типу атак на получение доступа, могут привести к тому, что БПЛА будет управляться не легитимным оператором, а злоумышленником. В результате перехвата управления злоумышленником БПЛА может упасть и разбиться, из-за чего станет недоступным.

Как видно из рисунка, по факту разные атаки в итоге могут привести к одним и тем же последствиям. Это связано с тем, что исполнение атаки может отличаться, и в зависимости от цели и

возможностей нарушителя последствия могут варьироваться от изменения направления полета БПЛА до его полного разрушения.

Среди приведенных выше атак выделена атака «Подмена навигационного сигнала». Эта атака выделена отдельно, потому что для ее реализации не нужно производить дополнительных разведывательных действий. Нужно обладать только специальным оборудованием для генерации поддельного сигнала. В случае с GPS сигналом, который распространяется свободно, нужно только иметь мощную антенну и правильно подделать координаты в зависимости от местоположения БПЛА. При этом последствиями для БПЛА от данной атаки могут быть, как угон, так и падение.

Приведем простой пример цепочки атак, которые приводят к одному возможному варианту последствий. Сценарий, представленный на рисунке 2, может включать в себя следующие примеры использования БПЛА: разведывательные операции группой БПЛА, поиск пострадавших, а также детектирование чрезвычайных ситуаций группой БПЛА, ретрансляция связи с помощью БПЛА, мониторинг полей, опрыскивание пестицидами группой БПЛА.

На рисунке 2 показаны три типовые точки входа в систему, которые связаны с подключением к доступному сервису и созданию поддельных пакетов с целью обрыва текущего соединения. Далее, у злоумышленника открывается широкий спектр возможностей, которые он может осуществить для нарушения технологического процесса функционирования БПЛА. Сценариев атак может быть большое количество, но, по сути, они сводятся к трем типам последствий. Это полное нарушение функционирования и крах БПЛА, получение БПЛА в пользование злоумышленника и использование захваченного БПЛА для атак на другие объекты.

Если говорить про инструментарий для проведения атак, то в основном злоумышленником используется программные средства, которые находятся открытом доступе. Кроме того, в сети интернет имеется большое количество готовых программ и скриптов, которые позволяют автоматизировать процесс перехвата БПЛА. Если говорить об аппаратном обеспечении, то основной упор делается на антенны беспроводной связи, которые должны поддерживать необходимые частоты и каналы связи, на которых работает БПЛА, а также иметь достаточную мощность для реализации атаки. Если же для проведения атаки мощности антенны недостаточно, то можно установить все необходимое оборудование на БПЛА и использовать его как инструмент для атаки.

В качестве недостатка, или уязвимости, который позволяет реализовать злоумышленнику атаку на БПЛА, показана физическая незащищенность каналов связи и самого БПЛА. Это наиболее простой способ проникновения в систему и реализации атак, и именно его практически невозможно устранить из-за «природы» БПЛА и открытости беспроводных каналов связи.

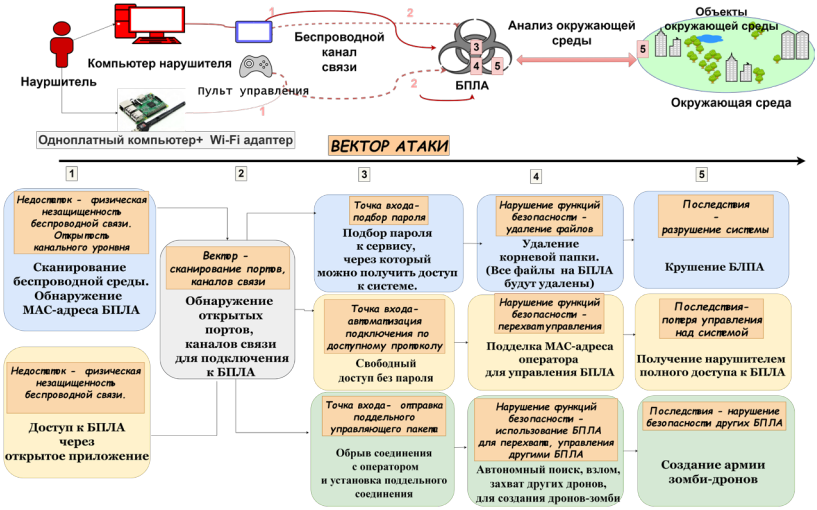


Рис. 2. Пример цепочки атаки с разными точками входа

После определения уязвимости, которую можно проэксплуатировать, злоумышленнику необходимо сформировать вектор атаки и найти точку входа в систему. Вектор атаки формируется на основе обнаружения открытых портов БПЛА. Так как для БПЛА используются программы управления на основе клиент-серверной архитектуры, то, помимо сетевого адреса, у БПЛА должен быть еще и открытый TCP/UDP порт (в зависимости от типов передаваемых данных). Сканирование портов возможно, когда злоумышленник уже находится в сети. В данном случае происходит анализ каналов связи, то есть тех радиочастот, на которых БПЛА может передавать данные. При обнаружении активности на радиочастоте можно сделать вывод о том, что в канале передаются данные. Далее в зависимости от того, на какой радиочастоте осуществляется передача данных, можно предположить, какой протокол связи используется для передачи. В зависимости от протокола связи определяется и точка входа в систему. Далее

непосредственно сам сценарий атаки развивается относительно того, какие именно цели преследует злоумышленник. Он может либо перехватить управление для угона БПЛА путем подделки управляющих команд, либо очистить файлы конфигурации БПЛА для полной его дестабилизации, или использовать его в качестве атакующего для воздействия на группу БПЛА.

Прерывание передачи между БПЛА в таких сценариях (Зашумление, Удаление сообщений) может привести к срыву миссии. Например, если координация в группе БПЛА будет нарушена, то они не смогут качественно выполнить свою работу и вернуться в исходную точку. Если же речь идет о ретрансляции связи, то миссия сразу будет сорвана. Такие события могут повлиять на окружающую среду и, в конечном счете, на человека. Например, беспилотники вели мониторинг местности, и один из них зафиксировал возгорание, но в этот момент на него было совершено нападение [5]. Он не смог вовремя сообщить о том, что происходит. Пока БПЛА не долетит до базы, будет потеряно время, и небольшое возгорание может перейти в пожар.

Атака прослушки канала связи является пассивной, и сама по себе не может повредить аппаратуре БПЛА. Но, как видно из сценария, представленного на рисунке 2, ее можно использовать для сбора данных о каналах связи, протоколах связи, что важно для дальнейшей реализации активной атаки.

Из приведенных примеров видно, что если атака приводит к угону БПЛА, его потере или падению, то эти последствия могут быть связаны и с информацией, которую обрабатывал БПЛА, и с самим БПЛА, и с объектом, с которым непосредственно взаимодействовал БПЛА. Также со временем могут возникнуть косвенные последствия [6].

Таким образом, важно как можно раньше обнаружить атаку на БПЛА, чтобы вовремя принять правильный план минимизации рисков и устранить инциденты информационной безопасности. Часто для обнаружения атак используются методы машинного обучения и искусственные нейронные сети.

2. Анализ методов и алгоритмов обнаружения спуфинговых атак с использованием генераторов данных. В статье [7] авторы предлагают новый алгоритм AMDES (Unmanned Aerial Intrusion Detection System with Multifractal Analysis – беспилотная система обнаружения вторжений с мультифрактальным анализом) для обнаружения атак подделки. Этот новый алгоритм основан на принципах вейвлет-мультифрактального анализа (Wavelet Leader

Multifractal Analysis – WLM), а также машинного обучения. Эта система работает путем сбора информации из сети с помощью сетевых сенсоров, работающих как устройства захвата и передачи информации (распределенные или централизованные датчики, в зависимости от топологии сети). Затем, на этапе предварительной обработки, собранные данные обрабатываются, чтобы лучше выявить их особенности. После того, как сигнатуры получены, следующим шагом становится сравнение сигнатур обычного трафика с теми, которые содержат атакующий трафик, а затем наблюдение за закономерностями, возникающими при различной частоте атак. Чтобы продемонстрировать осуществимость такой методологии при отсутствии работающего БПЛА, авторы разработали испытательный стенд на основе предварительно собранных сетевых записей RADAR. В представленном исследовании авторы собирали данные радиочастотного диапазона, фиксируя радиочастотные сигналы. Базовая станция контролирует работу БПЛА и постоянно обменивается данными телеметрии с БПЛА. Эти радиочастотные сигналы были записаны для анализа. Была обработана 31 запись RADAR, что соответствует данным за один месяц. Каждая исходная запись содержала около 800 000 экземпляров. Имитационные атаки проводились путем случайного выбора нескольких самолетов, а затем случайным изменением записанных траекторий от 0 до 10%. При этом авторы никак не показывают, насколько эффективен их метод создания аномальных событий и насколько они в целом сопоставимы с реальной атакой. Ведь и без атаки, во время реального полета БПЛА, особенно в сложных условиях, могут происходить события, заявляющие о его отклонении от курса. Почему обрабатывается только 10% изменений, авторами не обосновывается. Если вернуться к рисунку 1, то можно предположить следующее: атака была проведена, но неясно, насколько сильно она повлияла на БПЛА и к каким потенциальным последствиям могла привести.

В другой статье [8] описывается система обнаружения атак на основе нейронных сетей с использованием сигнатурного анализа. Для получения сигнатуры трафика в трех измерениях авторы измерили функцию масштабирования в зависимости от статистических моментов, которые могут принимать положительные или отрицательные значения, а также в зависимости от временной шкалы трафика. Затем, используя тот же метод WLM на основе симулятора гибридной сети БПЛА, авторы получили необходимые сигнатуры. Для получения экспериментальных данных авторы использовали стенд, где TCP-трафик генерируется пятью источниками, которые генерируют

длинные TCP-потоки к получателю через маршрутизатор с разной пропускной способностью канала. Рассматриваются два типа DDoS-атак: атака Constant Flash-Crowd (CFC) и атака Progressive Flash-Crowd (PFC). Соответствующие им аномалии были сгенерированы с помощью инструмента HPing3. Авторы получили интересные результаты, особенно в отношении набора данных для обучения нейронной сети с целью обнаружения атак. Тем не менее, остается вопрос, насколько атака может повлиять на БПЛА и насколько легко ее реализовать. Кроме того, реализовать его можно только в том случае, если злоумышленник будет находиться внутри сети и проводить предварительные разведывательные действия.

В статье [9] обсуждается новый метод обнаружения атак подделки на БПЛА. Авторы также используют нейронные сети, они тестируют несколько архитектур беспроводных сетей и подтверждают эффективность своего метода, показывающего достаточно быстрое обнаружение и низкое количество ложных срабатываний. Для обнаружения атак используются следующие факторы: номер спутника, измерение доплеровского сдвига, псевдодальность, время приемника, информация о декодированном времени, фазовый сдвиг несущей, коррелятор подсказок, выход позднего коррелятора, выход раннего коррелятора, запрос в фазе, квадратурный запрос, доплеровские измерения контура несущей, отношение сигнал/шум. Аналогично, при обнаружении атаки авторы полагаются только на внешние факторы и анализируют обстановку вокруг БПЛА. Авторы проводили исследование в лабораторных условиях, и до конца не ясно, как окружающая среда повлияет на обнаружение атаки. Достоинством этой работы является то, что авторы рассматривают несколько вариантов атак GPS-спуфинга, что повышает уровень обнаружения атаки. При этом такая архитектура позволяет детектировать только атаки GPS-спуфинга.

В статьях [10, 11] авторы описывают следующую схему для сбора данных как в случае, когда атака не проводится, так и в случае, когда атака проводится. Используются аппаратное обеспечение, которое представляет собой универсальное периферийное устройство с программно определяемым радио (SDR), и программное обеспечение GNSS-SDR с открытым исходным кодом на основе лицензии GNU. При этом эмулируются спутники с определенными параметрами: отношение сигнал/шум, доплеровский сдвиг, число спутников и т.д. Для эмуляции атаки GPS-спуфинга авторы рассматривают три случая: злоумышленник не знает точное местоположение и координаты дрона и случайным образом генерирует сигнал; злоумышленник знает

местоположение БПЛА и осознанно проводит атаку; третий случай подразумевает использование нескольких синхронно работающих антенн. Авторы используют два варианта нормализации данных, которые собраны в результате эксперимента. Первый вариант описан в статье [10] и включает в себя вычисление коэффициента корреляции Спирмена и модификацию нестационарных данных. Во втором исследовании авторы меняют способ нормализации и вычисляют коэффициент по методу корреляции Спирмена после применения минимаксных технологий. В итоге они используют различные методы машинного обучения и выбирают наилучший для детектирования атаки.

Авторы статьи [12] предлагают анализировать журналы полета БПЛА и из них выделять признаки атаки. Причем, в отличие от предыдущих работ, они предлагают разделить признаки по отдельным категориям и для каждой категории использовать отдельную нейросеть для анализа. Авторы делят журнал полетов на несколько наборов данных в формате CSV в зависимости от имеющегося на БПЛА датчика/темы. При этом данные могут опрашиваться с разной частотой, поэтому также необходимо интерполировать определенные значения. В частности, некоторые признаки были сгруппированы только для компонента GPS: широта, долгота, высота, а также данные о скорости и местоположении. Исходя из такой концепции, авторы считают, что разные атаки влияют на разные кластеры признаков. В действительности, зачастую, когда проводится атака, то она может влиять сразу на несколько типов данных. К примеру, если при атаке зашумления БПЛА предпринимает экстренную посадку, как это делает DJI Mavic Air, то его координаты также будут изменены. При этом система обнаружения атак может ложно определить, что проводится две атаки. Авторы считают, что данные датчика GPS принимаются автопилотом с частотой 5 Гц. Когда поддельные сигналы вводятся в среду моделирования, они отправляются с гораздо большей скоростью. Это заставляет автопилот переключаться на более мощный сигнал [13]. После чего оценка положения БПЛА изменится, что приведет к его отклонению от курса [14]. Когда атака прекращается, БПЛА снова фиксируется на законном сигнале и перемещается, чтобы скорректировать свое положение, и возобновляет свою траекторию в миссии. В действительности, когда реализуется атака, то перестроение происходит недостаточно плавно. В реальной среде, когда БПЛА летит в открытом небе и получает сигнал от реальных спутников, злоумышленник, имеющий даже мощную антенну, не может в полной точности смоделировать сигнал спутников. Возникает

дополнительный шум, что доказано в работах авторов, рассмотренных ранее. Кроме того, изменяется число спутников, на которых фиксируется БПЛА, могут измениться не только координаты, но и высота полета [15]. Таким образом, число факторов намного больше, чем предполагают авторы [12]. Авторы статьи [16] используют этот же набор данных, только проводят некоторые преобразования. К примеру, они делят признаки на еще более укрупненные пять категорий. При этом они удаляют лишние признаки согласно двум правилам. По первому правилу удаляются все не универсальные признаки, остаются только те, которые присущи всем БПЛА. Второе правило подразумевает исключение параметров, которые имеют постоянные, неизменные значения, и параметров, которые могут иметь пропущенные значения. Если первое правило действительно позволяет унифицировать набор данных, то по поводу второго правила есть вопросы. К примеру, есть датчики, которые показывают значение true/false – это некое состояние сенсора, которое действительно не должно меняться во время полета, но фиксация его изменения и экстренное реагирование на него могут привести к положительным последствиям. Авторы унифицировали длину каждой функции с помощью пула временных меток, а также использовали упоминаемую ранее минимаксную технологию для приведения данных к единому масштабу. В таблице 1 приведены сравнительные характеристики рассмотренных методов.

Таблица 1. Сравнение методов и алгоритмов обнаружения спуфинговых атак с использованием генераторов данных

Работа	Содержание	Достоинства	Недостатки
[7]	Система обнаружения вторжений на основе мультифрактального анализа и машинного обучения для UAS/RADAR.	Эффективные алгоритмы вейвлет-мультифрактального анализа и машинного обучения. Экспериментальный стенд на основе большого количества собранных реальных данных.	Не показана эффективность метода генерации аномальных событий. Не обоснованы количественные характеристики (берется только 10% изменений). Не показано влияние атаки на БПЛА. Выявляются признаки атаки во внешних по отношению к БПЛА сущностях. Не рассматривается внутреннее состояние БПЛА.
[8]	Система обнаружения вторжений в сеть для оперативной связи БПЛА: от разработки методологии до проверки в реальных испытаниях.	Применяются эффективные алгоритмы вейвлет-мультифрактального анализа и машинного обучения. Для обучения нейросетей были разработаны достаточные наборы данных	Не рассмотрено, насколько легко могут быть реализованы данные атаки, с какими ограничениями можно столкнуться. Авторы не исследуют, как атаки и их признаки напрямую влияют на сам БПЛА и его характеристики. Выявляются признаки атаки во внешних по отношению к БПЛА сущностях.

Продолжение Таблицы 1

Работа	Содержание	Достоинства	Недостатки
[9]	Методы динамического отбора для обнаружения атак с подменой GPS на БПЛА.	Протестированы различные архитектуры беспроводных сетей. Достаточно быстрое обнаружение и низкое количество ложных срабатываний. Несколько вариантов атак GPS-спуфинга.	Исследования проводились только в лабораторных условиях. Метод требует дополнительных мощностей. Авторы не исследуют, как атаки и их признаки напрямую влияют на сам БПЛА и его характеристики. Выявляются признаки атаки во внешних по отношению к БПЛА сущностях. Рассматривается только внешнее воздействие на БПЛА, не анализируется его внутреннее состояние.
[10], [11]	Модели контролируемого машинного обучения на основе дерева для обнаружения атак спуфинга GPS на БПЛА	Универсальная схема сбора данных. Широкий набор параметров. Различные методы обработки и нормализации данных, что позволяет выбрать оптимальный для конкретного случая. Набор вариантов проведения атак спуфинга.	Не сформулированы требования и ограничения для эмулируемых данных. Есть ограничения применимости предложенных методов. Выявляются признаки атаки во внешних по отношению к БПЛА сущностях. Рассматривается только внешнее воздействие на БПЛА, не анализируется его внутреннее состояние.
[12]	Новый метол обнаружения сенсорных атак на беспилотные летательные аппараты	Разделение признаков, позволяет не только обнаруживать атаки, но и потенциально классифицировать тип атаки или целевой датчик.	Разметка данных не учитывает пересечения параметров. Атаки формируются только в лабораторных условиях. Число факторов намного больше, чем предполагают авторы. Авторы не исследуют, как атаки и их признаки напрямую влияют на сам БПЛА и его характеристики. Выявляются признаки атаки во внешних по отношению к БПЛА сущностях. Рассматривается только внешнее воздействие на БПЛА, не анализируется его внутреннее состояние.
[16]	Неконтролируемая система обнаружения вторжений для беспилотных летательных аппаратов с меньшими усилиями по маркировке.	Авторы используют методы нормализации сырых данных. Авторы унифицировали длину каждой функции с помощью пула временных меток, а также использовали минимаксную технологию для приведения данных к единому масштабу.	Разметка данных не учитывает анализ данных от критически важных сенсоров. Авторы не исследуют, как атаки и их признаки напрямую влияют на сам БПЛА и его характеристики. Выявляются признаки атаки во внешних по отношению к БПЛА сущностях. Рассматривается только внешнее воздействие на БПЛА, не анализируется его внутреннее состояние.

Подводя итог рассмотренным исследованиям по теме обнаружения атак на БПЛА, можно резюмировать следующее.

Авторы предлагают оригинальные методы формирования и нормализации наборов данных, которые можно применять не только к

изучаемым авторами наборам данных, но и к другим данным. Практически везде используются разные архитектуры нейросетей, авторы декларируют высокую эффективность методов обнаружения атак. Во всех исследованиях выявляются признаки атаки во внешних по отношению к БПЛА сущностях, то есть в целом анализируются сетевой трафик или шум полосы пропускания, уровень шума в радио среде. Несомненно, рассмотренные факторы идентифицируют атаку и являются ее признаками, но нельзя однозначно определить, насколько эффективно атака может повлиять на сам БПЛА и к каким последствиям она может привести. Предлагаемые методы предполагают наличие третьей стороны, собирающей информацию и обнаруживающей атаку. Не всегда возможно проанализировать радиочастотный диапазон вблизи БПЛА, часто аппарат находится далеко. Если же сам БПЛА вынужден постоянно анализировать радиочастотный диапазон или активность сети, то это может повлиять на его производительность.

Таким образом, важной задачей становится сбор и обработка информации, связанной с БПЛА, и наше исследование направлено на разработку метода подготовки набора данных для разработки и тестирования систем обнаружения вторжений для БПЛА.

3. Архитектура экспериментального стенда. Открытый характер структуры сигнала GPS делает его уязвимым для атак с подменой GPS, которые могут осуществляться открыто или скрытно. В первом случае мощный сигнал, создаваемый злоумышленником, подавляет сигнал, поступающий со спутников. Эту атаку легко осуществить, но она требует значительных ресурсов [17]. При реализации скрытой атаки мощность сигнала постепенно увеличивается до тех пор, пока целевая система полностью не переключится на поддельный сигнал, транслируемый злоумышленником. Этот подход более сложен и требует большего количества компонентов и детальной подготовки, но потребляет меньше энергии и обеспечивает плавный переход целевой системы на поддельную. Если БПЛА полностью автономен, то бортовая система выведет БПЛА на ложное местоположение цели или наземную станцию. Этот тип атаки приведет к провалу миссии и возможной потере БПЛА. Если позиция атакуемого БПЛА выбрана недостаточно точно, система безопасности БПЛА может обнаружить атаку, после чего БПЛА может перейти на ручное управление или изменить траекторию по заданному сценарию поведения [18]. Неточное время также может привести к обнаружению атаки или сбою внутренней

синхронизации системы. Все эти факторы необходимо учитывать на подготовительном этапе атаки [19].

Проведение атаки возможно только в том случае, если система управления БПЛА переведена в автоматический режим и полностью полагается на систему навигации, использующую датчики GPS/ГЛОНАСС. Для получения экспериментальных данных для данного исследования и моделирования поведения БПЛА в штатных условиях и при атаке был выбран метод натурного моделирования. В ходе исследования разработан экспериментальный БПЛА, в основе которого были полетный контроллер PixHawk 4 и плата управления Raspberry PI 4. Состав стенда показан на рисунке 3. Для управления полетом БПЛА использовался планировщик QGroundControl, который обеспечивает полное управление полетом и планирование задач для любого БПЛА с поддержкой протокола MAVLink. По результатам миссии были сформированы два типа журналов, которые в дальнейшем были проанализированы: Dataflash и telemetry. Для проведения атаки использовался специализированный радиочастотный модуль HackRF One.

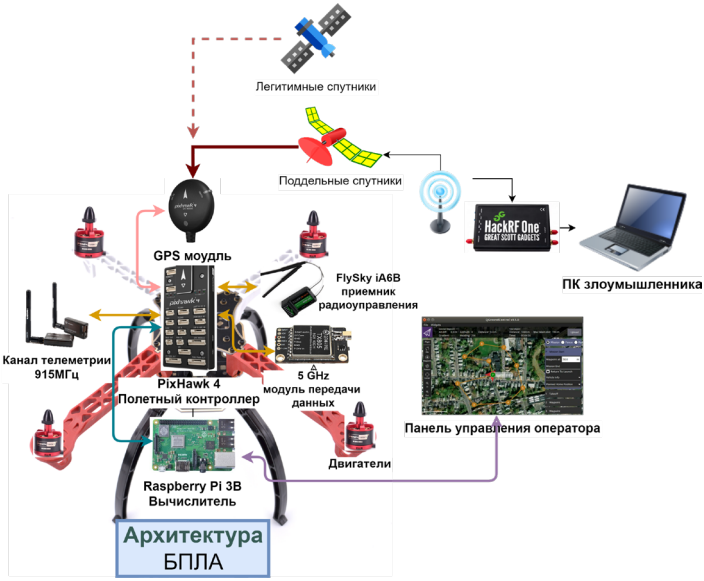


Рис. 3. Архитектура натурной модели БПЛА для проведения экспериментального исследования

С помощью данного стенда проходила отработка нескольких сценариев нормального полета, а затем нескольких сценариев атаки. Всего было выполнено до 20 тестовых испытаний. В результате испытаний были собраны экспериментальные данные для анализа из журналов логирования.

4. Экспериментальное исследование. Экспериментальное исследование проходило с применением метода натурного моделирования. Испытания проводились на полигоне в безветренную погоду при хорошей видимости. Экспериментальный БПЛА подвергался атаке подделки GPS сигнала. Атака осуществлялась путем направления сигнала большей GPS мощности с целью имитации спутников. Для реализации атаки использовалось устройство HackRF One. Для более корректной реализации атаки скачивался ежедневный файл эфемерид GPS, который находится на сайте НАСА (Национальное управление по аэронавтике и исследованию космического пространства). Далее необходимо сформировать файл с координатами для передатчика. После чего можно транслировать координаты через HackRF. В ходе испытаний с атакой БПЛА не подвергался атаке в течение 3–5 минут, а затем атака осуществлялась в течение 10 минут. В ходе атаки злоумышленник установил фиктивное местоположение БПЛА. Следовательно, наблюдалось изменение высоты БПЛА, а также смещение БПЛА в заданную атакующим точку. В нескольких экспериментах при резком прерывании атаки наблюдалось падение БПЛА.

В данной статье рассматриваются атаки, связанные с воздействием на GPS-сигнал, который позволяет БПЛА ориентироваться на местности. Большинство исследователей также анализируют GPS-сигналы, либо передачу данных по радиочастотным каналам. Анализ GPS-сигнала обусловлен тем, что большинство систем навигации для БПЛА построены на основе данного типа сигнала. Используемые в исследовании БПЛА могут позиционироваться с использованием как GLONASS, так и GPS систем. Тем не менее, позиционирование с помощью одной GLONASS системы является затруднительным, так как число спутников, которые фиксирует БПЛА (обычно 4 – 6) недостаточно для корректной работы. Число спутников BEIDOU в той местности, где испытывался БПЛА, также незначительное. Для корректной работы БПЛА требуется от 11 спутников, на данный момент такое количество может быть обеспечено только навигационной системой GPS.

В статье [20] подробно описан реализованный сценарий атаки на БПЛА, сам же экспериментальный стенд подробно описан в статье [21].

В целом план эксперимента состоял из следующих этапов:

1. БПЛА завис в воздухе над одной точкой на три минуты.
2. БПЛА был поднят в воздух и завис над точкой в течение минуты.
   2.1. БПЛА был атакован. Злоумышленник попытался отвести БПЛА в сторону.
   2.2. После того, как БПЛА начал движение и прошел 3–6 метров, атака закончилась.
3. После завершения атаки было два варианта развития событий.
   3.1. БПЛА пытался вернуться в исходную точку.
   3.2. БПЛА упал на землю.

Порядок проведения атаки:

Для передачи положения в определенной точке необходимо:

1) Сформировать файл с координатами для передатчика с помощью команды:

./gps-sdr-sim -b 8 -e brdc1900.20n -l 47.204715, 38.940236 -o Location.bin,

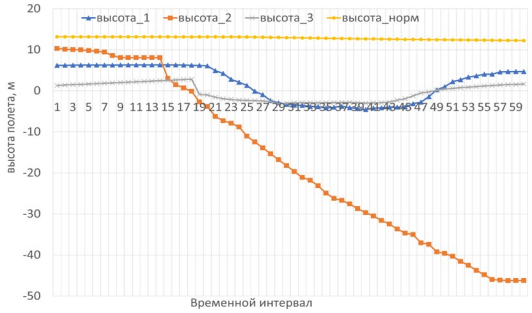
– где: brdc1900.20n – ежедневный файл эфемерид GPS, который находится на сайте НАСА;
– 47.204715, 38.940236 – широта и долгота;
– Location.bin – имя файла на выходе.

2) Транслировать координаты через HackRF командой:

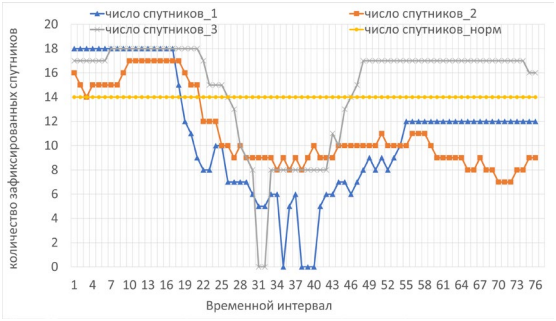
hackrf_transfer -f 1575420000 -s 2600000 -a 1 -x 15 -R -t Location.bin,

– где: f – частота вещания GPS спутников;
– x мощность сигнала (максимум 47);
– R – повторение.

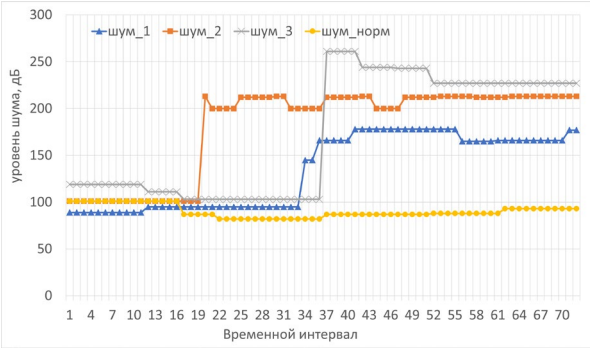
Проанализируем данные, полученные экспериментально. Результаты анализа показаны на рисунке 4. Графики получены путем реализации атаки на экспериментальный БПЛА согласно описанному сценарию. Атака заключалась в том, что с помощью передатчика и направленной антенной производилась трансляция поддельного местоположения БПЛА. Для трансляции местоположения использовалась частота, на которой работает протокол GPS. Передавалась геопозиция, в которой должен находиться БПЛА, которая включает в себя широту, долготу и высоту полета. На рисунке 4 приведены примеры изменений некоторых параметров под воздействием атаки на протяжении трех разных экспериментов и в нормальном состоянии.


высота_1
высота_2
высота_3
высота_норм
высота полета, м
Временной интервал

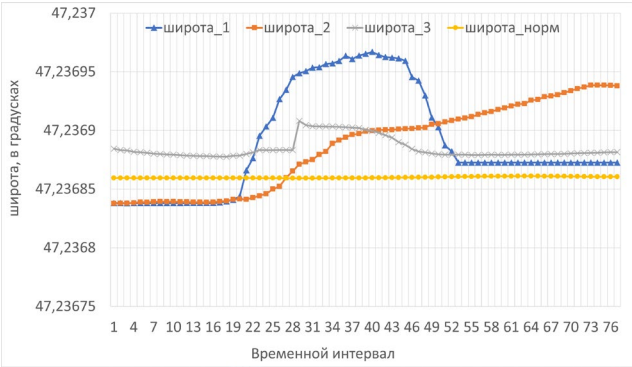
а)


число спутников_1
число спутников_2
число спутников_3
число спутников_норм
количество зафиксированных спутников
Временной интервал

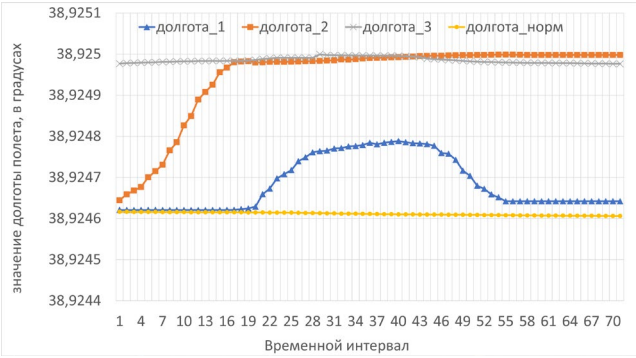
б)


шум_1
шум_2
шум_3
шум_норм
уровень шума, дБ
Временной интервал

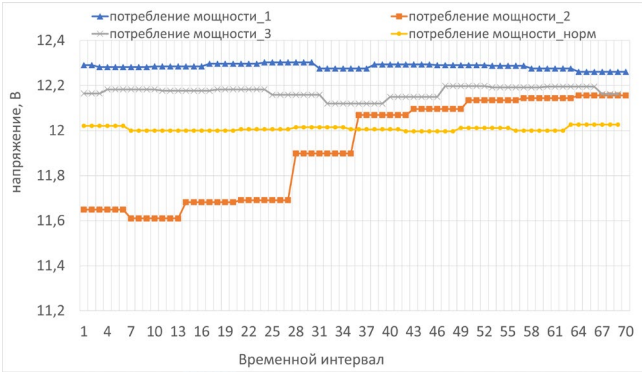
в)


широта_1
широта_2
широта_3
широта_норм
широта, в градусах
47,237
47,23695
47,2369
47,23685
47,2368
47,23675
1 4 7 10 13 16 19 22 25 28 31 34 37 40 43 46 49 52 55 58 61 64 67 70 73 76
Временной интервал

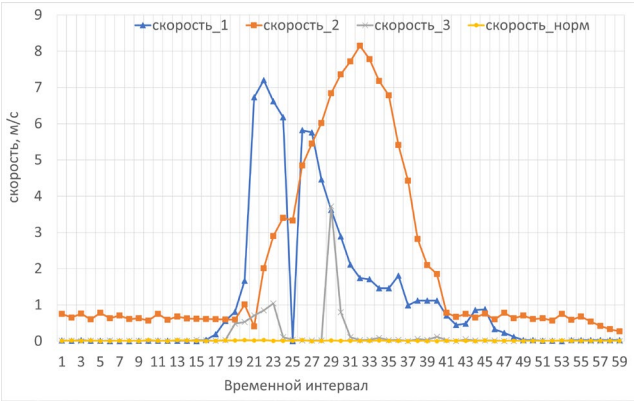
г)


долгота_1
долгота_2
долгота_3
долгота_норм
значение долготы полета, в градусах
38,9251
38,925
38,9249
38,9248
38,9247
38,9246
38,9245
38,9244
1 4 7 10 13 16 19 22 25 28 31 34 37 40 43 46 49 52 55 58 61 64 67 70
Временной интервал

д)


потребление мощности_1
потребление мощности_2
потребление мощности_3
потребление мощности_норм
напряжение, В
12,4
12,2
12
11,8
11,6
11,4
11,2
1 4 7 10 13 16 19 22 25 28 31 34 37 40 43 46 49 52 55 58 61 64 67 70
Временной интервал

е)



и)

Рис. 4. Изменение киберфизических параметров БПЛА под воздействием атаки: а) Оценка абсолютной высоты полета по GPS – Absolute Altitude GPS Estimate; б) Количество используемых спутников – Num Satellite Used; в) Уровень шума GPS – GPS Noise; г) Широта полета – Latitude; д) Долгота полета – Longitude; е) Напряжение аккумуляторной батареи – Battery voltage; и) Скорость – Velocity, м/с (заданные значения X, Y, Z)

При проведении экспериментального исследования фиксировался момент начала атаки, то есть время, когда HackRF начинает транслировать поддельный сигнал. Время на полетном контроллере синхронизировано со временем на пульте оператора, который запускает атаку. Поэтому имеется возможность проанализировать файлы журнала полета, сопоставив временные метки. Время начала атаки при каждом из трех экспериментов сопровождается изменением числа спутников, которые фиксирует БПЛА, а также увеличением значения сингал/шум. Остальные параметры могут начать изменяться немного позже. Из рисунка 4 (а) видно, что абсолютная высота полета стала отрицательной в первом эксперименте, это сопровождалось резким снижением и дальнейшим падением БПЛА. Отрицательная абсолютная высота свидетельствует о том, что БПЛА был полностью дезориентирован (примеры отрицательной абсолютной высоты встречаются на суше реже: впадина Каттара, Африка (-133 м), Северная Америка (-85 м), Приатлантические районы Нидерландов и др.). При проведении эксперимента БПЛА была задана точка вблизи Нидерландов, именно поэтому высота была отрицательной. Кроме того, как видно из рисунков 4 (д), 4 (г), значение широты и долготы также резко менялись в случае первого эксперимента. Это означает, что БПЛА

сразу после начала атаки начал резкое изменение маршрута полета (хотя должен был «зависать» над одной точкой, установленной оператором). При этом во время эксперимента наблюдалась резкая смена местоположения БПЛА с его дальнейшим падением. Это резкое изменение также вызвало увеличение скорости, как видно из рисунка 4 (и). Для остальных двух случаев атаки транслировалась точка, которая находилась на полигоне, поэтому таких значительных перепадов не наблюдалось. Из рисунка 4 (б) видно, что при реализации эксперимента 1, 3 GPS-приемник теряет связь с реальными спутниками и через некоторое время переключается на фальшивые. Это сопровождается тем, что число спутников в какой-то момент снижается до нуля. Для эксперимента 2 переход осуществляется более плавно без нулевых значений. Эксперимент 2 сильнее всего повлиял на перемещение БПЛА, также это отразилось на энергопотреблении, которое резко увеличилось, как видно из рисунка 4 (е) для эксперимента 2.

График «шум_норм» на рисунке 4 показывает изменение параметров при отсутствии воздействия со стороны атаки на БПЛА. Таким образом, как видно из рисунков, когда БПЛА должен зависать на месте при удержании высоты, то его показатели либо не должны меняться, либо могут незначительно смещаться.

Из рисунка 4 видно, что для всех трех экспериментов наблюдалось резкое изменение всех параметров. При нормальном состоянии изменения параметров могут наблюдаться, но это отклонение намного ниже. Исходя из этого, оценить и описать ситуацию, при которой возникает атака, можно с помощью среднеквадратического отклонения и среднего значения для каждого параметра. Регулируя данные метрики (среднее значение и среднеквадратическое отклонение), можно добиться конструирования графиков, которые отражают условия проведения атаки без прибегания к реализации реальной атаки. Кроме того, выявленные зависимости позволяют изменять данные нормального полета в режиме реального времени для симуляции атаки.

Полетный контроллер Pixhawk 4 позволяет собирать большое число параметров от встроенных сенсорных систем. Тем не менее, не все из них являются достаточно информативными для обнаружения атаки Подделка GPS сигнала. Данная атака, как было выявлено из экспериментального исследования и теоретического анализа литературы, направлена на «угон» БПЛА, а побочным следствием атаки может стать его падение.

В связи с этим, в данном исследовании предлагается моделирование следующих наборов параметров:

– Загруженность центрального процессорного устройства (ЦПУ). В данном случае речь идет о процессоре полетного контроллера БПЛА.

– Высота полета БПЛА (ha). Имеется в виду высота относительно земли, которая фиксируется внутренними датчиками БПЛА. Высота задается при формировании полетного задания или оператором с помощью пульта управления.

– Число спутников (Gn). БПЛА при полете фиксирует число спутников, от которых он получает сигнал в данный момент, для корректной работы данное число должно превышать 10.

– Уровень шума (Gnoi). Данный показатель фиксируется радио модулем, который получает сигнал, и при значении, превышающем 150, можно говорить об атаке.

– Координаты БПЛА (x,y,z). Координаты, которые фиксируются сенсорной системой БПЛА при позиционировании на местности.

– Скорость полета (S). Измеряется в м/с и задается оператором.

– Ускорение (V). Фиксируется для двигателей, как правило, фиксируется по осям x, y, z.

– Широта (Lat). Координаты БПЛА, получаемые от глобальной навигационной системы. Задаются оператором.

– Долгота (Lon). Координаты БПЛА, получаемые от глобальной навигационной системы. Задаются оператором.

5. Обзор наборов данных для получения и тестирования систем обнаружения атак, а также методов их формирования. Во многом эффективность систем обнаружения атак зависит от наборов данных, используемых для их обучения и тестирования, и исследователи по-разному подходят к вопросу формирования таких датасетов. Однако получение наборов данных хорошего качества для обучения и тестирования IDS является сложной задачей.

Большинство исследователей оценивают производительность систем IDS, используя так называемые эталонные наборы данных.

В 1998 году Лаборатория Линкольна Массачусетского технологического института создала первый набор данных для обнаружения вторжений, названный DARPA, в рамках исследования, финансируемого DARPA [22]. В 1999 году исследователи Калифорнийского университета обновили и проанализировали файлы

tcpdump DARPA, в результате чего был создан набор данных KDD CUP 99 [23–24].

В [25] авторы подробно рассматривают несколько таких классических наборов данных. Рассматривались DARPA / KDD CUP 99, NSL KDD CUP 99, CAIDA, CICDS 2017, ADFA-LD & ADFA-WD, KYOTO. Набор данных KDD Cup '99 широко используется в исследованиях IDS и разработке новых стратегий защиты компьютерных сетей от различных угроз. Сложность исследования, влияние дублированных и избыточных записей, а также неравное количество участников исследования – все это проблемы, которые могут поставить его под угрозу.

Авторы [26] также провели исследование широко используемых наборов данных IDS для исследования алгоритмов машинного обучения в области IDS и реализованных атак. Их исследование показывает, что до 60% работ используют набор данных NSL-KDD, до 30% используют набор данных CTU-13 и до 10% используют набор данных CIC-IDS2017.

В [27] авторы оценили производительность моделей IDS, обучая их с помощью наборов данных NSL-KDD и CIC-IDS2017 по отдельности. Они использовали состязательные методы: DeepFool, JSMA, FGSM и CW. Исследование проводилось только на основе атак типа «отказ в обслуживании» (DoS). Результаты оценки показывают, что общая производительность модели при обучении с использованием набора данных CIC-IDS2017 снизилась на 40 % и на 13 % при обучении с помощью NSL-KDD [28].

В [29] рассматриваются наборы данных для обучения IDS в привязке к атакам на системы интернета вещей (IoT). Специфика системы определяет и способы формирования наборов данных, которые чаще всего комплектуются из реальных данных, не обязательно содержащих данные об атаках (например, данные из системы диспетчерского управления и сбора данных SCADA). Но здесь также часто используются стандартные наборы данных, например, были приведены примеры использования наборов данных AWID, NSL-KDD. Подробно были рассмотрены CIC-IDS2017, UNSW-NB15, DS2OS, BoT-IoT, KDD Cup 1999, NSL-KDD. Были сделаны выводы о том, что в большинстве исследований использовались KDD99, NSL-KDD и реальные частные наборы данных. NSL-KDD широко используется исследователями с различными методами машинного обучения. Этот набор данных дал лучшую точность. Он широко использовался для атак Probing, U2R, DoS и R2L. KDD99 имеет те же функции, что и NSL-KDD, который включает 41 функцию

и 1 атрибут класса, который подпадает под 4 типа атак: зондирующие атаки, U2R-атаки, R2L-атаки и DoS-атаки. NSL-KDD используется чаще по сравнению с KDD99, но результаты последнего лучше, чем у других общедоступных наборов данных. Ученые показали, что включение общедоступных наборов данных, таких как NSLKDD, UNSW-NB15 и KDDCUP99, в модели обнаружения угроз IoT представляет собой серьезную проблему. Когда модели атак IoT сочетаются с общедоступными наборами данных с проблемами качества, результаты могут быть ниже среднего [30].

В самом деле, в последнее время стало доступно значительное количество наборов данных, которые охватывают относительно модернизированные сценарии сетевого трафика [31]. Кроме того, появились методики модификации существующих наборов данных. Так, в [32] для разработки и проверки контролируемых моделей машинного обучения в системах обнаружения атак также использовался набор данных NSL-KDD, записи в котором были тщательно отобраны – он состоит в общей сложности из 43 элементов, из которых 41 элемент представляет собой входящий трафик, а 2 атрибута состоят из меток и оценок [33, 34]. В представленном проекте был использован встроенный метод (дополнительный древовидный классификатор) для выбора функций, который сочетает в себе качества методов фильтрации и обертки и предоставляет функции в зависимости от их важности.

В работе [35] авторы также говорят о том, что одной из проблем в области систем обнаружения атак является то, что большая часть исследовательской работы проводилась с использованием старых наборов данных. В отличие от области изображений данные в области IDS быстро устаревают, поскольку шаблоны данных в сетях быстро меняются, а поведение атак становится изощренным. Набор данных должен отражать современное поведение сети и охватывать достаточные сценарии атак, чтобы модель IDS изучала широкий спектр характеристик трафика. Современные наборы данных включают в себя современное поведение сети и сценарии атак. Чем реалистичнее набор данных, тем эффективнее он может создать модель IDS в реальной среде. Авторы исследования анализируют наборы данных UNSW-NB15, Bot-IoT и CSE-CIC-IDS2018 и обсуждают, как работают различные алгоритмы классификации, когда модель IDS обучается с каждым из выбранных наборов данных.

Во всех рассмотренных работах говорится о том, что использование стандартных наборов данных не является достаточно

эффективным, поэтому разработка собственных алгоритмов генерации реалистичных наборов данных актуальна.

6. Метод моделирования данных. Особенностью разрабатываемого метода является то, что он позволяет выявить характеристики в изменении киберфизических параметров БПЛА на основе анализа последствий реальных атак и смоделировать данные характеристики, схожие с реальными данными, но при этом отличающиеся от реальных. Как было сказано ранее, проблемой многих работ является отрыв от связи с реальными сценариями атак и реальными киберфизическими системами. Изучив особенности изменения киберфизических параметров под воздействием атак, можно генерировать поддельные данные с целью тестирования атак в режиме реального времени. Кроме того, большинство методов моделирования наборов данных и генерации данных основаны на том, что некоторый внешний монитор следит за трафиком и активностью системы. При этом если речь идет о БПЛА, то он не всегда находится в пределах видимости базовой станции и может действовать автономно. Предлагаемый метод моделирования данных направлен на использование в системах обнаружения атак на узле, для случаев, когда узел анализирует изменение собственных параметров. Таким образом, новизной данного метода является возможность моделирования изменений киберфизических параметров БПЛА путем анализа того, как на них реагирует внутренняя система БПЛА, выделяя разные периоды активности, что способствует созданию наборов данных, которые с высокой вероятностью приближены к ситуации реальной атаки. В результате решается проблема актуальности генерируемых данных, их достоверности и реалистичности, а также появляется возможность тестирования систем обнаружения вторжений, которые работают внутри БПЛА и анализируют изменения киберфизических параметров БПЛА в режиме реального времени. Как видно из рисунка 5, при проведении атаки на БПЛА изменение данных не происходит прямолинейно и однозначно. Найти зависимость достаточно сложно, можно лишь попытаться описать структуру полученных данных. Для этого применим критерий χ^2. Выдвигается нулевая гипотеза о том, что наблюдаемые частоты соответствуют ожидаемым (т.е. между ними нет разницы, так как они взяты из одной и той же генеральной совокупности). Если это так, то разброс будет относительно небольшим, в пределах случайных колебаний. Мера распространения определяется статистикой χ^2. Далее, либо полученная статистика сравнивается с критическим значением (для соответствующих степеней свободы и уровня значимости), либо, что

корректнее, вычисляется наблюдаемое p-значение, т. е. вероятность получения такого или даже большего значения статистики при справедливости нулевой гипотезы. Например, известно, что высота полета должна быть равна 15, будем считать это нулевой гипотезой и подтвердим эту гипотезу, сравнив ее с текущим значением высоты. Воспользуемся формулой:

$$F\chi^2(A) = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{(A_{ij} - O_{ij})^2}{O_{ij}}, \quad (1)$$

$F\chi^2(A)$ – это статистическая функция, при больших n имеет приблизительно χ^2 – распределение с (r-1) (c-1) степенями свободы, где i – номер строки (от 1 до r), j – номер столбца (от 1 до c). Критерий χ^2 используется, чтобы определить, подтверждается ли гипотеза экспериментом. A_{ij} – фактическое значение параметра в текущий момент времени (то значение параметра, которое получено от полетного контроллера и записано в матрицу значений), интервал данных, который содержит результаты наблюдений, подлежащие сравнению с ожидаемыми значениями. O_{ij} – ожидаемое значение параметра в ячейке ij (то значение, которое было записано в матрицу при нормальном полете), или теоретическое, то которое рассчитано заранее. В данном случае имеется в виду, что сравнивается матрица значений, которые получены при нормальном полете и при текущем полете, сравнение происходит поэлементно.

На рисунке 5 видно, что есть периоды, когда значение падает ниже 0.5, а иногда и достигает единицы. Это связано с наличием изменений показателя высоты. Можно увидеть области, когда значение сильно отличается от заданного.

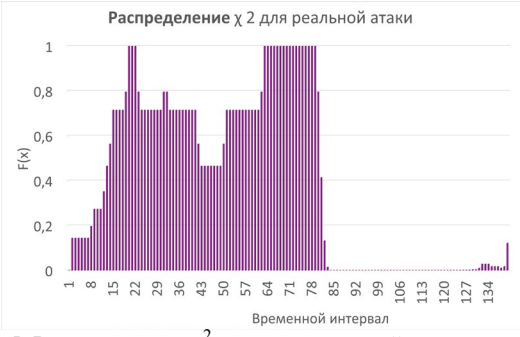


Рис. 5. Распределение χ^2 для индикаторной высоты полета

Прямоугольники характеризуют ситуацию, когда значение близко к заданному. Эта картина позволяет выявить периоды изменений. Далее для каждого из периодов вычисляем стандартное отклонение и среднее значение по формулам:

$$S_o = \sqrt{\frac{\sum (A - \overline{A})^2}{(n-1)}}, \quad (2)$$

$$M(A) = \int_{-\infty}^{\infty} af(a)da. \quad (3)$$

Пусть высота – это непрерывная случайная величина A, заданная плотностью распределения f(a), n – объем выборки, $\overline{A}$ – среднее арифметическое выборки. Вычисляем это значение для каждого из интервальных распределений, определенных с помощью распределения χ^2. Затем генерируем случайные значения в пределах этих параметров, используя функцию нормального распределения. Функция имеет следующие параметры:

– Вероятность P_{Gauss}. Вероятность, соответствующая нормальному распределению. Вместо значения вероятности генерируем случайное число сотдано формуле 4.

– Среднее $\overline{Cph}$. Распределение среднего арифметического для киберфизического параметра *Cph*.

– Стандартное отклонение σ_{Cph}. Стандартное отклонение распределения для киберфизического параметра.

$$F_{gen} = P_{Gauss}(f_{rand}; \overline{Cph}; \sigma_{Cph}), \quad (4)$$

где F_{gen} – функция для генерации значения киберфизического параметра.

В результате получаем следующий набор данных для высоты полета. Полученные данные выглядят не совсем похожими на реальные, что видно из рисунка 6. Реальные данные представлены внизу графика, данные, полученные этим методом, представлены рядом с эмулированными данными 3. Для их улучшения произведем над ними преобразования методом «скользящего среднего».

Воспользуемся формулой:

$$WA_t = \frac{\sum_{i=1}^{n-1} W_{t-i} \times a_{t-i}}{\sum_{i=1}^{n-1} W_{t-i}}, \quad (5)$$

где WA_t – значение взвешенного скользящего среднего в точке, n – количество значений исходной функции для расчета скользящего среднего, W_{t-i} – вес (весовой коэффициент), a_{t-i} – значение исходной функции в момент времени, удаленное от текущего на интервалы.

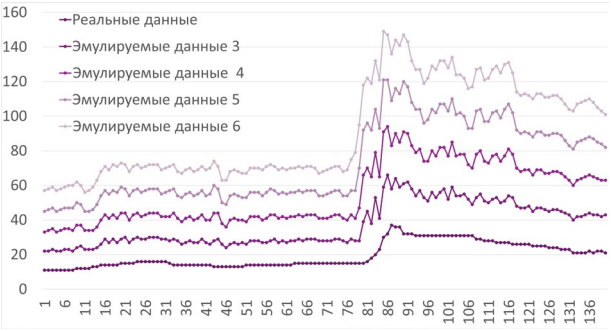
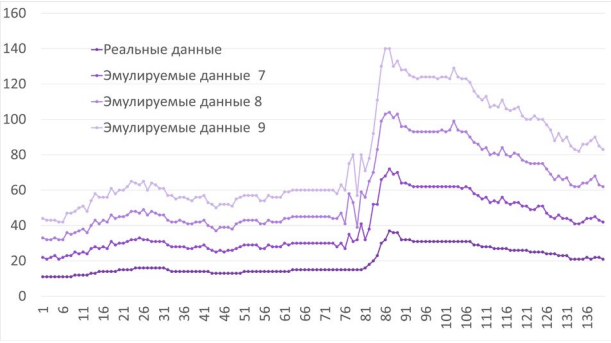
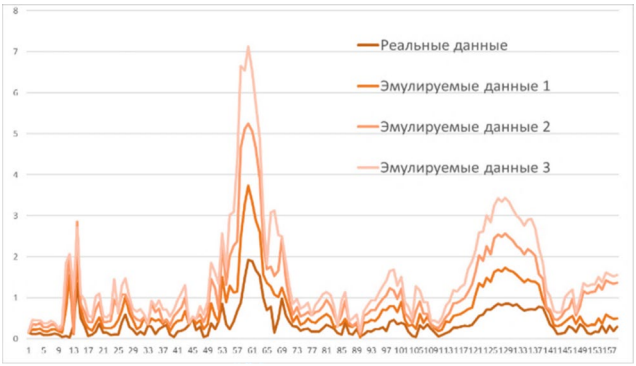


Рис. 6. Результат эмуляции данных для высоты полета

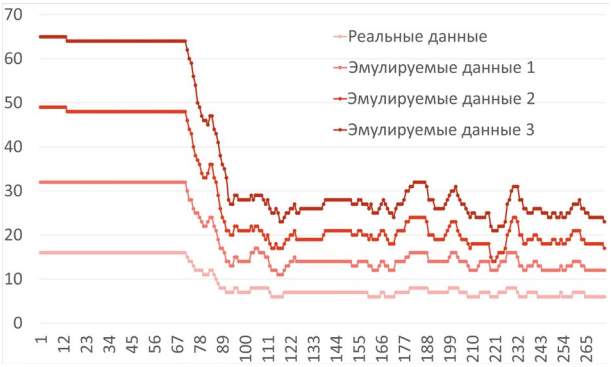
Три верхних графика были обучены с использованием метода скользящего среднего. Для улучшения метода попробуем вычислить среднее значение и стандартное отклонение не для всего интервала, а разбить его на еще меньшие интервалы, для которых значение χ^2максимально похоже. Результаты показаны на рисунке 7.



а)



б)



в)

Рис. 7. Результат эмуляции данных: а) высоты полета; б) ускорения БПЛА; в) числа спутников, которые зафиксировал БПЛА

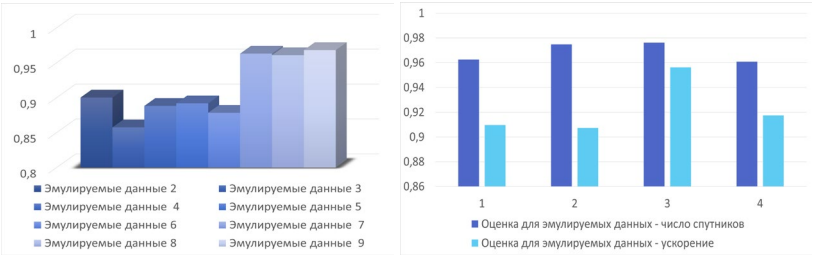
Визуально данные выглядят лучше. Необходимо подтвердить, что полученные данные коррелируют с исходными данными атаки.

Для этого воспользуемся коэффициентом корреляции Пирсона (r), который рассчитывается по следующей формуле:

$$r = \frac{\sum (a_{real} - \bar{a}_{real})(a_{emul} - \bar{a}_{emul})}{\sum (a_{real} - \bar{a}_{real})^2 \sum (a_{emul} - \bar{a}_{emul})^2}. \quad (6)$$

Результаты представлены в виде гистограммы на рисунке 8. На рисунке 8 (а) видно, что данные, полученные вторым методом, имеют более высокий коэффициент Пирсона, а значит, они в большей

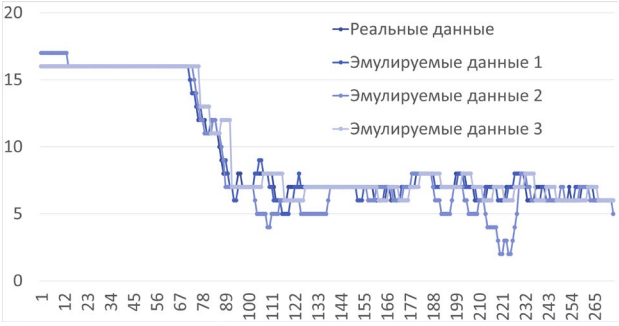
степени коррелируют с исходными. На рисунке 8 (б) представлены расчеты коэффициента Пирсона для ускорения и числа спутников, полученные вторым методом. В зависимости от целей, можно добиться того, чтобы сгенерированные данные были менее похожи на оригинал. Таким образом, мы можем изменять любые данные, независимо от их размера и порядка.



а) б)

Рис. 8. Гистограмма коэффициента корреляции Пирсона: а) для высоты полета б) для числа спутников и ускорения БПЛА

Этот метод, а также оценка качества данных позволит получить столько данных, сколько необходимо для обучения нейронной сети или тестирования метода обнаружения атак. При изменении среднего значения и среднеквадратического отклонения можно модифицировать поддельные данные, при этом форма данных и их правдоподобие не изменятся. На рисунке 9 представлены результаты генерации данных для числа спутников, высоты полета и ускорения.



а)

б)

в)

Рис. 9. Образцы сгенерированных данных для: а) числа спутников; б) высоты полета; в) ускорения

Из рисунка 10 (б) видно, что данные для высоты полета были дополнительно модифицированы и значения высоты были получены для более высоких диапазонов. При этом коэффициент корреляции Пирсона для сгенерированных данных равен 0,98, что говорит о достаточно высоком правдоподобии данных. Коэффициент правдоподобия позволил оценить реалистичность подделываемых данных.

7. Заключение. Признаком атаки, в частности, атаки на подмену навигационного сигнала, как показало экспериментальное и теоретическое исследование, является нестандартное изменение параметра, получаемое от полетного контроллера БПЛА. Под нестандартным изменением можно понимать увеличение/уменьшение математического ожидания параметра и рост среднеквадратического отклонения. Для того чтобы в автоматическом режиме определять такие участки графиков с изменением параметров, которое

характеризуется как нестандартное, необходимо использовать функцию, которая нормализует эти изменения. Каждый из анализируемых параметров имеет свою размерность и границы максимального/минимального значения. Поэтому для того, чтобы выявить признаки изменений, было выбрано распределение χ^2, которое позволяет определить вероятность соответствия между двумя временными рядами. Имея информацию о нормальном и аномальном полете БПЛА, можно сопоставить временные ряды и вычислить степень отклонения значения во время атаки. На основании распределения χ^2 удается выделить зоны наибольших и наименьших изменений. Разделив на участки графики с сырыми данными, можно, воспользовавшись обратной функцией нормального распределения, задав среднее значение и среднеквадратическое отклонение, получить набор случайных значений, которые будут похожими на те значения, которые возникают во время атаки. Тем не менее, эти значения генерируются слишком случайным образом и не коррелируют в достаточной степени с реальными, что оценивалось с помощью коэффициента Пирсона. Для улучшения качества генерируемых данных было принято решение использовать метод «скользящего среднего». Благодаря сглаживанию значений удалось повысить степень корреляции и получить высокие значения коэффициента Пирсона. Таким образом, данный механизм позволяет регулировать генерируемые данные на различных участках графика, а с помощью изменения среднеквадратического отклонения и среднего значения можно контролировать степень изменения параметра.

Таким образом, данное исследование позволило добиться следующих результатов.

Во-первых, было определено, что для обнаружения атаки и определения последствий, к которым она может привести, необходимо контролировать не только исходные параметры, но и внутренние кибер-физические параметры БПЛА. Это позволит спрогнозировать возможные последствия нападения и принять экстренные меры.

Во-вторых, был предложен метод имитации данных, соответствующих атаке. Этот метод позволяет имитировать данные с требуемой точностью. Также был предложен метод оценки качества сгенерированных данных.

Предложенный метод позволяет получать реалистичные данные изменения киберфизических параметров под воздействием атаки. Кроме того, данный метод является вычислительно достаточно простым и не потребует значительных вычислительных мощностей.

Метод позволяет быстро получать правдоподобные данные, при этом можно проводить их модификацию при необходимости.

В дальнейшем планируется проверить качество обучения нейронной сети на полученных данных, а также разработать нейронную сеть, способную самостоятельно генерировать данные.

Исследование выполнено за счет гранта Российского научного фонда № 22-11-00184, https://rscf.ru/project/22-11-00184/.

Литература

1. Eldefrawy M.H., Khan M.K., Alghathbar K. and Cho E.-S. Broadcast authentication for wireless sensor networks using nested hashing and the Chinese remainder theorem // Sensors. 2010. vol. 10. no. 9. pp. 8683-8695.
2. Strohmeier M., Lenders V., Martinovic I. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol // IEEE Communications Surveys & Tutorials. 2015. vol. 17. no. 2. pp. 1066-1087. doi: 10.1109/COMST.2014.2365951.
3. Manesh M.R., Kaabouch N. Cyber-attacks on unmanned aerial system networks: Detection countermeasure and future research directions // Computers & Security. 2019. vol. 85. pp. 386-401.
4. Wang S., Wang J., Su C., Ma X. Intelligent detection algorithm against UAVs' GPS spoofing attack // IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). 2020. pp. 382-389.
5. Duo B., Luo J., Li Y., Hu H., Wang Z. Joint trajectory and power optimization for securing UAV communications against active eavesdropping // China Communications. 2021. vol. 18. no. 1. pp. 88-99. doi: 10.23919/JCC.2021.01.008.
6. Wang Q., Dai H.-N., Wang H., Xu G., Sangaiah A.K. UAV-enabled friendly jamming scheme to secure industrial Internet of Things // Journal of Communications and Networks. 2019. vol. 21. no. 5. pp. 481-490. doi: 10.1109/JCN.2019.000042.
7. Zhang R., Condomines J.-P., Lochin E. A Multifractal Analysis and Machine Learning Based Intrusion Detection System with an Application in a UAS/RADAR System // Drones, 2022. vol. 6. p. 21. URL: https://doi.org/10.3390/drones6010021 (дата обращения: 25.07.2022).
8. Condomines J., Zhang R., Larrieu N. Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation // Ad Hoc Networks, 2018. vol. 90. URL: doi: 10.1016/j.adhoc.2018.09.004 (дата обращения: 25.07.2022).
9. Talaei K.T., Ismail. S., Kaabouch N. Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs // Sensors, 2022. vol. 22. p. 662. URL: https://doi.org/10.3390/s22020662 (дата обращения: 25.07.2022).
10. Aissou G., Slimane H.O., Benouadah S., Kaabouch N. Tree-based Supervised Machine Learning Models For Detecting GPS Spoofing Attacks on UAS // 2021 IEEE 12th Annual Ubiquitous Computing. Electronics & Mobile Communication Conference (UEMCON), 2021. pp. 0649-0653. doi: 10.1109/UEMCON53757.2021.9666744.
11. Aissou G., Benouadah S., El Alami H., Kaabouch N. Instance-based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS // 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022. pp. 0208-0214. doi: 10.1109/CCWC54503.2022.9720888.
12. Whelan J., Sangarapillai T., Minawi O., Almehmadi A., El-Khatib K. Novelty-based Intrusion Detection of Sensor Attacks on Unmanned Aerial Vehicles // Proceedings of

the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 2020. pp. 23-28. doi:10.1145/3416013.3426446.
13. Tippenhauer N.O., Pöpper C., Rasmussen K.B., Capkun S. On the requirements for successful GPS spoofing attacks // Proceedings of the 18th ACM conference on Computer and communications security, 2011. pp. 75–86
14. Kerns A.J., Shepard D.P., Bhatti J.A., Humphreys T.E. Unmanned aircraft capture and control via GPS spoofing // Journal of Field Robotics. 2014. vol. 31(4). pp. 617–636.
15. Basan E., Makarevich O., Lapina M., Mecella M. Analysis of the Impact of a GPS Spoofing Attack on a UAV // CEUR Workshop Proceedings, 2022. vol. 3094. pp. 6–16.
16. Park K.H., Park E., Kim H.K. Unsupervised Intrusion Detection System for Unmanned Aerial Vehicle with Less Labeling Effort // You. I. (eds) Information Security Applications. WISA 2020. Lecture Notes in Computer Science. Springer. Cham, 2020. vol 12583. URL: https://doi.org/10.1007/978-3-030-65299-9 (дата обращения: 25.07.2022).
17. Bekmezci I., Senturk E., Turker T. Security issues in Flying Adhoc Networks (FANETs) // Journal of Aeronautics and Space Technologies. 2016. vol. 9. no. 2. pp. 13-21.
18. Li C., Wang X. Jamming research of the UAV GPS/INS integrated navigation system based on trajectory cheating. // 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), 2016. pp. 1113-1117. doi: 10.1109/CISP-BMEI.2016.7852880.
19. Schmidt D., Radke K., Camtepe S., Foo E., Ren M. A survey and analysis of the GNSS spoofing threat and countermeasures // ACM Computing Surveys (CSUR), 2016. vol. 48. no. 4. pp. 64-69.
20. Basan E., Basan A., Nekrasov A., Fridge C., Gamec J., Gamcová M. A Self-Diagnosis Method for Detecting UAV Cyber Attacks Based on Analysis of Parameter Changes // Sensors, 2021. vol. 21. p. 509. URL: https://doi.org/10.3390/s21020509 (дата обращения: 25.07.2022).
21. Basan E., Basan A., Nekrasov A., Fridge C., Sushkin N., Peskova O. GPS-Spoofing Attack Detection Technology for UAVs Based on Kullback–Leibler Divergence. // Drones, 2022. № 6 (1). URL: https://doi.org/10.3390/drones6010008 (дата обращения: 25.07.2022).
22. Cunningham R.K., Lippmann R.P., Fried D.J., Garfinkel S.L., Graf. I., Kendall K.R. Evaluating Intrusion Detection Systems Without Attacking your Friends: The 1998 DARPA Intrusion Detection Evaluation (Lexington Lincoln Lab: Massachusetts Institute of Technology) URL: https://scholar.google.com/scholar?q=Cunningham+RK%2C+Lippmann+RP%2C+Fried+DJ%2C+Garfinkel+SL%2C+Graf+I+and+Kendall+KR+1999+Evaluating+Intrusion+Detection+Systems+Without+Attacking+your+Friends%3A+The+1998+DARPA+Intrusion+Detection+Evaluation+%28Lexington+Lincoln+Lab%3A+Massachusetts+Institute+of+Technology%29 (дата обращения: 25.08.2022).
23. Tavallaee M., Bagheri E., Lu W., Ghorbani A.A. A Detailed Analysis of the KDD CUP 99 Data Set // 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009. URL: https://scholar.google.com/scholar?q=Tavallaee+M%2C+Bagheri+E%2C+Lu+W+and+Ghorbani+AA+2009+A+Detailed+Analysis+of+The+KDD+CUP+99+Data+Set+2009+IEEE+Symposium+on+Computational+Intelligence+for+Security+and+Defense+Applications%2C+IEEE (дата обращения: 25.08.2022).
24. Uramová J., Scgeˇc P., Moravˇcík M., Papán J., Kontšek M., Hrabovsk`y J. Infrastructure for generating new ids dataset // 2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2018. pp. 603–610.

25. Nadiah N., Yusof M., Sulaiman N.S. Cyber Attack Detection Dataset: A Review // 2022 J. Phys.: Conf. Ser. 2319 012029 URL: https://iopscience.iop.org/article/10.1088/1742-6596/2319/1/012029 (дата обращения: 25.08.2022).
26. Martins N., Cruz J.M., Cruz T., Abreu P.H. Adversarial machine learning applied to intrusion and malware scenarios: a systematic review// IEEE Access, 2020. vol. 8. pp. 35403– 35419. URL: https://doi.org/10.1109/access.2020.2974752 (дата обращения: 25.08.2022).
27. Koroniotis N., Moustafa N., Sitnikova E., Turnbull B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset // Futur Gener Comput. Syst, 2019. vol. 100. pp.-779–96. URL: https://doi.org/10.1016/j. future.2019.05.041. (дата обращения: 25.08.2022).
28. Martins N., Cruz J.M., Cruz T., Abreu P.H. Analyzing the footprint of classifiers in adversarial denial of service contexts. // Progress in artificial intelligence. Berlin: Springer International Publishing, 2019. pp. 256–67. URL: https://doi.org/10.1007/978-3-030-30244-3_2210.1007/978-3-030-30244-3_22. (дата обращения: 25.08.2022).
29. Alshaibi A., Al-Ani. M., Al-Azzawi A., Konev A., Shelupanov A. The Comparison of Cybersecurity Datasets // Data, 2022. vol. 7. p. 22. URL: https://doi.org/10.3390/data7020022 (дата обращения: 25.08.2022).
30. Goswami G., Agarwal A., Ratha N., Singh R., Vatsa M. Detecting and Mitigating Adversarial Perturbations for Robust Face Recognition // Int. J. Comput. Vis., 2019. vol. 127. pp. 719–742.
31. Warzynski A., Kolaczek G. Intrusion detection systems vulnerability on adversarial examples // Innov. Intell. Syst. Appl. (INISTA), 2018. URL: https://doi.org/10.1109/inista. 2018. 84662 71. (дата обращения: 25.08.2022).
32. Rahim R., Ahanger A.S., Khan S.M., Masoodi F. Analysis of IDS using Feature Selection Approach on NSL-KDD Dataset 2021 // Raju Pal & Praveen K. Shukla (eds.), SCRS Conference Proceedings on Intelligent Systems, 2021. pp. 475–481. URL: https://doi.org/10.52458/978-93-91842-08-6-45 (дата обращения: 25.08.2022).
33. Hu W. et al. AdaBoost-Based Algorithm for Network // IEEE Transactions on Systems, Man, and Cybernetics. 2008. 38 (2). pp. 577–583.
34. Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) // Mil Commun Inf Syst Conf (MilCIS), 2015. URL: https://doi.org/10.1109/milcis.2015.7348942. (дата обращения: 25.08.2022).
35. Pacheco Y., Sun W. Adversarial machine learning: A comparative study on contemporary intrusion detection datasets. // August 2022 SN Computer Science. 2022. № 3(5). pp. 160–171. doi: 10.1007/s42979-022-01321-8.
36. Sharafaldin I., Gharib A., Lashkari A.H., Ghorbani A.A. Towards a Reliable Intrusion Detection Benchmark Dataset // Softw. Netw. vol. 2017(1). pp. 177–200.
37. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // Proceedings of the 4th International Conference on Information Systems Security and Privacy. 2018. vol. 1. pp. 108–116.

Басан Елена Сергеевна — канд. техн. наук, доцент, кафедра безопасности информационных технологий, Южный федеральный университет. Область научных интересов: разработка и исследование технологий обнаружения атак и вторжений, обнаружение аномального поведения, безопасность робототехнических систем, анализ угроз и уязвимостей. Число научных публикаций — 99. ebasan@sfedu.ru; улица Чехова, 2, 347922, Таганрог, Россия; р.т.: +7(951)520-5488.

Пескова Ольга Юрьевна — канд. техн. наук, доцент, кафедра безопасности информационных технологий, Южный федеральный университет. Область научных интересов: информационная безопасность. Число научных публикаций — 206. oyupeskova@sfedu.ru; улица Чехова, 2, 347922, Таганрог, Россия; р.т.: +7(8634)371-905.

Силин Олег Игоревич — студент, Южный федеральный университет. Область научных интересов: разработка и исследование технологий обнаружения атак и вторжений, расследование инцидентов, беспилотные летательные аппараты, оценка рисков. Число научных публикаций — 5. silin@sfedu.ru; улица Чехова, 2, 347922, Таганрог, Россия; р.т.: +7(928)326-4256.

Басан Александр Сергеевич — канд. техн. наук, доцент, Южный федеральный университет. Область научных интересов: разработка и исследование технологий обнаружения атак и вторжений, обнаружение аномального поведения, безопасность робототехнических систем, анализ угроз и уязвимостей. Число научных публикаций — 99. asbasan@sfedu.ru; улица Чехова, 2, 347922, Таганрог, Россия; р.т.: +7(988)537-0968.

Абрамов Евгений Сергеевич — канд. техн. наук, доцент, заведующий кафедрой, кафедра безопасности информационных технологий, Южный федеральный университет. Область научных интересов: технологии обнаружения сетевых атак, модели атак, технологии threat intelligence, применение методов искусственного интеллекта в информационной безопасности. Число научных публикаций — 80. abramoves@sfedu.ru; улица Чехова, 2, 347922, Таганрог, Россия; р.т.: 7(863)371-905.

Поддержка исследований. Исследование выполнено за счет гранта Российского научного фонда № 22-11-00184, https://rscf.ru/project/22-11-00184/.

DOI 10.15622/ia.21.6.8

E. BASAN, O. PESKOVA, O. SILIN, A. BASAN, E. ABRAMOV

DATA GENERATION FOR MODELING ATTACKS ON UAVS FOR THE PURPOSE OF TESTING INTRUSION DETECTION SYSTEMS

Basan E., Peskova O., Silin O., Basan A., Abramov E. **Data Generation for Modeling Attacks on UAVs for the Purpose of Testing Intrusion Detection Systems.**

Abstract. Today, issues related to ensuring the safety of UAVs are very relevant. Researchers need to develop new protection methods to detect attacks in a timely manner and implement mitigation measures. The authors propose a new concept of attack detection "from inside" the UAV. The idea is to analyze the cyber-physical parameters of the UAV, which may indicate an attack, and its possible consequences. It was determined that to detect an attack and determine the consequences to which it can lead, it is necessary to control not only the initial parameters, but also the internal cyber-physical parameters of the UAV. This will allow predicting the possible consequences of an attack and taking emergency measures. A scheme of the impact of an attack on UAVs and the relationship with security incidents, built using an ontological approach, has been worked out. Two main essences of the UAV are considered - the physical and digital aspects of the UAV. Examples of chains of attacks leading to various consequences are also shown. In the review part, the analysis of methods and algorithms for detecting spoofing attacks using data generators is carried out, based on which conclusions are drawn about their advantages and disadvantages. Further, based on the experiments performed, the authors propose a method for assessing the quality of data and a method for generating anomalous data sets similar to real attack data, which can be used to develop and test methods for detecting and blocking attacks. The architecture of the experimental stand, which was used in the framework of full-scale simulation, is described. At this stand, designed to parse GPS spoofing attacks (GPS spoofing), several scenarios of a normal flight, and then several attack scenarios, were tested. Based on the results of the experiments, a method has been proposed that allows simulating the data corresponding to the attack with the required accuracy. A method for assessing the quality of fake data has also been proposed.

Keywords: data analysis, statistics, attacks, risks, UAVs.

References

1. Eldefrawy M.H., Khan M.K., Alghathbar K., Cho E.-S. Broadcast authentication for wireless sensor networks using nested hashing and the Chinese remainder theorem. Sensors. 2010. vol. 10. no. 9. pp. 8683-8695.
2. Strohmeier M., Lenders V., Martinovic I. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. IEEE Communications Surveys & Tutorials, 2015. vol. 17. no. 2. pp. 1066-1087. doi: 10.1109/COMST.2014.2365951.
3. Manesh M.R., Kaabouch N. Cyber-attacks on unmanned aerial system networks: Detection countermeasure and future research directions. Computers & Security. 2019. vol. 85. pp. 386-401.
4. Wang S., Wang J., Su C., Ma X. Intelligent detection algorithm against UAVs' GPS spoofing attack. IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS), 2020. pp. 382-389.
5. Duo B., Luo J., Li Y., Hu H., Wang Z. Joint trajectory and power optimization for securing UAV communications against active eavesdropping. China Communications. 2021. vol. 18. no. 1. pp. 88-99. doi: 10.23919/JCC.2021.01.008.

6. Wang Q., Dai H.-N., Wang H., Xu G., Sangaiah A.K. UAV-enabled friendly jamming scheme to secure industrial Internet of Things. Journal of Communications and Networks. 2019. vol. 21. no. 5. pp. 481-490. doi: 10.1109/JCN.2019.000042.
7. Zhang R., Condomines J.-P., Lochin E. A Multifractal Analysis and Machine Learning Based Intrusion Detection System with an Application in a UAS/RADAR System. Drones, 2022. vol. 6. p. 21. URL: https://doi.org/10.3390/drones6010021 (accessed 25.07.2022).
8. Condomines J., Zhang R., Larrieu N. Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. Ad Hoc Networks, 90. URL: https://doi.org/10.1016/j.adhoc.2018.09.004 (accessed 25.07.2022).
9. Talaei K.T., Ismail S., Kaabouch N. Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs. Sensors 2022, vol. 22. p. 662. URL: https://doi.org/10.3390/s22020662 (accessed 25.07.2022).
10. Aissou G., Slimane H.O., Benouadah S., Kaabouch N. Tree-based Supervised Machine Learning Models For Detecting GPS Spoofing Attacks on UAS. 2021 IEEE 12th Annual Ubiquitous Computing. Electronics & Mobile Communication Conference (UEMCON), 2021. doi: 10.1109/UEMCON53757.2021.9666744. pp. 0649-0653.
11. Aissou G., Benouadah S., El Alami H., Kaabouch N. Instance-based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022. pp. 0208-0214. doi: 10.1109/CCWC54503.2022.9720888.
12. Whelan J., Sangarapillai T., Minawi O., Almehmadi A., El-Khatib K. Novelty-based Intrusion Detection of Sensor Attacks on Unmanned Aerial Vehicles. Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 2020. pp. 23–28. doi: 10.1145/3416013.3426446.
13. Tippenhauer N.O., Pöpper C., Rasmussen K.B., Capkun S. On the requirements for successful GPS spoofing attacks. Proceedings of the 18th ACM conference on Computer and communications security, 2011. pp. 75–86
14. Kerns A.J., Shepard D.P., Bhatti J.A., Humphreys T.E. Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics. 2014. vol 31(4). pp. 617–636.
15. Basan E., Makarevich O., Lapina M., Mecella M. Analysis of the Impact of a GPS Spoofing Attack on a UAV. CEUR Workshop Proceedings, 2022. vol. 3094. pp. 6–16.
16. Park K.H., Park E., Kim H.K. Unsupervised Intrusion Detection System for Unmanned Aerial Vehicle with Less Labeling Effort. You. I. (eds) Information Security Applications. WISA 2020. Lecture Notes in Computer Science. Springer. Cham, 2020. vol 12583. URL: https://doi.org/10.1007/978-3-030-65299-9 (accessed 25.07.2022).
17. Bekmezci I., Senturk E., Turker T. Security issues in Flying Adhoc Networks (FANETs). Journal of Aeronautics and Space Technologies. 2016. vol. 9. no. 2. pp. 13-21.
18. Li C., Wang X. Jamming research of the UAV GPS/INS integrated navigation system based on trajectory cheating. 9th International Congress on Image and Signal Processing. BioMedical, Engineering and Informatics (CISP-BMEI), 2016. pp. 1113-1117. doi: 10.1109/CISP-BMEI.2016.7852880.
19. Schmidt D., Radke K., Camtepe S., Foo E., Ren M. A survey and analysis of the GNSS spoofing threat and countermeasures. ACM Computing Surveys (CSUR). 2016. vol. 48. no. 4. pp. 64-69.
20. Basan E., Basan A., Nekrasov A., Fidge C., Gamec J., Gamcová M. A Self-Diagnosis Method for Detecting UAV Cyber Attacks Based on Analysis of Parameter Changes.

Sensors 2021. 2021. vol. 21. p. 509. URL: https://doi.org/10.3390/s21020509 (accessed 25.07.2022).
21. Basan E., Basan A., Nekrasov A., Fidge C., Sushkin N., Peskova O. GPS-Spoofing Attack Detection Technology for UAVs Based on Kullback–Leibler Divergence. Drones, 2022. № 6 (1). URL: https://doi.org/10.3390/drones6010008 (accessed 25.07.2022).
22. Cunningham R.K., Lippmann R.P., Fried D.J., Garfinkel S.L., Graf I., Kendall K.R. Evaluating Intrusion Detection Systems Without Attacking your Friends: The 1998 DARPA Intrusion Detection Evaluation (Lexington Lincoln Lab: Massachusetts Institute of Technology). URL: https://scholar.google.com/scholar?q=Cunningham+RK%2C+Lippmann+RP%2C+Fried+DJ%2C+Garfinkel+SL%2C+Graf+I+and+Kendall+KR+1999+Evaluating+Intrusion+Detection+Systems+Without+Attacking+your+Friends%3A+The+1998+DARPA+Intrusion+Detection+Evaluation+%28Lexington+Lincoln+Lab%3A+Massachusetts+Institute+of+Technology%29 (accessed: 25.08.2022).
23. Tavallaee M., Bagheri E., Lu W., Ghorbani A.A. A Detailed Analysis of the KDD CUP 99 Data Set. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009. URL: https://scholar.google.com/scholar?q=Tavallaee+M%2C+Bagheri+E%2C+Lu+W+and+Ghorbani+AA+2009+A+Detailed+Analysis+of+The+KDD+CUP+99+Data+Set+2009+IEEE+Symposium+on+Computational+Intelligence+for+Security+and+Defense+Applications%2C+IEEE (accessed: 25.08.2022).
24. Uramová J., Scgeˇc P., Moravˇcík M., Papán J., Kontšek M., Hrabovsk`y J. Infrastructure for generating new ids dataset. 2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2018. pp. 603–610.
25. Nadiah N., Yusof M., Sulaiman N.S. Cyber Attack Detection Dataset: A Review // 2022 J. Phys.: Conf. Ser. 2319 012029 URL: https://iopscience.iop.org/article/10.1088/1742-6596/2319/1/012029 (accessed: 25.08.2022).
26. Martins N., Cruz J.M., Cruz T., Abreu P.H. Adversarial machine learning applied to intrusion and malware scenarios: a systematic review. IEEE 2020. vol. 8. pp. 35403–35419. URL: https://doi.org/10.1109/access.2020.2974752 (accessed: 25.08.2022).
27. Koroniotis N., Moustafa N., Sitnikova E., Turnbull B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. Futur Gener Comput. Syst, 2019. vol. 100. pp. 779–796. URL: https://doi.org/10.1016/j. future.2019.05.041. (accessed: 25.08.2022).
28. Martins N., Cruz J.M., Cruz T., Abreu P.H. Analyzing the footprint of classifiers in adversarial denial of service contexts. Progress in artificial intelligence. Berlin: Springer International Publishing, 2019. pp. 256–67. URL: https://doi.org/10.1007/978-3-030-30244-3_2210.1007/978-3-030-30244-3_22. (accessed: 25.08.2022).
29. Alshaibi A., Al-Ani. M., Al-Azzawi A., Konev A., Shelupanov A. The Comparison of Cybersecurity Datasets. Data, 2022. vol. 7. p. 22. URL: https://doi.org/10.3390/data7020022 (accessed: 25.08.2022).
30. Goswami G., Agarwal A., Ratha N., Singh R., Vatsa M. Detecting and Mitigating Adversarial Perturbations for Robust Face Recognition. Int. J. Comput. Vis., 2019. vol. 127. pp. 719–742.
31. Warzynski A., Kolaczek G. Intrusion detection systems vulnerability on adversarial examples. Innov Intell Syst Appl (INISTA), 2018. URL: https://doi.org/10.1109/inista. 2018. 84662 71. (accessed: 25.08.2022).
32. Rahim R., Ahanger A.S., Khan S.M., Masoodi F. Analysis of IDS using Feature Selection Approach on NSL-KDD Dataset 2021. Raju Pal & Praveen K. Shukla (eds.),

SCRS Conference Proceedings on Intelligent Systems, 2021. pp. 475–481. URL: https://doi.org/10.52458/978-93-91842-08-6-45 (accessed: 25.08.2022).
33. Hu W. et al. AdaBoost-Based Algorithm for Network. IEEE Transactions on Systems, Man, and Cybernetics. 2008. 38(2). pp. 577–583.
34. Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). Mil Commun Inf Syst Conf (MilCIS), 2015. URL: https://doi.org/10.1109/milcis.2015.7348942. (accessed: 25.08.2022).
35. Pacheco Y., Sun W. Adversarial machine learning: A comparative study on contemporary intrusion detection datasets. August 2022 SN Computer Science. 2022. № 3(5). pp. 160–171. doi: 10.1007/s42979-022-01321-8
36. Sharafaldin I., Gharib A., Lashkari A.H., Ghorbani A.A. Towards a Reliable Intrusion Detection Benchmark Dataset. Softw. Netw. vol. 2017(1). pp. 177–200.
37. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy. 2018. vol. 1. pp. 108–116.

Basan Elena — Ph.D., Associate professor, Department of information technology security, Southern Federal University. Research interests: development and research of attack and intrusion detection technologies, abnormal behavior detection, security of robotic systems, analysis of threats and vulnerabilities. The number of publications — 99. ebasan@sfedu.ru; 2, Chekhov St., 347922, Taganrog, Russia; office phone: +7(951)520-5488.

Peskova Olga — Ph.D., Associate professor, Department of information technology security, Southern Federal University. Research interests: information security. The number of publications — 206. oyupeskova@sfedu.ru; 2, Chekhov St., 347922, Taganrog, Russia; office phone: +7(8634)371-905.

Silin Oleg — Student, Southern Federal University. Research interests: development and research of attack and intrusion detection technologies, incident investigation, unmanned aerial vehicles, risk assessment. The number of publications — 5. silin@sfedu.ru; 2, Chekhov St., 347922, Taganrog, Russia; office phone: +7(928)326-4256.

Basan Alexander — Ph.D., Associate professor, Southern Federal University. Research interests: development and research of attack and intrusion detection technologies, abnormal behavior detection, security of robotic systems, analysis of threats and vulnerabilities. The number of publications — 99. asbasan@sfedu.ru; 2, Chekhov St., 347922, Taganrog, Russia; office phone: +7(988)537-0968.

Abramov Evgeniy — Ph.D., Associate Professor, Head of department, Department of information technology security, Southern Federal University. Research interests: network attack detection technologies, attack models, threat intelligence technologies, application of artificial intelligence methods in information security. The number of publications — 80. abramoves@sfedu.ru; 2, Chekhov St., 347922, Taganrog, Russia; office phone: 7(863)371-905.

Acknowledgements. The research was supported by the Russian Science Foundation grant No. 22-11-00184, https://rscf.ru/project/22-11-00184/.