МЕТОДИКА ОЦЕНКИ СТЕПЕНИ ВЛИЯНИЯ НАВИГАЦИОННЫХ АТАК НА КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ

Басан Е. С.[1], Лесников А. А.[2], Михайлова В. Д.[3], Могильный А. Б.[4], Фирсова М. Г.[5]

DOI: 10.21681/2311-3456-2025-2-90-104

Целью работы *является разработка методики классификации инцидентов безопасности киберфизических систем за счет анализа степени влияния атак на ключевые компоненты системы на основе онтологических моделей.*

Метод: *для разработки методологии классификации инцидентов безопасности киберфизических систем использовался метод обнаружения аномалий на основе вычисления значения энтропии. Модель атаки была получена на основе анализа физической природы атаки и воздействия на цифровые компоненты системы. Также для определения правил классификации инцидентов использовался онтологический подход, который позволяет прогнозировать риски безопасности для киберфизической системы.*

Результаты: *проведен анализ влияния различных типов атак на киберфизические системы, атаки разделены на классы и влияние на систему по уровню последствий и воздействия и приведены к общему виду. Анализ позволил разработать модель атак на киберфизические системы, интегрирующую различные векторы реализации угроз и унифицированные пороги реагирования. Это упрощает создание корреляционных правил, поскольку критичность срабатывания напрямую зависит от степени воздействия на целевую подсистему. Дополнительно была создана методика классификации инцидентов и идентификации ключевых компонентов киберфизических систем на основе онтологического подхода, обеспечивающая прогнозирование рисков и оптимизацию конфигурации системы. Также разработаны правила для классификации деструктивных воздействий с едиными порогами срабатывания по каждому параметру, допускающие увеличение как количества параметров, так и типов значения параметра.*

Практическая значимость: *итогом работы является набор уникальных правил для классификации деструктивных воздействий с единым порогом срабатывания для каждого параметра киберфизической системы.*

Вклад каждого соавтора: *Басан Е. С. – общее руководство проектом, разработка онтологических моделей и структурной схемы предлагаемого метода обнаружения и классификации атак; Лесников А. А. – разработка структуры и механизмов подсистемы обнаружения атак и аномалий; Михайлова В. Д. – проведение анализа существующих методов обнаружения аномалий и атак в киберфизических системах; Могильный А. Б. – проведение эксперимента, анализ результатов; Фирсова М. Г. – подготовка наборов данных для проведения и анализа результатов эксперимента.*

Ключевые слова: *киберфизическая система, деструктивное воздействие, инцидент, последствия, набор атак, онтологические модели, риски, правила классификации.*

Введение

В настоящее время все большее распространение получают киберфизические системы (КФС). КФС определяется как система, в которой программные и физические компоненты тесно связаны между собой, и такая система работает автономно без прямого вмешательства человека, полагаясь на свои датчики и/или навигационную систему для определения своего местоположения в пространстве [1].

В работе [2] авторы говорят о значительном росте популярности КФС для сокращения взаимодействия между людьми и производственным процессом.

Yaacoub и другие [3] выделили ряд уязвимостей в КФС, включая слабую сетевую инфраструктуру и отсутствие систем обнаружения вторжений. Хотя в работе детально анализируются атаки на БПЛА, беспилотные автомобили и морских роботов, угрозы навигационным системам остались нерассмотренными. Параллельно авторы отмечают расширяющееся применение КФС.

В работе [4] авторы говорят о значительном росте рынка КФС. В работе также рассмотрены векторы атак на КФС, но не уделяется внимания атакам

1 Басан Елена Сергеевна, кандидат технических наук, доцент кафедры Безопасности информационных технологий им. О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета, г. Таганрог, Россия. E-mail: ebasan@sfedu.ru, ORCID 0000-0001-6127-4484.

2 Лесников Александр Александрович, ассистент кафедры Безопасности информационных технологий им. О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета, г. Таганрог, Россия. E-mail: alesnikov@sfedu.ru

3 Михайлова Василиса Дмитриевна, ассистент кафедры Безопасности информационных технологий им. О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета, г. Таганрог, Россия. E-mail: vmihaylova@sfedu.ru

4 Могильный Антон Богданович, ассистент кафедры Безопасности информационных технологий им. О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета, г. Таганрог, Россия. E-mail: mogilnyy@sfedu.ru

5 Фирсова Мария Геннадьевна, ассистент кафедры Безопасности информационных технологий им. О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета, г. Таганрог, Россия. E-mail: mshulika@sfedu.ru

на навигационные системы. Упоминание атак на системы связи присутствует только в контексте Wi-Fi, однако использование Wi-Fi для КФС на сегодняшний день не является предпочтительным.

В [5] авторы показали обширный обзор атак на КФС. Они отмечают актуальность атак на системы глобального позиционирования, в особенности на КФС.

КФС функционирует в условиях неопределённости, что делает анализ и классификацию угроз критически важными. Система должна не только точно определять причину инцидента и прогнозировать его последствия, но и оперативно выбирать план реагирования. В традиционных информационных системах для этого используют Security Information and Event Management (SIEM) системы, собирающие данные от межсетевых экранов, антивирусов и систем обнаружения вторжений, а также выявляющие взаимосвязи между событиями с помощью корреляционных правил [6, 7].

Однако в КФС такой подход может быть неэффективным: во-первых, корреляционные правила настраиваются вручную, как и реакция на инциденты; во-вторых, в КФС часто отсутствуют стандартные средства защиты и источники оповещений. Главная проблема – необходимость мгновенного реагирования, поскольку даже незначительный инцидент способен нарушить работу всей системы.

Именно поэтому разработка системы управления инцидентами безопасности для КФС является актуальной задачей, при этом необходимо правильно определять и классифицировать события. Так как КФС включает в себя довольно широкий спектр реализаций, в данной работе будет акцентировано внимание на беспилотных автоматизированных системах (БАС).

Большинство работ на тему обнаружения атак или аномальных событий в БАС сосредоточены на атаках подмены сигнала GPS (Global Positioning System). Meng и другие предложили метод обнаружения атак в группе БАС на основе анализа характеристик сигнала GPS [8]. Для этого используются данные местоположения в трехмерном пространстве с применением модели взаимного расположения БАС, что является одной из ключевых основ для сбора информации. Обнаружение атак состоит в перекрестной проверке данных о местоположении БАС.

В работе [9] был предложен нейросетевой метод обнаружения подмены сигнала GPS, использующий 36 параметров сигнала (координаты, скорость, точность позиционирования и др.). Метод идентифицирует пять классов атак, угрожающих конфиденциальности, целостности и доступности БАС. Авторы предлагают оценивать изменения состояния системы с помощью временных вероятностных автоматов, однако подход ограничен жесткими пороговыми значениями, заданными на основе эталонных данных о нормальной работе системы.

В [10] авторы разработали систему безопасности для БАС в аграрной сфере. Модель угроз учитывает злонамеренные действия, направленные на срыв работы БАС и фальсификацию данных. Исследователи рассмотрели атаки, включая распределенный отказ в обслуживании, несанкционированный доступ, подбор пароля и компрометацию сети. Для сбора информации предлагается использовать брокера и fog-платформу, агрегирующую данные с датчиков. Обнаружение вторжений основано на датасете CICIDS2017, содержащем параметры сетевого трафика: длительность сессии, тип протокола, IP-адреса, порты, объём переданных пакетов и байт.

Nayfeh и др. используют в своей работе машинное обучение для обнаружения и классификации атак подмены GPS на БАС [11]. В исследовании использовались статические и динамические атаки для сбора и стандартизации параметров GPS-сигналов, пригодных для обучения моделей. Результаты показали точность обнаружения >92 %, уровень пропущенных атак ≤13 % и ложных срабатываний ≤4 % при времени реакции <1 мс.

Однако методы на основе нейросетей требуют качественных данных для обучения, а некоторые классы угроз сложно различимы. Кроме того, необходимо точно сопоставлять типы атак с их последствиями. Нейросети эффективны лишь на этапе классификации при известных начальных условиях. Также важно учитывать влияние искусственного шума и различия в датчиках КФС, которые могут искажать результаты.

В данной работе проведен детальный анализ характеристик КФС и их динамики при различных атакующих воздействиях. Основная задача заключалась в установлении взаимосвязей между компонентами КФС, их функционированием и видами внешних воздействий для улучшения точности распознавания угроз. Особое внимание уделено изучению атак на навигационные системы: определены их разновидности, а также выявлены причинно-следственные связи между начальным воздействием и результирующими последствиями. Зачастую одни и те же наборы параметров подвергаются воздействию со стороны разных типов атак. Тогда различить классы атак становится сложнее. При этом разный тип атаки может в разной степени изменять параметр, в рамках данного исследования планируется выявить зависимости между типами атак и уровнями их влияния на систему. В сущности, разные атаки могут схожим образом влиять на параметры, группы параметров. В данном исследовании предлагается использовать уровень влияния атаки для повышения точности классификации.

1. Разработка модели атак на КФС

1.1. Натурная модель КФС

Для определения типов атак на КФС была разработана полномасштабная модель системы. Анализируемая в данной работе модель включает в себя систему связи, панель управления оператора, аппаратную и программную модели (рис. 1).

Система связи использует два частотных канала: для телеметрии и команд управления. Для обмена данными между программой управления и автопилотом Pixhawk применяется протокол MAVLink [12,13], а для взаимодействия с оператором и между модулями – MQTT по модели издатель-подписчик [14].

Автопилот имеет набор топиков (тем), через которые он публикует обновления показаний датчиков с помощью модуля uORB [15].

В рамках данной работы КФС использует глобальную навигационную систему для позиционирования (GPS) в сочетании с ГЛОНАСС [16]. Кроме того, используется инерциальный измерительный блок

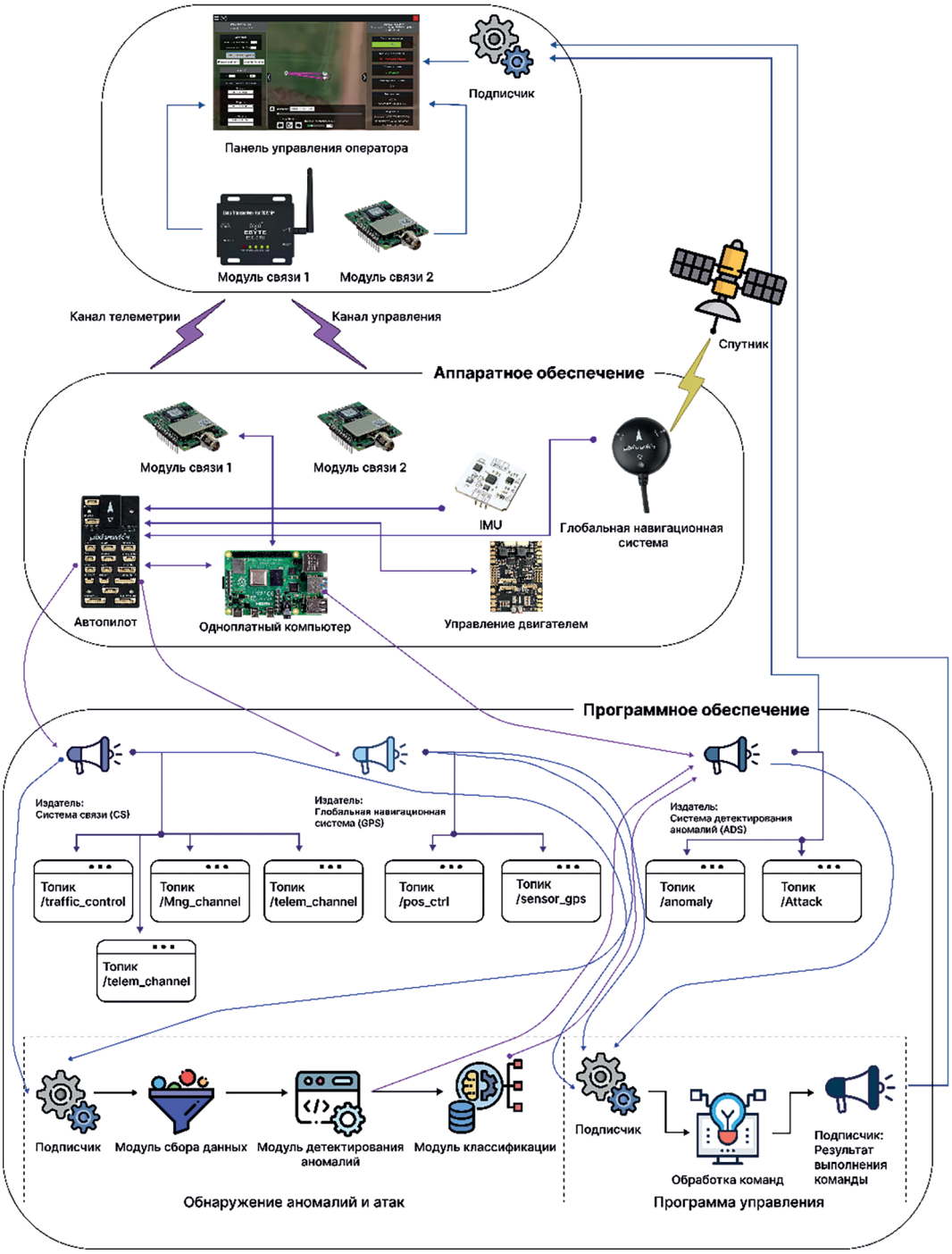

Рис. 1. Архитектура модели КФС

(IMU), включающий акселерометр, барометр, гироскоп и компас [17].

В программную модель включены только топики и наборы данных, которые могли бы сигнализировать об атаке. Программная модель также включает модуль анализа атак, который работает на основе поиска аномалий. Для каждого анализируемого параметра обнаруживается аномалия, и на основе этого делается первое предположение о проблеме. Далее на основе правил корреляции определяется конкретный тип воздействия. Прослойкой между оператором, полетным контроллером и модулем анализа атак является управляющая программа. Модуль анализа атак, в свою очередь, также публикует информацию об обнаруженных аномалиях и атаках.

1.2. Модель аномалий и атак для КФС

При создании технологии обнаружения атак необходимо обеспечить классификацию различных видов атак и последствий. Проводится анализ актуальных векторов атак для объекта оценки безопасности (КФС в данном случае), в частности для навигационной системы и системы управления.

В данной работе рассматриваются активные атаки, то есть такие, которые могут нарушить целостность и доступность системы. Активные атаки способны вызывать различные последствия для КФС, от незначительных отклонений до полной потери работоспособности. Для КФС были выделены четыре типа последствий, которые могут наступить в результате реализации активной атаки:

1. Блокирование – полная дестабилизация работы подсистем и потеря контроля над объектом, приводящие к ее разрушению;
2. Дестабилизация – нарушение ключевых функций, вызывающее сбои в работе или невыполнение отдельных задач объектом;
3. Нарушение – незначительные отклонения параметров от нормы без критических последствий;
4. Допустимые колебания – естественные отклонения, вызванные ошибками модулей или внешними факторами, не влияющие на работоспособность.

Внешние воздействия описываются n-мерным вектором признаков:

$$d_i = F(di, a, w, t, i_{di}, n_i, p_i), \quad (1)$$

где d_i – n-мерный вектор различных типов аномалий, которые могут быть оказаны на объект оценки, определенный в пространстве DI^n; а – r-мерный вектор набора атак, принимающий значения из множества A^r; w – m-мерный вектор набора погодных условий и состояний окружающей среды, влияющих на систему, принимающий значения из множества W^m; t – период времени, в течение которого было обнаружено деструктивное воздействие; i_{di} – тип воздействия, принимающий значение из множества I; n_i – набор параметров системы, затронутой атакой; p_i – набор параметров для реализации атаки [18].

В исследовании используется онтологический подход для моделирования взаимосвязей между типами кибератак, их потенциальными последствиями и элементами защищаемой системы. Этот метод обеспечивает формальное представление сложных взаимозависимостей между различными категориями объектов безопасности. В рамках исследования были определены классы атак на систему и классы подсистем объекта оценки безопасности, взаимосвязи между которыми устанавливались через характер оказываемого воздействия (рис. 2).

Схема описывает методы реализации атак и степени их влияния на подсистемы КФС. Кроме того, это позволяет понять, как можно снизить риски безопасности, изменив конфигурацию КФС. Слева показаны две основные категории атак: атаки подмены, которые сохраняют работоспособность системы, но изменяют ее поведение в интересах злоумышленника, и атаки глушения, направленные на блокировку нормального функционирования системы. Злоумышленник может намеренно отключить систему, чтобы при её повторном запуске имитировать легитимный источник управления, получая таким образом несанкционированный контроль над её функционированием. Атаки глушения особенно эффективны против систем без резервных каналов и избыточных подсистем, которые находятся под прямым управлением оператора - такие системы на схеме выделены фиолетовым цветом. Подверженные дестабилизации системы показаны оранжевыми прямоугольниками справа на рис. 2.

Схема на рис. 2 и схема на рис. 3 были модифицированы на основе предыдущих исследований [19]. Помимо целей атаки необходимо учитывать факторы ее реализации.

Ранее классификация атак с подменой навигационных сигналов была представлена в [20], где были рассмотрены три типа атак: атака повтора (злоумышленник записывает спутниковый сигнал, а затем ретранслирует его с усилением или задержкой), асинхронные и синхронные атаки подмены GPS. Асинхронные атаки просты в реализации и не требуют от злоумышленника дополнительных знаний и навыков. Атака заключается в усилении сигнала злоумышленника с целью перекрыть сигнал жертвы. Эффективность атаки зависит от точности имитации характеристик сигнала, в частности кода псевдослучайного шума (PRN) [21]. Поэтому необходимо сначала заглушить настоящий сигнал глобальной навигационной спутниковой системы (GNSS), а затем

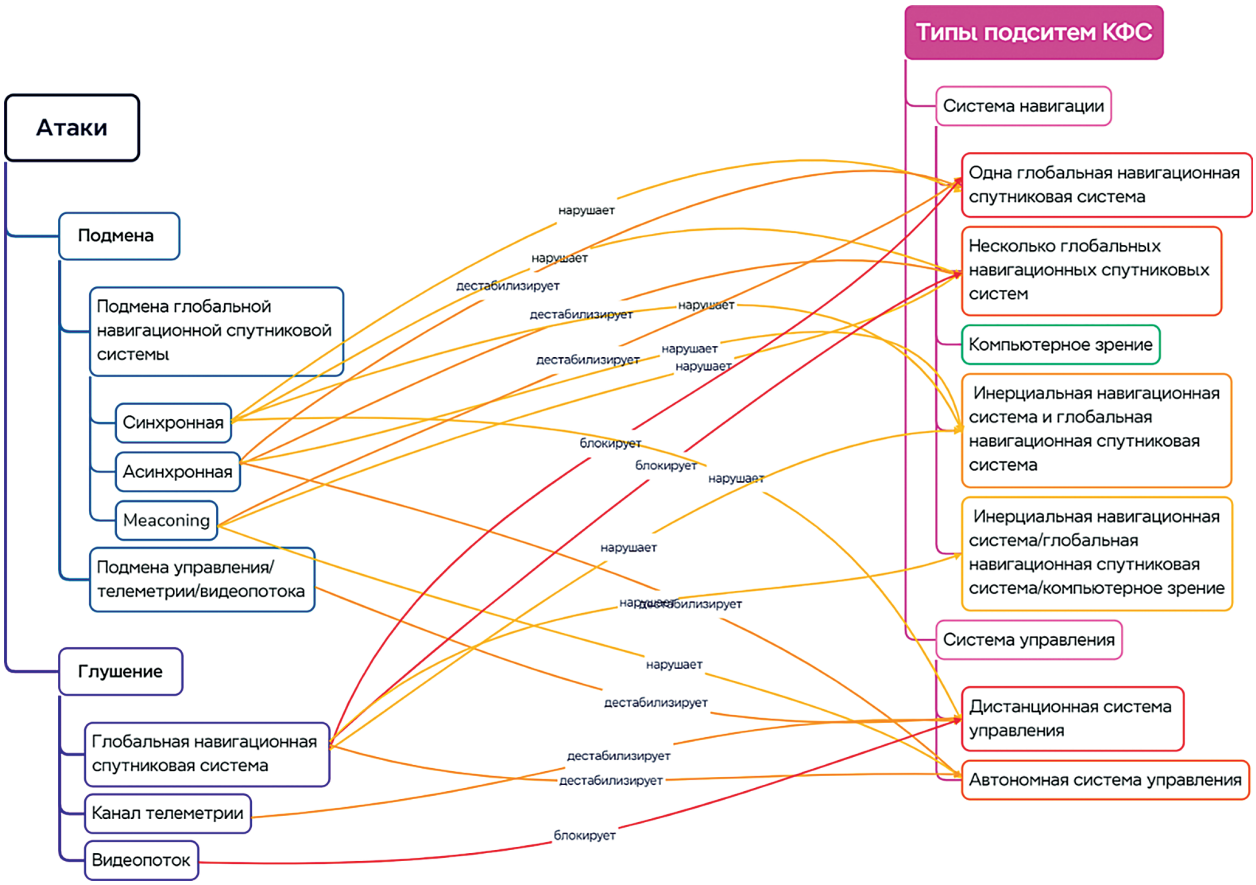

Рис. 2. Онтологическая модель взаимосвязей между атаками и подсистемами КФС

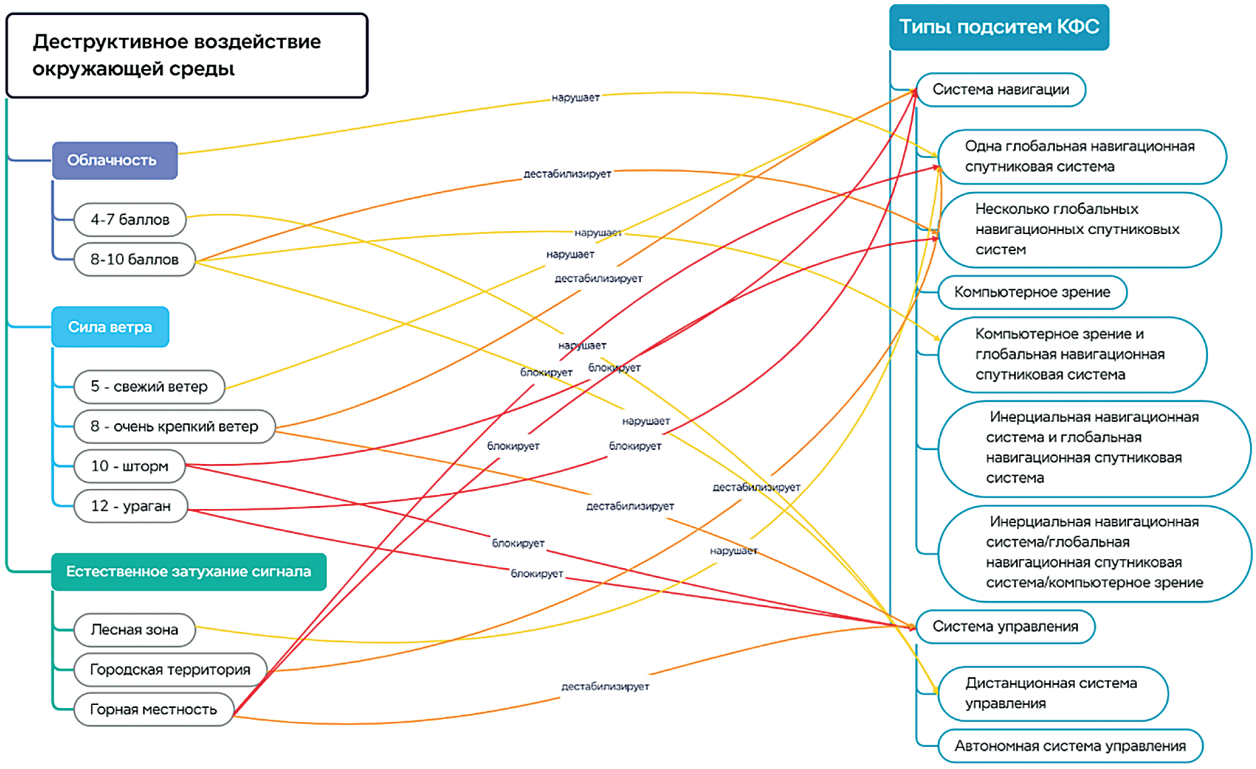

Рис. 3. Влияние факторов окружающей среды на подсистемы КФС

подменить его искусственно сгенерированным, чтобы обмануть приёмное устройство. Поддельный сигнал формируется следующим образом:

$$y(t) = Re\left\{\sum_{i=1}^{n}\sqrt{P_{si}}\,D_{si}(t-\tau_{si}(t))\,C_i(t-\tau_{si}(t))\,e^{i[2\pi f_c t-\varphi_{si}(t)]}\right\}, \quad (2)$$

где i – номер спутника GPS, a = 1, 2, ..., 32; P_{si} – амплитуда ложного сигнала; D_{si} – бит данных или сообщений ложного сигнала; $\tau_{si}(t)$ – задержка кода (из-за передачи сигнала от спутника к приемнику) ложного сигнала; $C_i(t)$ – код распределения ложного сигнала (часто это PRN-код двоичной фазовой манипуляции (BPSK) или PRN-код двоичной смещенной несущей (BOC)); $\varphi_{si}(t)$ – фазовый шум несущей ложного сигнала.

Для проведения эффективной асинхронной атаки необходимо сначала нарушить отслеживание получателем подлинных сигналов. В результате мощность генерируемых сигналов в фазовом центре антенны приемника на 40–50 дБ выше, чем у подлинных спутниковых сигналов.

Синхронная атака предполагает плавную подмену легитимного сигнала ложным без обнаружения жертвой. В отличие от асинхронной, она реализуется в два этапа:

1. Начальная фаза – передача слабого сигнала, имитирующего легитимный;
2. Основная фаза – постепенное увеличение мощности ложного сигнала (минимум на 4 дБ выше оригинала).

Ключевой особенностью является синхронизация фаз кода $\tau_{s1}(t)$,..., $\tau_{sNs}(t)$, обеспечивающая незаметный переход приемника на поддельный сигнал. Поддельные фазы несущей $\varphi_{s1}(t)$,..., $\varphi_{Nss}(t)$ обычно проектируются так, чтобы они менялись согласованно с фазами поддельного кода, так что $\omega c[\tau_{si}(tb) - \tau_{si}(ta)] = [\varphi_{si}(tb) - \varphi_{si}(ta)]$ для любых двух значений времени ta и tb и для каждого поддельного сигнала i.

Атака повтора предполагает запись и последующее воспроизведение навигационных сигналов. В результате приемник вычисляет координаты, скорость и время (PVT), соответствующие местоположению передатчика злоумышленника, но с учетом временного смещения [22].

Таким образом, с точки зрения модели подмены сигнала навигации данную атаку можно определить следующим образом:

$$a_{gi} = H_1(N_i, P_{si}, G_i, D_{si}, \tau_{si}, \varphi_{si}, i_{di}, PVT_{si}, CH_{si}, t), \quad (3)$$

$$a_m = H_2(N_i, P_{mi}, G_i, C_{mi}, PVT_i, t), \quad (4)$$

где a_{gi} – n-мерный вектор признаков атаки подмены навигационного сигнала; H_1 –функция, описывающая изменение этих параметров относительно друг друга; N_i – тип нарушителя, осуществляющего атаку; P_{si} – мощность поддельного сигнала; G_i – коэффициент усиления передающей антенны; i_{di} – тип воздействия, принимающий значения из набора I; PVT_{si} – положение, скорость и время приема; CH_{si} – количество поддельных каналов.

Атака с постановкой помех основана на передаче более мощного сигнала, совпадающего по частоте с легитимным. Чаще всего для этого применяют частотную модуляцию непрерывной волны. Эффективность глушения (мощность J) обратно пропорциональна расстоянию r до цели. Эффективность помех оценивается отношением плотности несущих к шуму C/N_0:

$$(C/N_0)_{eff} = \frac{1}{\frac{1}{(C/N_0)} + \frac{J/S}{QR_C}} = J_{eff}, \quad (5)$$

где $(C/N_0)_{eff}$ – эффективное отношение несущей к шуму; J/S – отношение мощности помехи к мощности сигнала на приемнике; Q – параметры спектрального распределения внешнего радиоизлучения относительно спектра полезного сигнала (Q = 2,22 для широкополосной гауссовой помехи); R_C – базовая скорость кода псевдослучайного шума (PRN) в чипах в секунду.

При постоянной передаваемой мощности источника глушения J_t принимаемая мощность глушения $J(r)$ увеличивается с уменьшением расстояния до объекта r в соответствии с уравнением потерь в свободном пространстве, когда источник глушения движется к приемнику:

$$J(r) = J_t\left(\frac{c}{4\pi rf}\right)^2, \quad (6)$$

где f – частота источника глушения, c – скорость света. Уравнение (6) показывает зависимость мощности источника глушения от расстояния до объекта глушения. Поскольку расстояние находится в знаменателе, то при его увеличении принимаемая мощность источника глушения будет уменьшаться.

Анализ приведенных выше формул показывает, что уровень сигнала несущей снижается по мере возникновения помех, отношение сигнал/шум (SNR) также уменьшается, а следовательно, точность позиционирования ухудшается вплоть до полной потери.

При идеальных условиях мощность, принимаемая антенной объекта P_r в децибелах (что, следовательно, помогает оценить эффективность глушения атаки), может быть найдена:

$$P_r = P_t + G_t + G_r + 20\log\frac{\lambda}{4\pi r}, \quad (7)$$

где P_t – передаваемая мощность; G_t – коэффициент усиления передающей антенны; G_r – коэффициент усиления приемной антенны; λ – длина волны несущей.

Определение модели атак с использованием помех будет выглядеть следующим образом:

$$a_j = H_3\,(N_i,\, P_{ji},\, G_{ji},\, i_{di},\, J_{eff},\, r,\, CH_{ji},\, t), \qquad (8)$$

где a_j – n-мерный вектор признаков атаки подмены навигационного сигнала; H_3 – функция, описывающая изменение заданных параметров относительно друг друга; N_i – тип нарушителя, осуществляющего атаку; P_{ji} – мощность сигнала помехи; G_{ji} – коэффициент усиления антенны; i_{di} – тип воздействия, принимающий значения из множества I.

Граф связности модели атаки показан на рис. 4. Данный граф позволяет описать вектор атаки с точки зрения злоумышленника, оценить то, на какие параметры воздействует нарушитель.

На рис. 2 показаны наиболее уязвимые комбинации подсистем КФС. Помимо кибератак, на работу системы воздействует окружающая среда. В естественной среде КФС весьма уязвима к движущимся и неподвижным препятствиям, а также к погодным условиям. Поэтому были рассмотрены факторы окружающей среды, которые могут повлиять на КФС. На примере БПЛА (рис. 3) проанализируем влияние природных факторов на функционирование КФС.

1.3. Методика оценки влияния навигационных атак на КФС

Для того чтобы определить наборы параметров, необходимые для обнаружения воздействия на навигационные подсистемы и систему связи КФС, набор параметров должен быть универсальным для большинства КФС.

Различные типы атак оказывают различное воздействие на КФС. Как показано на рис. 2, глушение навигационного сигнала полностью блокирует работу ГНСС, тогда как его подмена приводит лишь

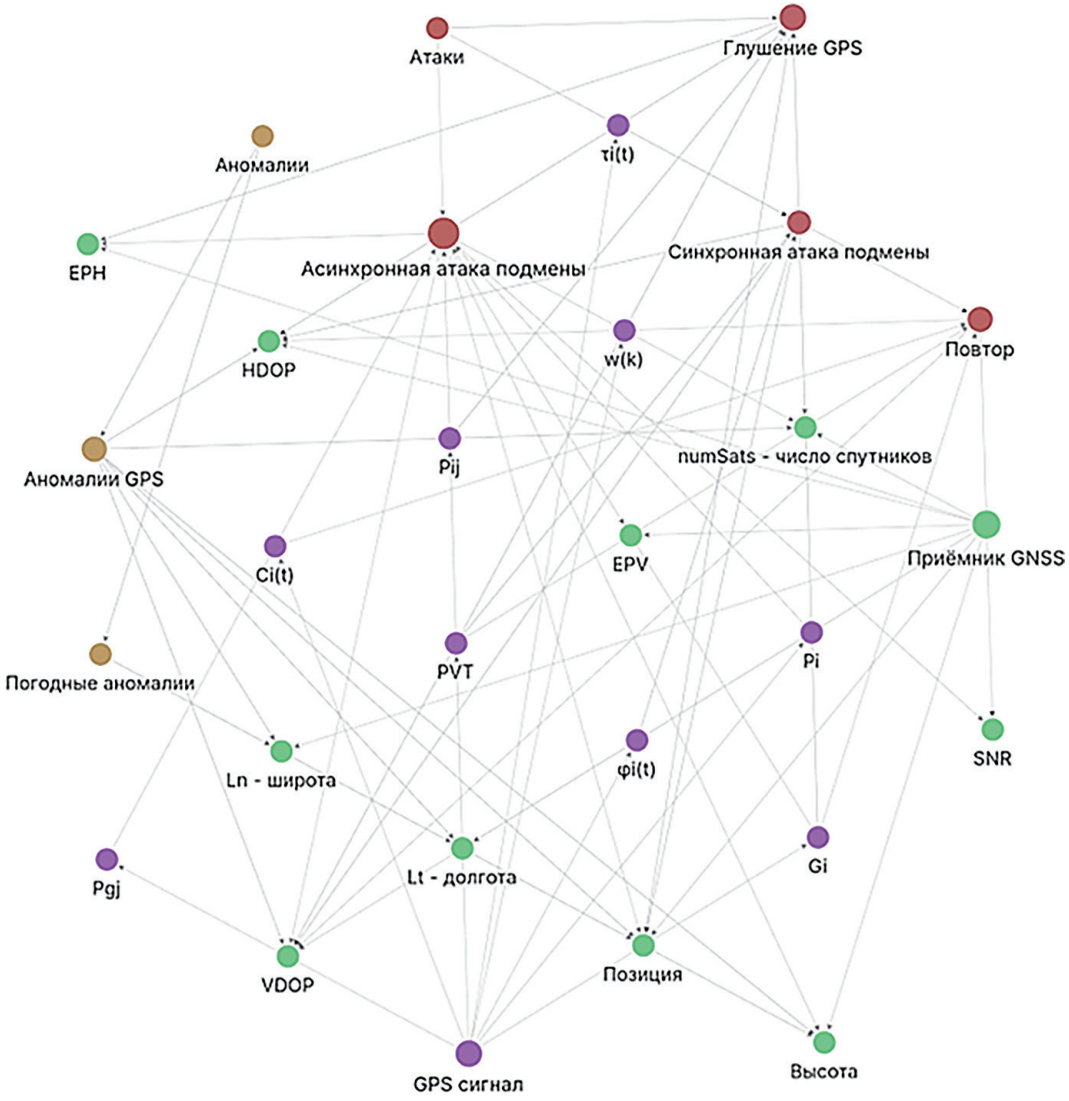

Рис. 4. Граф, связывающий атаки и аномалии с параметрами сигнала глобальной навигационной системы

к дестабилизации системы. Кроме того, природные факторы, такие как ветер и облачность, также способны нарушать функционирование навигационных систем.

Для оценки этих воздействий разработан метод, основанный на анализе изменений ключевых параметров системы. Каждому типу воздействия соответствует уникальный вектор параметров, отражающий степень его влияния. Предложенные корреляционные уравнения, верифицированные экспертами и подтвержденные экспериментально, позволяют классифицировать характер воздействия путем сопоставления наблюдаемых изменений параметров с эталонными векторами.

Данный подход обеспечивает точную идентификацию угроз за счет комплексного анализа реакции системы на внешние воздействия различной природы. С помощью теории множеств были формализованы онтологические схемы и получены итоговые выражения, как показывают равенства (9)–(15):

$$JNS = B \cap \{GNSS\}, \quad (9)$$

$$SNS = D \cap \{GNS\}, \quad (10)$$

$$CA = (A \cap \{pos_{ctrl}\}), \quad (11)$$

$$CH = (A \cap \{pos_{ctrl}\}) \cup (A \cap \{CS\}) * (A \cap \{satellites_{used}\}), \quad (12)$$

$$N = (A \cap \{pos_{ctrl}\}) \cup (A \cap \{CS\}) \cap (A \cap \{jamming_{indicator}\}) \cap (A \cap \{noise\}), \quad (13)$$

$$WA = (A \cap \{pos_{ctrl}\}), \quad (14)$$

$$WH = (V \cap \{pos_{ctrl}\}), \quad (15)$$

где JNS – атака глушения навигационного сигнала; B – блокирующий тип воздействия; $GNSS$ – набор параметров, связанных с глобальной навигационной спутниковой системой; $telem_{channel}$ – количество параметров, связанных с качеством передачи данных по каналу телеметрии; pos_{ctrl} – количество параметров, связанных с управлением положения; D – тип воздействия дестабилизации; SNS – атаки подмены навигационного сигнала; V – тип воздействия нарушения; CA – облачность в диапазоне 60–79 %; A – допустимый тип воздействия; CH – облачность в диапазоне 80–100 %; N – тип техногенного деструктивного воздействия; WA – скорость ветра в диапазоне 5–9,9 м/с; WH – скорость ветра в диапазоне 10–18 м/с.

Анализ степени воздействия угроз или факторов среды осуществляется путём исследования изменений в информационных рядах параметров. В работе применён стандартный метод энтропийной оценки, позволяющий количественно определять различия между нормализованными наборами данных. Данный подход, описанный в исследованиях [23, 24], обеспечивает объективную оценку внешних воздействий на систему. Концептуальная схема метода обнаружения и классификации атак представлена на рис. 5.

Пороги обнаружения атак формировались с учетом онтологической модели с заданными интервалами воздействия и анализа нормализованных энтропийных показателей, где рост значения энтропии прямо коррелирует с уровнем аномалии в параметрических рядах. Эти пороги можно нормализовать независимо от размерности параметров:

$$A: n_i \le 0{,}04V: 0{,}04 < n_i \le 0{,}1D: 0{,}1 < n_i \le 1B: n_i > 1. \quad (16)$$

Во-вторых, проведено моделирование, позволяющее оценить зависимость интенсивности атаки от степени изменения параметров.

2. Экспериментальное подтверждение

Эффективность метода обнаружения атак и аномалий для КФС проверялась на экспериментальном стенде в виде квадрокоптера, который подвергался как природным воздействиям, так и искусственно созданным кибератакам

В данной работе рассматривается только злоумышленник со средним потенциалом, который способен осуществлять простые сценарии атак против одной навигационной системы.

Рис. 5. Метод обнаружения и классификации атак

Сценарий 1. КФС выполняет движение в режиме миссии. Атака не проводится. Во время выполнения полетной миссии скорость ветра составляет не менее 2 м/с. Данный сценарий проверяет наличие нормальных колебаний параметров движения КФС, которые могут быть вызваны погодными условиями. В этом случае миссия выполняется с допустимыми колебаниями параметров движения.

Сценарий 2. КФС выполняет движение в режиме миссии. Проводится синхронная атака для подмены навигационного сигнала. Во время выполнения миссии скорость ветра составляет не более 2 м/с. В этом случае задание КФС выполняется с неприемлемыми колебаниями параметров движения [25].

Сценарий 3. КФС движется в режиме миссии. Проводится атака подмены асинхронного навигационного сигнала. Во время выполнения задания скорость ветра составляет не более 2 м/с. В ходе выполнения сценария проверяется сильное изменение параметров движения КФС, которое вызвано асинхронной атакой. В этом случае задание не выполняется, и КФС выходит из строя [25].

Сценарий 4. КФС выполняет движение в режиме миссии. Проводится атака глушения навигационного сигнала. Во время выполнения задания скорость ветра составляет не более 2 м/с. В этом случае задание не выполняется, и КФС терпит крушение [25].

Эксперимент проводился в полевых условиях вдали от городской застройки с использованием оборудования, описанным в разделе 1.1. Бортовой компьютер – Raspberry Pi 4 (8 ГБ ОЗУ) с флэш-картой, где записаны программные модули. Наземный модуль управления, развернутый на ноутбуке, обеспечивал передачу заданий и мониторинг.

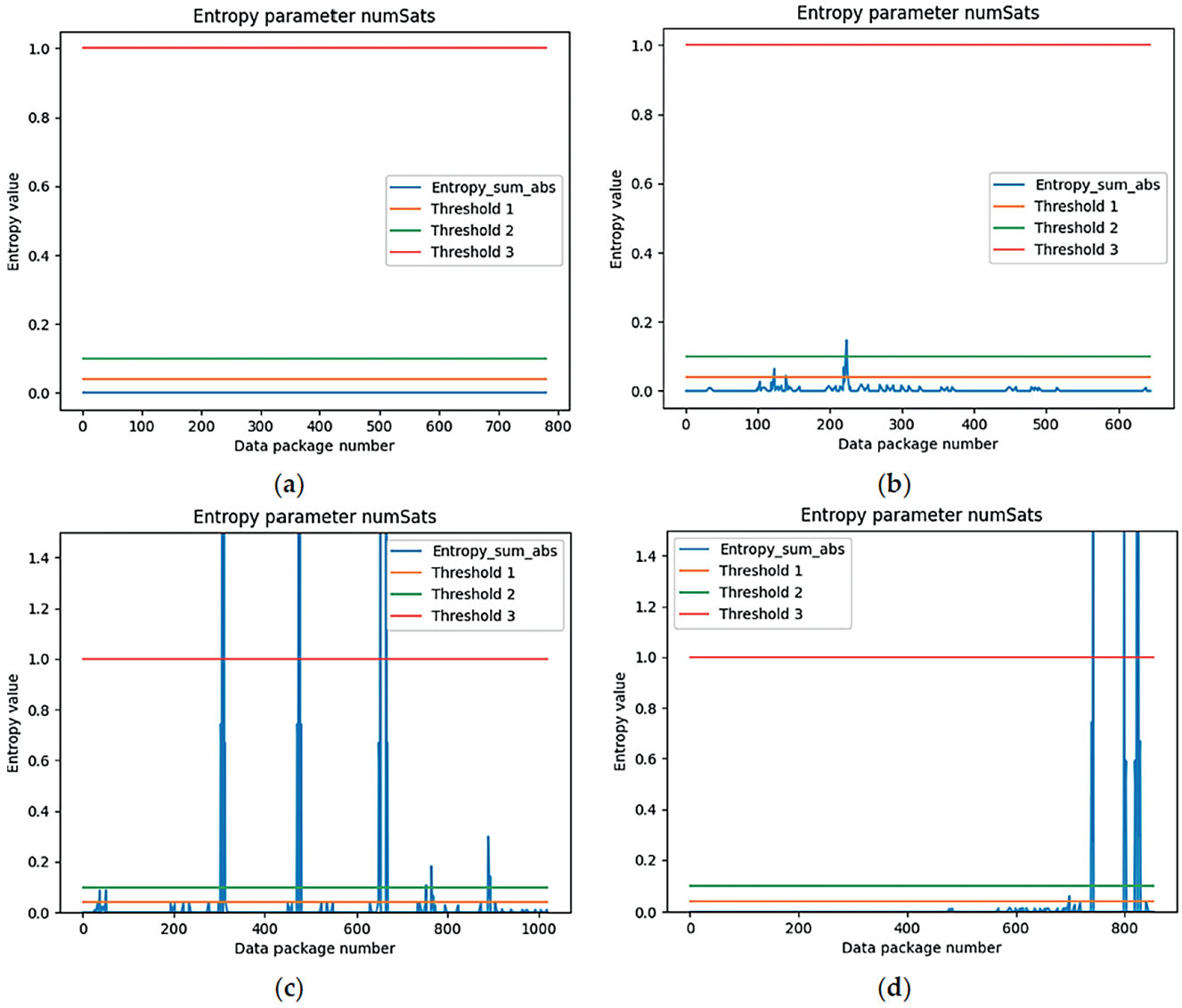

Рис. 6. Изменения значений энтропии количества спутников GPS во время (a) сценария 2; (b) сценария 2; (c) сценария 3; и (d) сценария 4

Задание объекта состояло из четырех ключевых точек маршрута, нарушитель находился между точками 1 и 2.

Синхронная атака обеспечивает плавное отклонение КФС от маршрута, при этом злоумышленник остается незамеченным, тогда как асинхронная вызывает резкое отключение от спутников, делая атаку более заметной.

Для оценки воздействия анализировались координаты (широта/долгота) и рассчитанное смещение КФС между измерениями.

Смещение определялось как геодезическое расстояние (в метрах) между последовательными координатами по модели Земли Всемирной геодезической системы 1984 (WGS 84), что обеспечило более точную оценку воздействия по сравнению с анализом отдельных координат.

Для анализа собранных данных из журналов для каждого сценария рассчитывалось значение энтропии и оценивался каждый параметр (рис. 6).

Для оценки воздействия атак анализировалось изменение пространственного положения КФС. Исходные координаты (широта/долгота) дополнялись расчетом величины смещения между последовательными измерениями (рис. 7), что позволило получить более информативную метрику влияния атак.

Далее выбиралось максимальное значение энтропии и для каждого параметра строились графики с оценкой пересечения уровней отклика, как показано на рис. 8, для параметра отношение сигнал/шум (*SNR*). Глушение позволяет снизить *SNR* на приемнике, поскольку легитимные сигналы отключаются и остается только шум, поэтому график выглядит достаточно однородным. При атаках любого типа

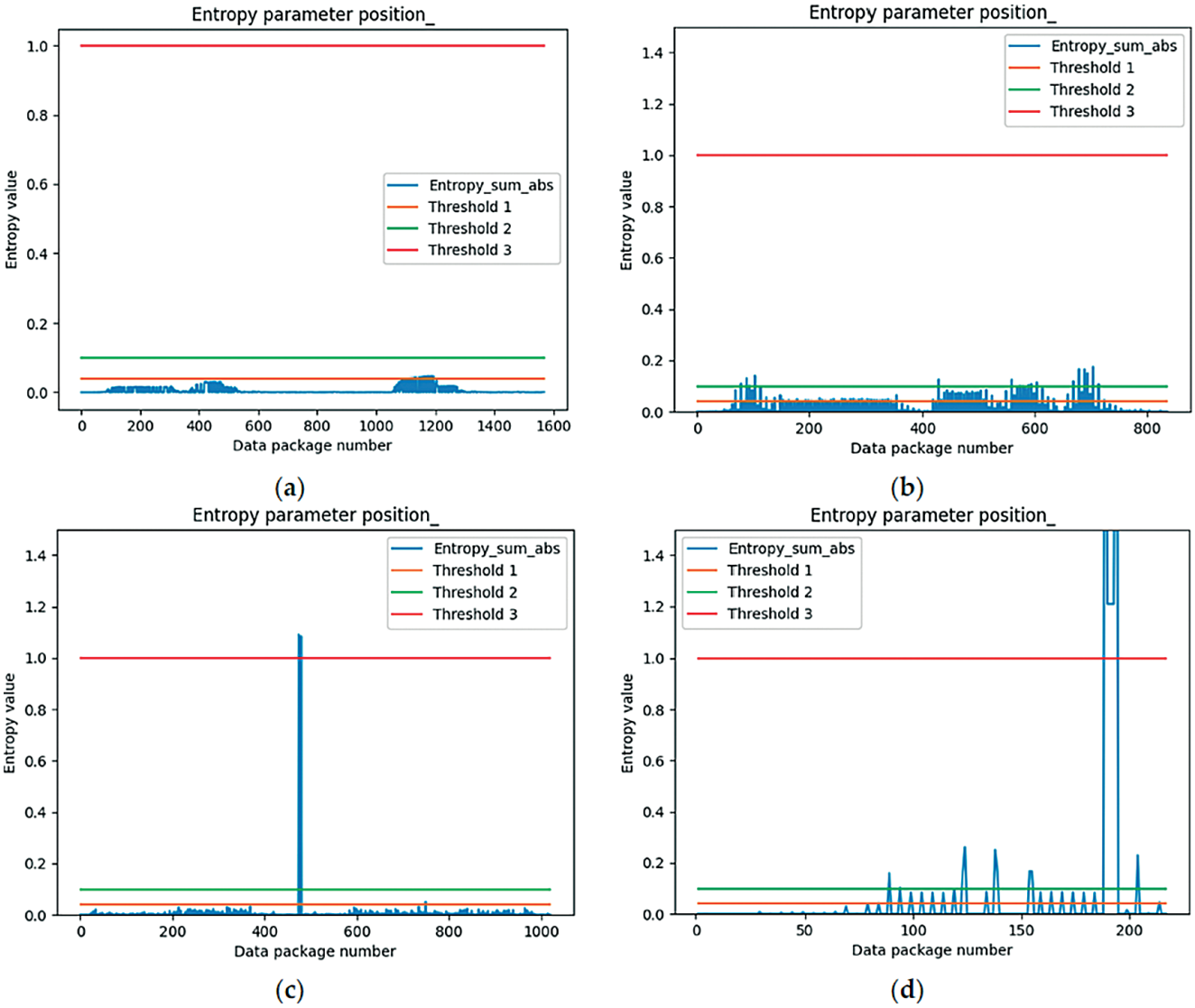

Рис. 7. Изменения значений энтропии параметра смещения во время (a) сценария 1; (b) сценария 2; (c) сценария 3; и (d) сценария 4

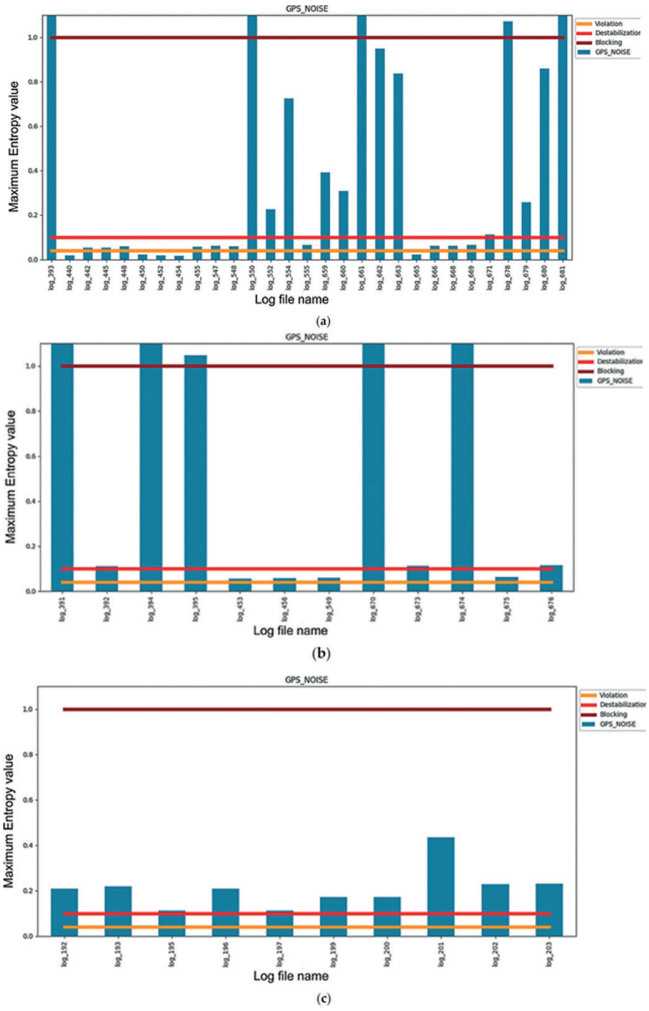

Рис. 8. Изменения в показателях энтропии SNR параметра в соответствии с (a) сценарием 2; (b) сценарием 3 и (c) сценарием 4

злоумышленнику необходимо обеспечить доминирование своего сигнала над легитимным. Однако при синхронной атаке подмены мощность сигнала увеличивается постепенно, избегая резкого перехвата, что подтверждается анализом логов.

Значения стандартного отклонения горизонтальной ошибки положения (EPH) и стандартного отклонения вертикальной ошибки положения (EPV) рассчитываются полетным контроллером на основе среднеквадратичных значений горизонтального разбавления точности ($HDOP$) и вертикального разбавления точности ($VDOP$). Эти параметры используются в прошивке полетного контроллера для оценки качества сигналов.

Как говорилось ранее, глушение снижает отношение сигнал/шум на приемнике, поскольку легитимные сигналы отключаются и остается только шум, поэтому график выглядит достаточно однородным. В результате были детализированы правила корреляции для выявления следующих случаев воздействия на КФС:

$$Async = (hdop \geq B) \cap (vdop \geq B) \cap (numSats \geq B) \cap \cap ((EPH > V) \cup (EPV > V) \cap ((Position > V) \cup \cap (SNR > V)) \cap (numSats > B), \quad (17)$$

$$Sync = ((hdop \geq D) \cup (vdop \geq D)) \cap (numSat \geq V) \cap \cap ((EPH > V) \cup (EPV > V) \cup (V \leq Position < B)) \cup \cap (SNR > V), \quad (18)$$

$$Anomaly_{GPS} = (((hdop \geq D) \cup (vdop \geq D) \cap \cap ((numSat \geq V)(SNR \geq V))) \cap (EPV \geq V)) \cup \cap (Position \geq V))), \quad (19)$$

$$GPS_{Jamm} = (hdop \geq B) \cap (vdop \geq B) \cap (numSats \geq B) \cap \cap (EPH \geq D) \cap (EPV \geq V) \cap (SNR > D) \cap \cap (numSats > B) \cap (Position > D). \quad (20)$$

Предложенные правила группируют параметры по их значимости для идентификации разных типов атак: синхронные требуют срабатывания хотя бы одного позиционного параметра (плавное воздействие); асинхронным необходима активация всех параметров (резкая дестабилизация). Валидация проводилась на выборке из 10 логов каждого класса (табл. 1). Точность оценивалась по ошибкам I и II рода, а также времени обнаружения [26].

Для каждого параметра оценивалось наличие аномалии. Далее, если набор параметров перешел требуемый порог реагирования, то тип атаки определялся в соответствии с правилами классификации (9)–(15). Принимая во внимание тот факт, что было выполнено четыре типа сценариев и собраны данные по результатам сценариев, становится известно, какое влияние на КФС произошло в каком случае. Для каждого случая определялось соответствие или

Таблица 1.

Результаты тестирования правил корреляции

Сценарии	Ошибки I рода	Ошибки II рода	Время обнаружения, с	Вероятность обнаружения атаки или аномалии
Сценарий 1	0	0,01	0,25	0,99
Сценарий 2	0,03	0	0,25	0,97
Сценарий 3	0,08	0	0,25	0,92
Сценарий 4	0,1	0	0,25	0,9
Среднее значение	0,05	0,0025	0,25	0,95

несоответствие ожидаемому сценарию и вычислялись ошибки. При этом каждый параметр анализировался и оценивалась степень его изменения, а также ожидаемое изменение. Среднее время обнаружения составило 0,25 с; это связано с частотой обновления данных. Данные считывались четыре раза в секунду, чтобы обнаружить признаки воздействия при первом пакете обновлений. Ошибок второго рода практически не было, то есть не было ложных срабатываний. Это очень важно, если после классификации атаки нужно принять решение о том, как реагировать, а ложное срабатывание может привести к каким-то дополнительным ненужным действиям.

Заключение

В результате исследования были выявлены и детализированы типы атак на КФС. Определено, что атаки подмены могут по-разному влиять на КФС. Конечное влияние на параметры КФС зависит от уровня подготовки. Важным этапом создания системы классификации атак является выбор параметров для оценки, а также метода их нормализации. При использовании методов машинного обучения классы атак должны быть четко различимы. При этом асинхронные, синхронные и глушение могут перекрываться. Это связано с тем, что асинхронная атака может быть реализована посредством первоначального глушения для отключения от легитимных спутников. Важно оценить интенсивность и моменты изменения параметров, поэтому необходимо выстраивать цепочки правил корреляции. Например, асинхронная атака начнется с увеличения отношения сигнал/шум, поскольку злоумышленник пытается выдать более мощный сигнал для приемника. В результате будет наблюдаться снижение количества доступных спутников и точности позиционирования. Однако при воздействии глушителя параметр SNR не меняется кардинально, так как полезный сигнал не доходит до приемника. Как правило, параметры горизонтальной ошибки положения (EPH) и вертикальной ошибки положения (EPV) изменяются вместе с изменением положения, так как эти параметры оценивают точность позиционирования.

Важным результатом исследования является выявление наборов параметров с подсистемами КФС. Как видно из онтологических моделей, некоторые параметры пересекаются в разных подсистемах. Введение порогов реагирования и степени влияния атак на параметры позволяет разделить классы атак и аномалий. Определение правильного набора параметров для классификации является ключевой задачей, чтобы избежать избыточности и корреляции параметров. Полученные правила показывают, что, применяя степень изменения параметров, можно получить уникальный набор правил корреляции для разных типов атак, даже похожих друг на друга. В дальнейшем это можно будет использовать для оценки вероятности инцидента и типа нарушителя. Кроме того, получены единые пороги срабатывания, которые можно применять к разным параметрам, что позволяет масштабировать метод для любой подсистемы любой КФС. Унифицированные пороги срабатывания являются универсальным инструментом для анализа интенсивности атаки. Таким образом, представленные модели атак, включающие наборы параметров, которые использует злоумышленник при воздействии на объект, и полученные правила корреляции связывают начальный и конечный векторы атак на объект. Полученные результаты можно использовать для разделения разных типов деструктивных воздействий на классы для обнаружения и противодействия атакам на КФС. Основная идея заключается в том, что, добавляя фактор интенсивности или степени воздействия к описанию вектора атаки, можно более гибко разделять разные типы атак, а также прогнозировать последствия. На основе этого подхода в дальнейшем планируется разделить атаки типа «отказ в обслуживании» и определить их интенсивность и степень воздействия на систему. Внутренняя устойчивость для КФС первична. В дальнейшем также планируется ввести временной фактор. В ходе исследования также была замечена определенная согласованность в работе параметров. Добавление временного фактора позволит обнаружить атаку на ранней стадии.

Работа выполнена в рамках научно-исследовательского проекта № ВнГр/24-01-КТ «Разработка демонстрационной модели БПЛА с повышенной отказоустойчивостью».

Литература

1. Umar, A.; Giwa, M. A.; Kassim, A. Y.; Ilyasu, M. U.; Abdulwahab, I.; Agbon, E. E.; Ogedengbe, M. T. Development of an Android-Based, Voice-Controlled Autonomous Robotic Vehicle. Eng. Proc. 2023, 58, 48. DOI:10.3390/ecsa-10-16026.
2. Loganathan, A.; Ahmad, N. S. A systematic review on recent advances in autonomous mobile robot navigation. Eng. Sci. Technol. Int. J. 2023, 40, 101343. DOI:10.1016/j.jestch.2023.101343.
3. Yaacoub, J.-P. A.; Noura, H. N.; Salman, O.; Chehab, A. Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations. Int. J. Inf. Secur. 2022, 21, 115–158. DOI:10.1007/s10207-021-00545-8.
4. Elikhchi, H. D.; Hamid, T.; Akpoduado, M. Robotics cyber security issues. In Lecture Notes in Networks and Systems, Proceedings of the ICACTCE'23—The International Conference on Advances in Communication Technology and Computer Engineering. ICACTCE 2023, Bolton, UK, 24–25 February 2023; Iwendi, C., Boulouard, Z., Kryvinska, N., Eds.; Springer: Cham, Switzerland, 2023; Volume 735. DOI:10.1007/978-3-031-37164-6_15.
5. Botta, A.; Rotbei, S.; Zinno, S.; Ventre, G. Cyber security of robots: A comprehensive survey. Intell. Syst. Appl. 2023, 18, 200237. DOI:10.1016/j.iswa.2023.200237.
6. Grishaeva, S. A.; Borzov, V. I. Information security risk management. In Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, 7–11 September 2020; pp. 96–98.
7. Aleksandrova, S. V.; Vasiliev, V. A.; Aleksandrov, M. N. Problems of implementing information security management systems. In Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, 7–11 September 2020; pp. 78–81. DOI: 10.1109/ITQMIS51053.2020.9322896.
8. Meng, L.; Zhang, L.; Yang, L.; Yang, W. A GPS-adaptive spoofing detection method for the small UAV cluster. Drones 2023, 7, 461. DOI:10.3390/drones7070461.
9. Sun, Y.; Yu, M.; Wang, L.; Li, T.; Dong, M. A deep-learning-based GPS signal spoofing detection method for small UAVs. Drones 2023, 7, 370. DOI:10.3390/drones7060370.
10. Sajid, J.; Hayawi, K.; Malik, A. W.; Anwar, Z.; Trabelsi, Z. A Fog Computing Framework for Intrusion Detection of Energy-Based Attacks on UAV-Assisted Smart Farming. Appl. Sci. 2023, 13, 3857. DOI:10.3390/app13063857.
11. Nayfeh, M.; Li, Y.; Shamaileh, K. A.; Devabhaktuni, V.; Kaabouch, N. Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification. Comput. Secur. 2023, 126, 103085. DOI: 10.1016/j.cose.2022.103085.
12. N. Sabuwala and R. D. Daruwala, «Securing Unmanned Aerial Vehicles by Encrypting MAVLink Protocol», 2022 IEEE Bombay Section Signature Conference (IBSSC), Mumbai, India, 2022, pp. 1–6, doi: 10.1109/IBSSC56953.2022.10037546.
13. J. Song, H. Yuan and B. Zhang, «Pixhawk-based scalable platform for multi-purpose surface unmanned vehicle», 2022 4th International Academic Exchange Conference on Science and Technology Innovation (IAECST), Guangzhou, China, 2022, pp. 1577–1580, doi: 10.1109/IAECST57965.2022.10061960.
14. W. Wang, Y. Zhao, Y. Liu, G. Liu, F. Zheng and C. Sun, «MQTT Protocol and Implementation of Equipment Management System for Industrial Internet of Things», 2024 43rd Chinese Control Conference (CCC), Kunming, China, 2024, pp. 6139–6144, doi: 10.23919/CCC63176.2024.10662474.
15. A. Miu, L. Ruse, R. Deaconescu and D. Tudose, «Integrating TLS/SSL with MQTT in NuttX Operating System», 2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 2024, pp. 1–6, doi: 10.1109/RoEduNet64292.2024.10722675.
16. I. I. Rezvan, R. I. Vorobiev and S. V. Vorobieva, «The Accuracy Indicators Analysis of GPS and GLONASS Receivers», 2021 XV International Scientific-Technical Conference on Actual Problems Of Electronic Instrument Engineering (APEIE), Novosibirsk, Russian Federation, 2021, pp. 216–219, doi: 10.1109/APEIE52976.2021.9647658.
17. H. M. Saputra, T. Permadi, C. H. A. H. B. Baskoro, N. S. M. Nor, B. Abdussalam and M. Y. Rezaldi, «Effect of IMU Sensor Positioning on 1-DOF Angle Measurement Accuracy for Robotic Charging Station (RoCharg-v1) Manipulator», 2023 International Conference on Computer, Control, Informatics and its Applications (IC3INA), Bandung, Indonesia, 2023, pp. 96–101, doi: 10.1109/IC3INA60834.2023.10285798.
18. Basan, E. S.; Sushkin, N. A.; Babenko, L. K. Methodology for Detecting Attacks in the Context of Destructive Influences. In Proceedings of the 2023 IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE), Novosibirsk, Russia, 10–12 November 2023; pp. 1120–1124. DOI: 10.1109/APEIE59731.2023.10347616.
19. Değirmenci, E.; Kırca, Y.S.; Özçelik, ˙I.; Yazıcı, A. ROSIDS23: Network intrusion detection dataset for robot operating system. Data Brief 2023, 51, 109739. DOI:10.1016/j.dib.2023.109739.
20. Spravil, J.; Hemminghaus, C.; von Rechenberg, M.; Padilla, E.; Bauer, J. Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring. J. Mar. Sci. Eng. 2023, 11, 928.
21. Ren, Y.; Restivo, R. D.; Tan,W.; Wang, J.; Liu, Y.; Jiang, B.; Wang, H.; Song, H. Knowledge distillation-based GPS spoofing detection for small UAV. Future Internet 2023, 15, 389. DOI:10.3390/fi15120389.
22. Yang, L.; Wen, C. Optimal jamming attack system against remote state estimation in wireless network control systems. IEEE Access 2021, 9, 51679–51688. DOI:10.1109/ACCESS.2020.3046483.
23. Jung, J. H.; Hong, M. Y.; Choi, H.; Yoon, J. W. An analysis of GPS spoofing attack and efficient approach to spoofing detection in PX4. IEEE Access 2024, 12, 46668–46677. DOI:10.1109/ACCESS.2024.3382543.
24. 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, 8. DOI:10.3390/drones6010008.
25. 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, 21, 509. DOI:10.3390/s21020509.
26. Huang, X.; Tian, Y.; He, Y.; Tong, E.; Niu, W.; Li, C.; Liu, J.; Chang, L. Exposing spoofing attack on flocking-based unmanned aerial vehicle cluster: A threat to swarm intelligence. Secur. Commun. Netw. 2020, 2020, 8889122. DOI:10.1155/2020/8889122.
27. Basan, E.; Basan, A.; Nekrasov, A.; Fidge, C.; Ishchukova, E.; Basyuk, A.; Lesnikov, A. Trusted operation of cyber-physical processes based on assessment of the system's state and operating mode. Sensors 2023, Vol. 23. No. 4. 1996. DOI: 10.3390/s23041996.

METHODOLOGY FOR ASSESSING THE DEGREE OF INFLUENCE OF NAVIGATION ATTACKS ON CYBER-PHYSICAL SYSTEMS

Basan E. S.[6], Lesnikov A. A.[7], Mikhailova V. D.[8], Mogilny A. B.[9], Firsova M. G.[10]

Keywords: *cyber-physical system, destructive impact, incident, consequences, set of attacks, ontological models, risks, classification rules.*

The aim of the work *is to develop a methodology for classifying cyber-physical system security incidents by analyzing the degree of impact of attacks on key system components based on ontological models.*

Research method: *anomaly detection method based on entropy calculation was used to develop a methodology for classifying cyber-physical system security incidents. The attack model was obtained based on the analysis of the physical nature of the attack and the impact on the digital components of the system. An ontological approach was also used to determine the rules for classifying incidents, which allows predicting security risks for a cyber-physical system.*

Research results: *an analysis of the impact of various types of attacks on cyber-physical systems was carried out, attacks were divided into classes and the impact on the system by the level of consequences and impact was brought to a general form. Based on the analysis results, a model of attacks on cyber-physical systems was built, taking into account different ways of implementing an attack, and uniform attack response thresholds were defined, which allows creating universal correlation rules and simplifies this process, since the response threshold is associated with the degree of impact of the attack on the final subsystem. A methodology for classifying incidents and identifying key components of a cyber-physical system based on ontological models was developed, which allows predicting risks and selecting the optimal system configuration. Rules for classifying destructive impacts with uniform response thresholds for each parameter were also developed, while it is possible to increase both the number of parameters and the types of parameter values.*

Scientific novelty: *the result of the work is a set of unique rules for classifying destructive impacts with a uniform response threshold for each parameter of a cyber-physical system*

References

1. Umar, A.; Giwa, M. A.; Kassim, A. Y.; Ilyasu, M. U.; Abdulwahab, I.; Agbon, E. E.; Ogedengbe, M. T. Development of an Android-Based, Voice-Controlled Autonomous Robotic Vehicle. Eng. Proc. 2023, 58, 48. DOI:10.3390/ecsa-10-16026.
2. Loganathan, A.; Ahmad, N. S. A systematic review on recent advances in autonomous mobile robot navigation. Eng. Sci. Technol. Int. J. 2023, 40, 101343. DOI:10.1016/j.jestch.2023.101343.
3. Yaacoub, J.-P. A.; Noura, H. N.; Salman, O.; Chehab, A. Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations. Int. J. Inf. Secur. 2022, 21, 115–158. DOI:10.1007/s10207-021-00545-8.
4. Elikhchi, H. D.; Hamid, T.; Akpoduado, M. Robotics cyber security issues. In Lecture Notes in Networks and Systems, Proceedings of the ICACTCE'23—The International Conference on Advances in Communication Technology and Computer Engineering. ICACTCE 2023, Bolton, UK, 24–25 February 2023; Iwendi, C., Boulouard, Z., Kryvinska, N., Eds.; Springer: Cham, Switzerland, 2023; Volume 735. DOI:10.1007/978-3-031-37164-6_15.
5. Botta, A.; Rotbei, S.; Zinno, S.; Ventre, G. Cyber security of robots: A comprehensive survey. Intell. Syst. Appl. 2023, 18, 200237. DOI:10.1016/j.iswa.2023.200237.
6. Grishaeva, S. A.; Borzov, V. I. Information security risk management. In Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, 7–11 September 2020; pp. 96–98.
7. Aleksandrova, S. V.; Vasiliev, V. A.; Aleksandrov, M. N. Problems of implementing information security management systems. In Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, 7–11 September 2020; pp. 78–81. DOI: 10.1109/ITQMIS51053.2020.9322896.
8. Meng, L.; Zhang, L.; Yang, L.; Yang, W. A GPS-adaptive spoofing detection method for the small UAV cluster. Drones 2023, 7, 461. DOI:10.3390/drones7070461.
9. Sun, Y.; Yu, M.; Wang, L.; Li, T.; Dong, M. A deep-learning-based GPS signal spoofing detection method for small UAVs. Drones 2023, 7, 370. DOI:10.3390/drones7060370.
10. Sajid, J.; Hayawi, K.; Malik, A. W.; Anwar, Z.; Trabelsi, Z. A Fog Computing Framework for Intrusion Detection of Energy-Based Attacks on UAV-Assisted Smart Farming. Appl. Sci. 2023, 13, 3857. DOI:10.3390/app13063857.

6 Elena S. Basan, Ph.D. (in Tech.), Associate Professor of the Department of Information Technology Security named after O. B. Makarevich, Institute of Computer Technology and Information Security, Southern Federal University, Taganrog, Russia, E-mail: ebasan@sfedu.ru

7 Aleksandr A. Lesnikov, Assistant of the Department of Information Technology Security named after O. B. Makarevich, Institute of Computer Technology and Information Security, Southern Federal University, Taganrog, Russia, E-mail: alesnikov@sfedu.ru

8 Vasilisa D. Mikhailova, Assistant of the Department of Information Technology Security named after O. B. Makarevich, Institute of Computer Technology and Information Security, Southern Federal University, Taganrog, Russia, E-mail: vmihaylova@sfedu.ru

9 Anton B. Mogilny, Assistant of the Department of Information Technology Security named after O. B. Makarevich, Institute of Computer Technology and Information Security, Southern Federal University, Taganrog, Russia, E-mail: mogilnyy@sfedu.ru

10 Maria G. Firsova, Assistant of the Department of Information Technology Security named after O. B. Makarevich, Institute of Computer Technology and Information Security, Southern Federal University, Taganrog, Russia, E-mail: mshulika@sfedu.ru

11. Nayfeh, M.; Li, Y.; Shamaileh, K. A.; Devabhaktuni, V.; Kaabouch, N. Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification. Comput. Secur. 2023, 126, 103085. DOI: 10.1016/j.cose.2022.103085.
12. N. Sabuwala and R. D. Daruwala, «Securing Unmanned Aerial Vehicles by Encrypting MAVLink Protocol», 2022 IEEE Bombay Section Signature Conference (IBSSC), Mumbai, India, 2022, pp. 1–6, doi: 10.1109/IBSSC56953.2022.10037546.
13. J. Song, H. Yuan and B. Zhang, «Pixhawk-based scalable platform for multi-purpose surface unmanned vehicle», 2022 4th International Academic Exchange Conference on Science and Technology Innovation (IAECST), Guangzhou, China, 2022, pp. 1577–1580, doi: 10.1109/IAECST57965.2022.10061960.
14. W. Wang, Y. Zhao, Y. Liu, G. Liu, F. Zheng and C. Sun, «MQTT Protocol and Implementation of Equipment Management System for Industrial Internet of Things», 2024 43rd Chinese Control Conference (CCC), Kunming, China, 2024, pp. 6139–6144, doi: 10.23919/CCC63176.2024.10662474.
15. A. Miu, L. Ruse, R. Deaconescu and D. Tudose, «Integrating TLS/SSL with MQTT in NuttX Operating System», 2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 2024, pp. 1–6, doi: 10.1109/RoEduNet64292.2024.10722675.
16. I. I. Rezvan, R. I. Vorobiev and S. V. Vorobieva, «The Accuracy Indicators Analysis of GPS and GLONASS Receivers», 2021 XV International Scientific-Technical Conference on Actual Problems Of Electronic Instrument Engineering (APEIE), Novosibirsk, Russian Federation, 2021, pp. 216–219, doi: 10.1109/APEIE52976.2021.9647658.
17. H. M. Saputra, T. Permadi, C. H. A. H. B. Baskoro, N. S. M. Nor, B. Abdussalam and M. Y. Rezaldi, «Effect of IMU Sensor Positioning on 1-DOF Angle Measurement Accuracy for Robotic Charging Station (RoCharg-v1) Manipulator», 2023 International Conference on Computer, Control, Informatics and its Applications (IC3INA), Bandung, Indonesia, 2023, pp. 96–101, doi: 10.1109/IC3INA60834.2023.10285798.
18. Basan, E. S.; Sushkin, N. A.; Babenko, L. K. Methodology for Detecting Attacks in the Context of Destructive Influences. In Proceedings of the 2023 IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE), Novosibirsk, Russia, 10–12 November 2023; pp. 1120–1124. DOI: 10.1109/APEIE59731.2023.10347616.
19. Değirmenci, E.; Kırca, Y.S.; Özçelik, ˙I.; Yazıcı, A. ROSIDS23: Network intrusion detection dataset for robot operating system. Data Brief 2023, 51, 109739. DOI:10.1016/j.dib.2023.109739.
20. Spravil, J.; Hemminghaus, C.; von Rechenberg, M.; Padilla, E.; Bauer, J. Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring. J. Mar. Sci. Eng. 2023, 11, 928.
21. Ren, Y.; Restivo, R. D.; Tan,W.; Wang, J.; Liu, Y.; Jiang, B.; Wang, H.; Song, H. Knowledge distillation-based GPS spoofing detection for small UAV. Future Internet 2023, 15, 389. DOI:10.3390/fi15120389.
22. Yang, L.; Wen, C. Optimal jamming attack system against remote state estimation in wireless network control systems. IEEE Access 2021, 9, 51679–51688. DOI:10.1109/ACCESS.2020.3046483.
23. Jung, J. H.; Hong, M. Y.; Choi, H.; Yoon, J. W. An analysis of GPS spoofing attack and efficient approach to spoofing detection in PX4. IEEE Access 2024, 12, 46668–46677. DOI:10.1109/ACCESS.2024.3382543.
24. 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, 8. DOI:10.3390/drones6010008.
25. 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, 21, 509. DOI:10.3390/s21020509.
26. Huang, X.; Tian, Y.; He, Y.; Tong, E.; Niu, W.; Li, C.; Liu, J.; Chang, L. Exposing spoofing attack on flocking-based unmanned aerial vehicle cluster: A threat to swarm intelligence. Secur. Commun. Netw. 2020, 2020, 8889122. DOI:10.1155/2020/8889122.
27. Basan, E.; Basan, A.; Nekrasov, A.; Fidge, C.; Ishchukova, E.; Basyuk, A.; Lesnikov, A. Trusted operation of cyber-physical processes based on assessment of the system's state and operating mode. Sensors 2023, Vol. 23. No. 4. 1996. DOI: 10.3390/s23041996.