МЕТОДИКА ВЫБОРА ЭФФЕКТИВНЫХ КОНТРМЕР ДЛЯ ПОВЫШЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Басан Е. С.[1], Силин О. И.[2], Фирсова М. Г.[3]

DOI: 10.21681/2311-3456-2025-1-28-40

Цель работы *состоит в разработке методики повышения отказоустойчивости киберфизической системы за счет применения контрмер в зависимости от выявленных угроз при воздействии на нее атак.*

Метод исследования: *разрабатываемая методика строится на основе концептуальной модели, которая описывает киберфизические параметры и структурно-функциональные характеристики системы, а также позволяет определить актуальные угрозы, влияющие на киберфизическую систему. Методика формально описывает угрозы, представляющие опасность для киберфизических систем, оценивает риски этих угроз и предлагает эффективные контрмеры для снижения риска возникновения угроз. Для иерархического представления знаний о киберфизических параметрах и угрозах используется онтологических подход. Онтология позволяет описать соотношение воздействующих на структурно-функциональные характеристики угроз, а также выявить контрмеры, которые способствуют минимизации рисков информационной безопасности.*

Результаты исследования: *разработана методика, которая на основе анализа структурно-функциональных характеристик системы и их критичности позволяет выявить актуальные угрозы и подобрать эффективные контрмеры для их минимизации. Проведен анализ основных параметров киберфизических систем, составлена концептуальная модель, которая позволяет описать структуру киберфизической системы. В результате анализа основных параметров киберфизических систем были определены такие, которые наиболее подвержены кибератакам. Также был создан перечень контрмер, которые позволяют минимизировать риски безопасности, что повышает отказоустойчивость киберфизической системы. Итогом работы является перечень атак, которые являются актуальными для киберфизических систем, а также ряд контрмер, которые позволяют минимизировать выявленные кибератаки, при этом контрмеры разделены на три категории.*

Научная новизна: *применение онтологического подхода для описания киберфизических параметров и структурно-функциональных характеристик киберфизической системы, что позволило выявить наиболее подверженные атакам и оценить риски безопасности.*

Ключевые слова: *интернет вещей, сенсоры, кибератака, угрозы, уязвимости, структурно-функциональные характеристики, средства передачи данных, меры противодействия, инцидент.*

Введение

Киберфизическая система (КФС) представляет собой взаимосвязь физических и программных компонентов, которые управляются и контролируются компьютерными алгоритмами. В архитектуру КФС входят сенсоры, микроконтроллеры, инструменты обработки данных, средства передачи данных и интерфейс пользователя. При этом КФС подвержены широкому спектру кибератак. Существует шесть классов кибератак, которым подвержены КФС и их компоненты, а именно: глушение каналов передачи данных, перехват сообщений, удаление сообщений, внедрение сообщений, подделка сообщений и атака на контроллеры системы. Всесторонний обзор мер противодействия важен, поскольку меры противодействия могут не ограничиваться конкретным перечнем атак. Знание широкого спектра существующих контрмер может подготовить систему и к существующим, и к новым кибератакам.

Рассмотрим существующие методы и методики анализа угроз КФС и Интернета вещей.

Авторами статьи [1] делается попытка выделить известные угрозы на разных уровнях архитектуры Интернета вещей (Internet of Things – IoT) с учетом возможности реализации атак. Авторы представляют развернутую методологию реализации атак на IoT, а также необходимые меры повышения информационной безопасности. Авторы предлагают руководство по разработке методологии обеспечения безопасности IoT на основе отраслевых документов, которая включает в себя оценку рисков, применение

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

2 Силин Олег Игоревич, ассистент кафедры Безопасности информационных технологий им. О. Б. Макаревича Института компьютерных технологий и информационной безопасности Южного федерального университета, г. Таганрог, Россия. E-mail: silin@sfedu.ru

3 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

средств информационной безопасности, повышающих конфиденциальность, целостность и доступность системы, а также метод расчета рисков. Основная цель оценки состоит в том, чтобы определить все инциденты безопасности, которые могут произойти в организации, и впоследствии инициировать процесс обработки риска, чтобы минимизировать ущерб от таких событий. Отсутствие автоматизации процесса в данном случае является серьезным недостатком. Кроме того, при оценке не учитываются риски, связанные с объектом, которым «управляет» Интернет вещей.

Авторы [2] рассматривают различные подходы применения онтологического инжиниринга для Интернета вещей и его необходимость. Авторы отметили, что вопросы интеграции онтологий для обеспечения безопасности Интернета вещей обсуждаются в научных работах многих авторов. В одной из рассмотренных авторами работ была предложена распределенная система на основе онтологии для удовлетворения требований конфиденциальности учреждений здравоохранения. Также в статье говорится, что сегодня существуют различные онтологические модели для распознавания угроз в системе Интернета вещей. Описанный инструмент IoTChecker для определения аномалий в конфигурациях безопасности Интернета вещей использует несколько онтологий Интернета вещей для распознавания угроз.

Также в разных странах существуют нормативные документы, которые могут применяться для анализа угроз и формирования мер противодействия для КФС.

В [3] авторы исследовали использование КФС в качестве агентов при проведении кибератак. В некоторых из этих сценариев атак КФС сначала должна стать целью атаки для захвата, прежде чем взятую под контроль КФС можно будет превратить в агента атаки. При этом атака может быть совершена не только в киберпространстве, но и на физическом уровне. В работе также представлен ряд контрмер для предотвращения выявленных атак. Некоторые из этих контрмер включают в себя физические механизмы.

Акцентируя внимание на мониторинге безопасности КФС, авторы [4] предлагают подход корреляции событий безопасности в КФС на основе генерации графов. Подход состоит из четырех этапов: предварительная обработка данных, анализ сходства событий, генерация графа и классификация узлов. Подход предполагает проведение семи видов атак, а затем дальнейший анализ событий безопасности. Для анализа сходства событий используется алгоритм BIRCH (сбалансированное итеративное сокращение и кластеризация с использованием иерархий), который позволяет выполнять иерархическую кластеризацию на больших наборах данных. Затем формируется RSE-график, который может отображать взаимосвязь между репрезентативными событиями. В итоге узлы графа классифицируются с помощью сверточных нейронных сетей графа (GCN), которые учитывают локальную окрестность узла в графе для составления прогнозов. Экспериментальная часть показала, что подход может быть использован для построения графа репрезентативных событий безопасности и обнаружения состояний безопасности, что впоследствии поможет при прогнозировании рисков безопасности системы.

В работе [5] автор рассматривает технологии кибербезопасности для КФС и фреймворки управления рисками. Обзор существующих подходов управления рисками кибербезопасности показал, что ни один из фреймворков явно не рассматривает экосистему безопасности КФС, существует лишь несколько исследований, применяющих количественную оценку к кибератакам и их последствиям. Именно это, по мнению автора, должно нас мотивировать на разработку структуры методики обеспечения кибербезопасности, управления и минимизации рисков КФС, которая улучшает существующие подходы.

Необходимо отметить, что большинство исследований на сегодняшний день являются теоретическими, учеными только делаются попытки изучения и выявления общих принципов обеспечения безопасности КФС и определения угроз и требований по безопасности, характерных для такой инфраструктуры.

В данной работе представлены две разработанные методики для анализа безопасности КФС: методика оценки рисков безопасности и методика выбора эффективных контрмер, приведены примеры их применения.

1. Методики оценки рисков безопасности киберфизических систем

Первым этапом при выборе контрмер для обеспечения безопасности и повышения отказоустойчивости КФС является выявление и оценка рисков безопасности системы. Рассмотрим существующие схемы диагностики инцидентов безопасности и проактивную методику оценки рисков, а также опишем разработанную в данном исследовании методику оценки рисков для КФС на основе вышесказанного.

1.1. Диагностика инцидентов безопасности для киберфизических систем

Схема диагностики состоит из нескольких шагов. Причинно-следственная связь первого типа использует знания предметной области о взаимодействиях компонентов системы для выявления потенциальных причин. Наличие списка потенциальных причин дает больше шансов обнаружить подозрительные

события. На втором этапе идет анализ следов с целью обнаружения потенциальных причин. Однако после второго этапа нельзя точно утверждать, какая из обнаруженных причин является действительной. В результате на третьем этапе требуется анализ фактической причинности, чтобы различать актуальные и неактуальные причины. Для диагностики КФС необходимо сначала описать взаимодействия между его программным обеспечением и физическими компонентами [6].

Продемонстрируем работу предлагаемой схемы диагностики на экспериментальном образце беспилотной автоматизированной системы (БАС). Атака на систему Global Positioning System (GPS) приводит к ложному показанию GPS БАС и потери координат местоположения. Применение схемы заключается в поэтапном анализе данных обратной связи БАС. Также атака может вывести GPS систему из строя, что можно понять по анализу показаний данной системы. К таким показаниям чаще всего относится высота полета БАС (рис. 1).

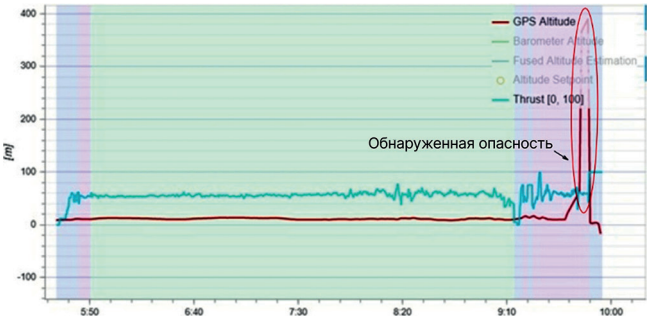

Рис. 1. Показания высоты полета БАС при проведенной атаке

Изучив график, можно сделать вывод, что после проведения атаки на GPS систему, начинают колебаться показания высоты и оборотов, далее по показаниям системы GPS выделяется резкий набор высоты, хотя фактически БАС не набирает ее, а остается на прежней высоте, что можно понять, просмотрев показания оборотов двигателей.

Также эта атака может вывести GPS-систему из строя, что тоже можно понять по данным от системы (рис. 2).

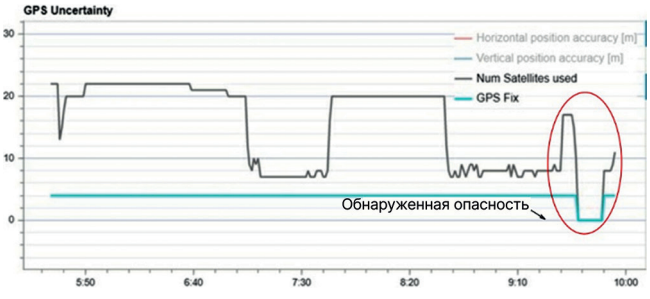

Рис. 2. Показания GPS системы

На графике серой линией обозначено количество используемых GPS спутников, синей линией соответственно их сопряженность с системой БАС. Проанализировав график, можно сделать вывод о том, что после атаки на GPS-систему количество используемых спутников начало изменяться в отрицательном и положительном направлении, в итоге на некоторое время сравнялось с нулем, тем самым БАС потерял фиксацию и вышел из строя на некоторый промежуток времени, за счет чего наблюдалось ошибочное показание системы GPS.

1.2. Проактивная методика оценки риска

В предлагаемой методике оценивается риск нарушения безопасности на основе компонентных моделей. Соответственно, общая оценка риска системы в целом является суммированием оценок риска ее компонентов. Схема предоставляет информацию о подверженности компонентов атакам на целостность, конфиденциальность или доступность компонента. В зависимости от уровня восприимчивости для каждой атаки каждому компоненту присваиваются значения от 0 до 1 (0 означает «не восприимчив», 1 соответствует «высоко восприимчив»). Для расчета риска удельные вероятности возникновения атаки умножаются на значение восприимчивости. Результат оценки риска по представленной схеме является многомерным [7]. В соответствии с общей задачей разные аспекты безопасности играют разные роли и должны быть соответствующим образом взвешены.

Рассмотрим результаты применения описанной методики на экспериментальном образце БАС. Базовая конфигурация оборудования включает в себя одну беспроводную линию связи, совместимую с IEEE 802.11b/g, пульт управления, всенаправленную антенну, связь не шифруется. Также БАС содержит одну камеру, не имеет носителей информации, использует инерциальную навигационную систему в качестве сенсорного оборудования, механизм обработки ошибок включает в себя только «режим экстренной посадки». Рассмотрим результаты оценки рисков для каждого компонента системы по свойствам целостности, конфиденциальности и доступности (табл. 1), которые получены в соответствии с рассмотренной методикой.

Результаты применения методики к данному БАС обоснованы использованием двух диапазонов связи (C-диапазона и Wi-Fi-b соответственно), наличием камеры, не участвующей в системе позиционирования. Также используется энергозависимое хранилище, потенциально приводящее к риску целостности и доступности. Механизм обработки ошибок включает в себя только экстренную посадку, в остальных случаях пилот должен справляться с неисправностями вручную.

Таблица 1.

Результаты оценки риска для прототипа БАС

Составная часть	Целостность	Конфиденциальность	Доступность
Система связи	1,1	2,3	1,5
Хранилище данных	0,9	0	0,9
Датчики	3,6	0	1,8
Обработка ошибок	0,9	0,9	0,9
Общий итог	6,5	3,2	5,1
Система связи	1,1	2,3	1,5

1.3. Разработка методики оценки риска для киберфизических систем

Разработанная в данном исследовании методика представляет собой схематично описанную цепочку последовательностей воздействия конкретной группы атак на киберфизические параметры (КФП) системы, неверные показания которых могут привести к определенным последствиям.

Пользователь выбирает определенную группу атак из следующих: получение доступа, подделка, отказ в обслуживании, атаки на целостность. После этого по онтологической схеме (рис. 3) определяется влияние этой группы на КФП, затем на основе выбранных КФП выбираются структурно-функциональные характеристики (СФХ), которые они составляют. При выборе характеристик схема определяет перечень предстоящих последствий в случае неисправности этих систем. Затем определяется вероятность того, что каждое воздействие повлияет на три основных параметра. Таким образом, с помощью схемы можно

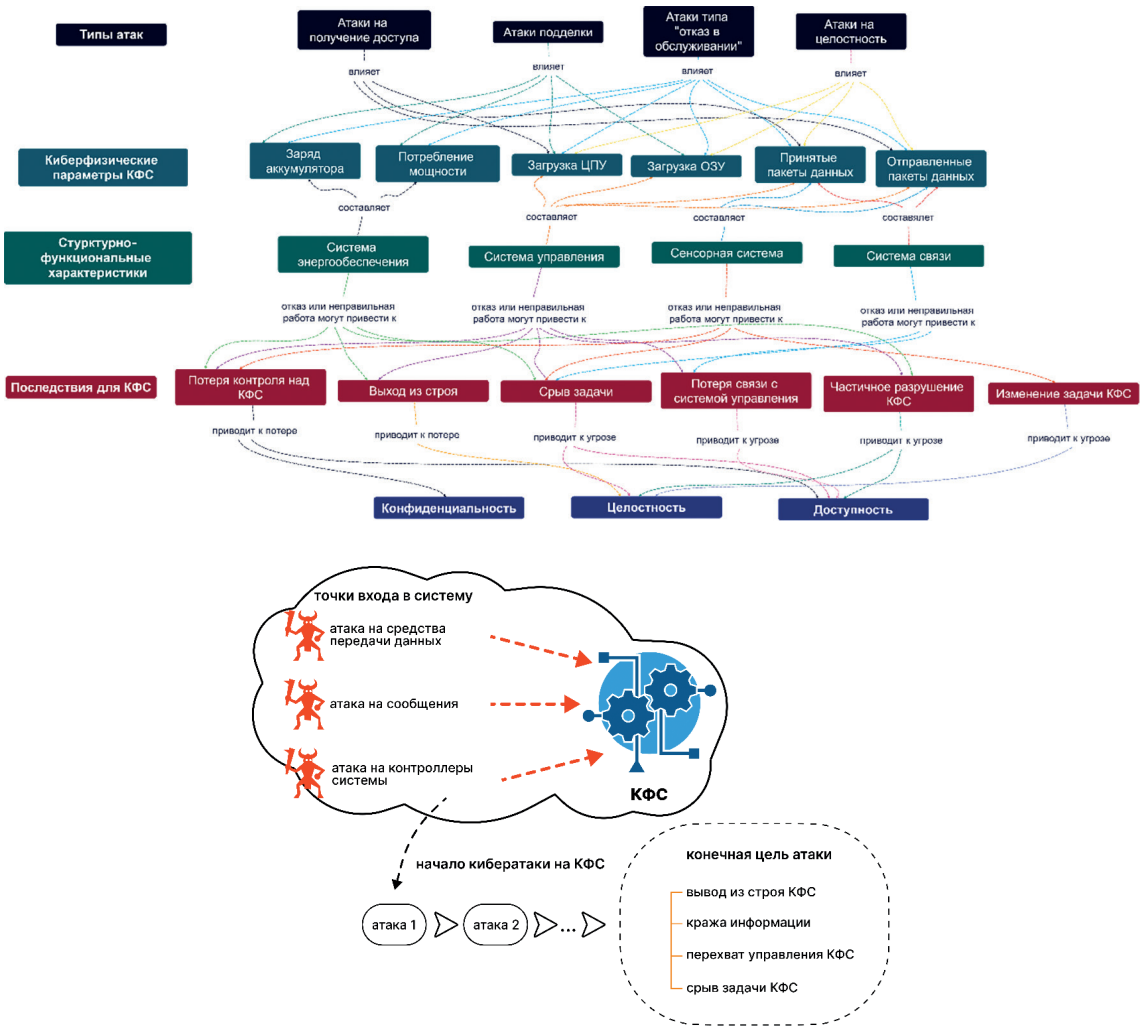

Рис. 3. Методика оценки рисков

Таблица 2.

Методика оценки рисков

Параметр	Обозначение	Формула	Результат
коэффициент влияния атаки	Z	$Z = \frac{\sum K_z}{K}$ (1)	Критичный (1) Высокий (0,8) Средний (0,5) Низкий (0,2)
общее количество КФП	K		
КФП, подверженный влиянию атаки	K_z		
коэффициент отказа системы	X	$Z = \frac{\sum X_z}{X_o}$ (2)	
количество последствий в результате влияния атаки	X_v		
общее число последствий	X_o		

определить от воздействия атак на КФП до суммарной вероятности потери конфиденциальности, целостности и доступности [8].

Методика позволяет рассчитать коэффициенты влияния атаки и отказа системы (табл. 2). Коэффициент влияния атаки (Z) представляет собой отношение КФП, подверженных влиянию атаки (K_z), к общему количеству КФП (K). Коэффициент отказа системы (X) представляет собой отношение количества последствий в результате влияния атаки (X_v) к общему числу последствий (X_o). Коэффициенты имеют четыре уровня критичности, которые лежат в диапазоне от 0 до 1. Границы уровней определены исходя из теоретического анализа.

С помощью схемы (рис. 3) проанализируем тип атаки «На получение доступа». Данный тип атак оказывает влияние на пять КФП: загрузка центрального процессора (ЦПУ), число зафиксированных спутников, уровень GPS шума, принятые пакеты данных, отправленные пакеты данных.

В итоге произведя расчеты с помощью формулы (1) можно сделать вывод, что влияние этой атаки на КФП является 0,35. Подвергшиеся влиянию атаки КФП составляют три системы БАС: система управления, система навигации, система связи.

Далее определяем, к каким последствиям приводит отказ или неправильная работа системы управления БАС. Рассчитываем по формуле (2) коэффициент

Таблица 3.

Влияние подгрупп атак на киберфизические параметры БАС

КФП	Атаки на получение доступа	Атаки подделки	Атаки типа «Отказ в обслуживании»	Атаки на целостность
Заряд аккумулятора		+	+	
Потребление мощности		+	+	
Загрузка ЦПУ	+	+	+	+
Загрузка ОЗУ		+	+	+
Число	6,5	3,2	5,1	
зафиксированных	1,1	2,3	1,5	
спутников	+	+		
Координаты БПЛА		+	+	+
Долгота		+	+	+
Широта		+	+	+
Высота полета			+	
Скорость полета		+	+	+
Уровень шумов	+		+	
Вибрация БПЛА			+	+
Принятые пакеты данных	+		+	+
Отправленные пакеты данных	+		+	+

опасности отказа системы, затем с помощью схемы можно рассчитать риски для конфиденциальности, целостности и доступности путем непосредственного влияния каждого из последствий на них. Ниже представлены расчеты влияния атак на КФП БАС по данной методике (табл. 3) и уровень опасности при воздействии определенных типов атак (табл. 4). Чем выше значение, тем больше уровень опасности.

Таблица 4.

Уровень опасности типов атак

Подгруппы атак	Уровень опасности
Атаки на получение доступа	0,36
Атаки подделки	0,64
Атаки типа «Отказ в обслуживании»	0,93
Атаки на целостность	0,64
Атака типа «Spoofing»	0,64
Атака типа «Tampering»	0,64
Атака типа «Repudiation»	0,28
Атака типа «Information Disclosure»	0,35
Атака обратного инжиниринга	0,35
Атака типа «SkyJack»	0,35

Разработанная методика охватывает распространенные атаки на КФП КФС и помогает выявить и оценить риски безопасности, которые могут возникнуть в результате атаки. Кроме того, методика позволяет определить меры противодействия для снижения рисков безопасности, а также рассчитать эффективность их применения.

2. Методика выбора эффективных контрмер

При рассмотрении мер противодействия кибератакам основное внимание уделяется атакам, которые нацелены на КФС, но не используют КФС в качестве агентов атаки на другие цели.

Сначала кибератаки классифицируются на основе типа точки входа, которая может быть средством передачи данных, сообщением или контроллером системы. В соответствии с этой классификацией существует шесть категорий атак, которые будут описаны далее. Базируясь на данной классификации, была проанализирована существующая литература на предмет контрмер для таких категорий атак.

Можно выделить три типа контрмер: классические, резервные и специальные. Классические препятствуют началу кибератаки. Так можно постоянно выполнять мониторинг и обработку информационного потока, чтобы заблаговременно обнаружить деструктивное воздействие. Когда классические контрмеры неэффективны, резервные предупреждают оператора либо пользователя КФС об атаке. К примеру, использование более чем одного типа датчиков для каждого критического измерения повысит отказоустойчивость системы и не даст начавшейся кибератаке вывести из строя КФС. После обнаружения атаки специальные меры способствуют снижению ущерба. Если заранее создать предопределенные процедуры управления КФС, то во время атаки система перейдет в автономную работу или отключится.

2.1. Кибератаки

Кибератака – это наступательное действие со злым умыслом, влияющее на вычислительные и коммуникационные функции. Хотя атаки могут привести к некоторым дополнительным сбоям в требованиях кибербезопасности, такие сбои могут не быть конечной целью злоумышленника. Через серию последовательных сбоев в кибербезопасности злоумышленник может стремиться в итоге вывести из строя или перехватить управление КФС, поставить под угрозу выполнение задачи или просто украсть собранную информацию (рис. 4). Таким образом, кибератака может представлять собой сложный многоэтапный процесс.

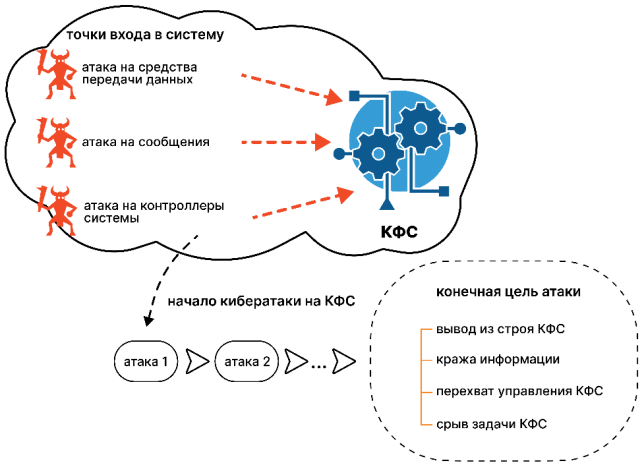

Рис. 4. Иллюстрация кибератаки на КФС

Как говорилось ранее, кибератаки классифицируются на основе типа точки входа в систему, в нашем случае это средства передачи данных, сообщения или контроллеры системы. Таким образом, мы выделили шесть категорий кибератак (рис. 5):

1) глушение канала передачи данных;
2) перехват сообщений;
3) удаление сообщений;
4) внедрение сообщений;
5) подмена сообщений;
6) атаки на контроллеры системы.

Глушение канала осуществляется путем создания более мощного радиосигнала, который значительно превышает мощность легитимных сигналов в целевом канале. В результате полезные сигналы подавляются

Рис. 5. Схема представлений данных о кибератаках

и проявляются только как шум в приемниках. Такая атак направлена на то, чтобы сделать канал связи недоступным для получателя. Следовательно, глушение каналов – это форма атаки типа «отказ в обслуживании» на физическом уровне.

Перехват сообщений – это пассивная атака, при которой злоумышленник получает посредством прослушивания сообщения, передаваемые по каналу связи. В этой атаке противник должен интерпретировать и понимать перехваченные сообщения. Целью атаки может быть перехват данных о системе. Кроме того, злоумышленник может получить другую вторичную информацию из перехваченных сообщений.

Удаление сообщения – это злонамеренное действие, которое отбрасывает сообщение, которое должно было быть передано предполагаемому получателю. Эта атака осуществляется злоумышленником, который предполагает ретранслировать сообщение, когда отправитель и предполагаемый получатель не находятся в пределах досягаемости каждого из них. По сравнению с перехватом сообщений эта атака может быть менее сложной, поскольку для этого злоумышленнику нужно просто отбросить сообщение.

Внедрение сообщений – это форма кибератаки, при которой создаются незаконные сообщения, а затем передаются через канал управления.

Подмена сообщений – это злонамеренный акт создания и передачи поддельной версии сообщения, а также их отображение в том виде, в котором они передаются от законного отправителя. В этом контексте злоумышленник является незаконным отправителем поддельного сообщения.

Контроллеры КФС отвечают за управление процессами, сетевые коммуникации, управление устройствами и т.д. Атаки на контроллеры могут привести к нарушению работы системы, потере контроля над процессами или даже физическим повреждениям.

2.2 Разработка набора контрмер

В литературе [9]–[16] предложен ряд мер противодействия различным кибератакам на КФС. В результате анализа контрмеры были разделены на три категории в зависимости от функциональных возможностей – классические, резервные и специальные, которые имеют свои функциональные возможности (рис. 6).

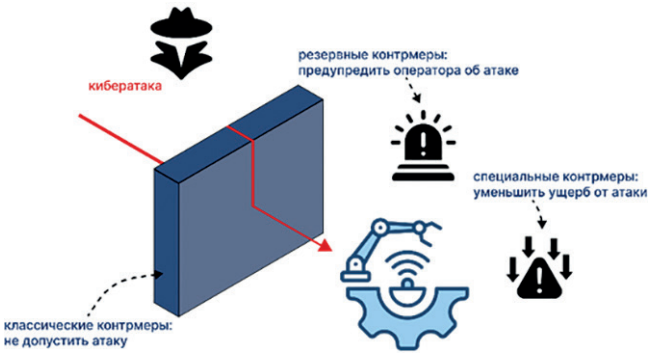

Рис. 6. Функциональные возможности различных контрмер кибератакам

Классические контрмеры позволяют предотвратить начало кибератаки. Когда классические меры противодействия не дали результата и атака была успешно начата, важными становятся резервные контрмеры для предупреждения оператора КФС о такой атаке. После обнаружения наличия атаки специальные контрмеры помогают уменьшить негативное воздействие и ограничить ущерб (табл. 5).

Также следует выделить еще одну категорию контрмер – профилактические. Профилактические контрмеры работают тремя способами:

1) ввести строгий контроль доступа к системе, чтобы только авторизованный персонал и программный агент могли устанавливать контакт с КФС;
2) защищать конфиденциальность, целостность и подлинность информации таким образом, чтобы никакие поддельные или ошибочные данные и команды не принимались;
3) использовать только системную прошивку и программные компоненты без уязвимостей.

Не все три метода предотвращения применимы ко всем кибератакам. Например, в качестве контрмеры против атаки на контроллеры системы в [17] и [18] необходимо спроектировать и внедрить в КФС только сенсоры с приемлемыми характеристиками в пределах ожидаемого рабочего диапазона. Но такая контрмера бесполезна для других атак. Кроме

Таблица 5.

Виды контрмер

Кибератаки	Контрмеры		
	Классические	**Резервные**	**Специальные**
Глушение канала передачи данных	Когнитивное радио, для переключения между каналами	Несколько приемников с разными частотами работы оборудования	Предопределенная процедура управления КФС для автономной работы или отключения
Перехват сообщений	Шифрование информации	Совместное использование радиосвязи и оптических каналов связи	Перенаправление злоумышленника на фальшивую цель
Удаление сообщения	Постоянный мониторинг и обработка информационного потока	Несколько приемников и передатчиков	Предопределенная процедура управления КФС для автономной работы или отключения
Внедрение сообщений	Проверка сообщений и использование шифрования информации	Несколько приемников и передатчиков	Атака с глушением канала как средство защиты
Подмена сообщений	Проверка сообщений, использование аутентификации и использование шифрование информации	Использование более чем одного типа датчиков для каждого критического измерения	Атака с глушением канала как средство защиты
Атаки на контроллеры системы	Строгая аутентификация узла для допуска только доверенных программ для предотвращения атак вирусов и вредоносных программ	Использование более чем одного типа датчиков для каждого критического измерения	Предопределенная процедура управления КФС для автономной работы или отключения

того, контроллеры системы должны быть оснащены функциями защиты от несанкционированного доступа, чтобы предотвратить открытие дополнительных точек входа для атак. Другим примером является использование устойчивых к помехам схем передачи, таких как расширение спектра с прямой последовательностью и расширение спектра со скачкообразной перестройкой частоты для предотвращения атак с глушением каналов. Такая контрмера обычно бесполезна для других атак, которые не запускаются на физическом уровне.

Кроме того, сообщения аутентификации и ассоциации, которые по умолчанию передаются в открытом виде, должны быть зашифрованы, чтобы предотвратить прослушивание беспроводной сети, которое предшествует атаке. Шифрование сообщения может защитить его конфиденциальность и, таким образом, предотвратить атаку с перехватом сообщений (рис. 7).

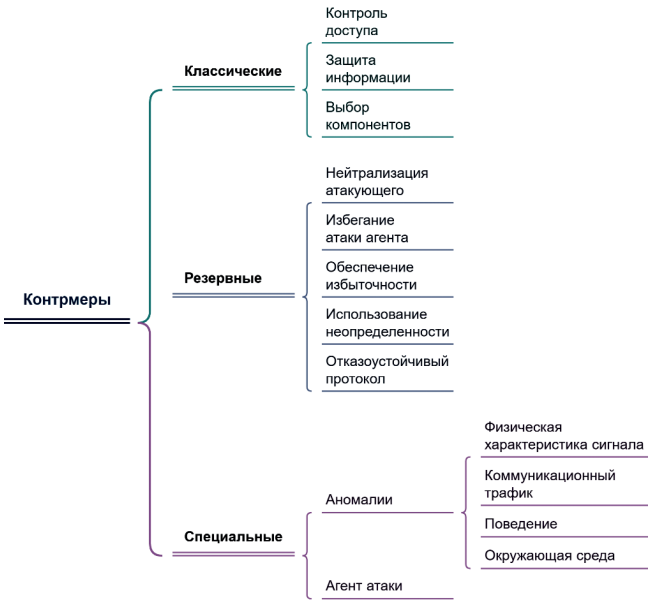

Рис. 7. Использование шифрования в качестве контрмер

Помимо криптографических методов, конфиденциальность информации также может быть достигнута с помощью методов защиты физического уровня. В контексте средств передачи данных авторы [19] предложили защищаться от полнодуплексного подслушивания путем передачи на физическом уровне сигналов искусственного шума вместе с информационными сигналами. Разработана схема определения оптимального коэффициента распределения мощности между искусственным шумом и информационными сигналами, при котором комбинация вероятности прекращения передачи и вероятности нарушения секретности минимизируется.

2.3. Разработка методики выбора эффективных контрмер

Методика представляет собой схематично описанную последовательность выбора эффективных контрмер для защиты КФС от атак противника [20]. Данную методику можно представить в виде концептуальной модели (рис. 8).

После определения типа кибератаки из схемы определяются контрмеры, которые можно использовать для предотвращения или смягчения последствий.

Методика позволяет рассчитать вероятность наступления того или иного последствия, а также успешность применения контрмер (табл. 6). Вероятность наступления последствия представляет собой отношение поврежденных в результате атаки систем к общему числу систем. Степень защиты после применения контрмер представляет собой отношение эффективных контрмер к общему числу контрмер. Коэффициенты имеют четыре уровня критичности, которые лежат в диапазоне от 0 до 1. Границы уровней определены исходя из теоретического анализа. Эффективность контрмер определяется показателями K и W, где значение W должно быть больше значения K, что означает степень защиты выше вероятности возникновения последствия. Если степень защиты будет ниже вероятности возникновения последствия, то каждая успешно примененная контрмера снижает вероятность наступления последствия на 10 %.

Проверим разработанную методику на экспериментальном образце БАС. Базовая конфигурация оборудования включает в себя полетный контроллер Pixhawk 4, одну беспроводную линию связи, совместимую с IEEE 802.11b/g [21], пульт управления, всенаправленную антенну, связь не шифруется. Также БАС содержит одну камеру, не имеет носителей информации, в качестве сенсорного оборудования используется ИНС. Механизм обработки ошибок

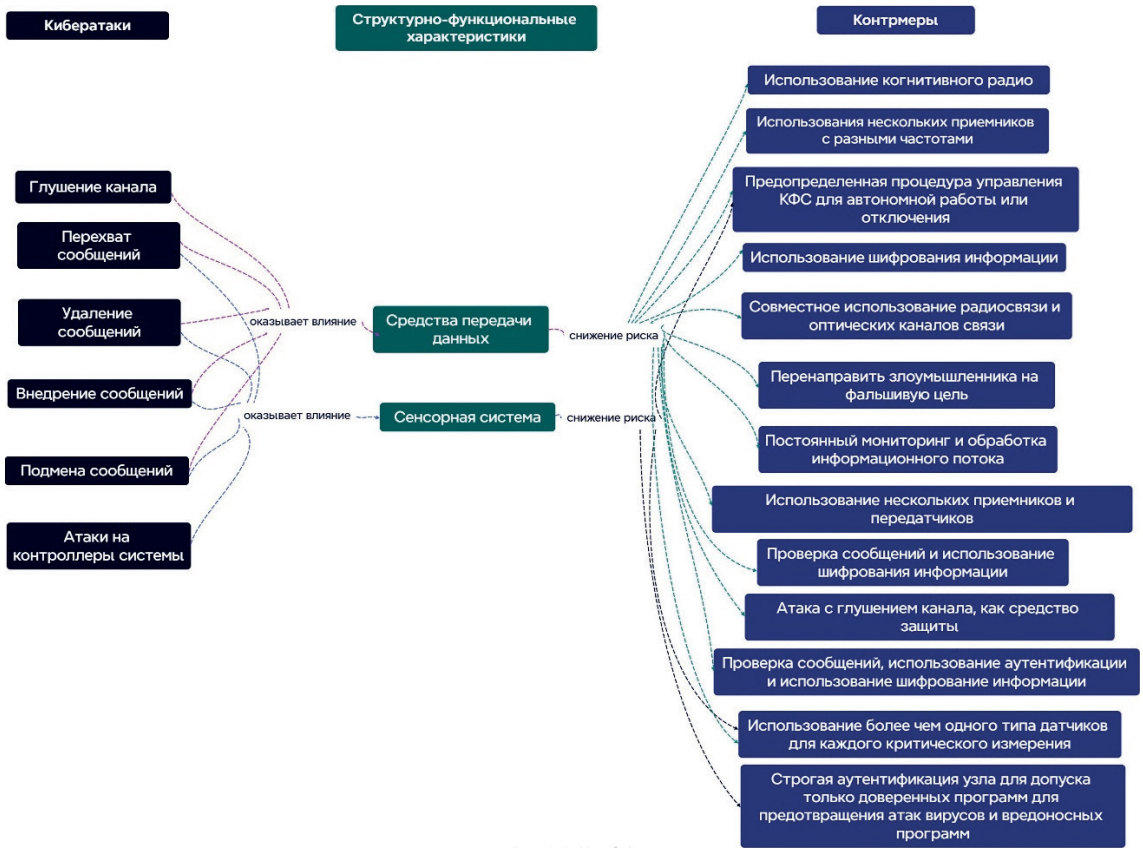

Рис. 8. Методика выбора эффективных контрмер

Таблица 2.

Методика оценки рисков

Параметр	Обозначение	Формула	Результат
вероятность наступления последствия	K	$K = \frac{\sum p_z}{P}$ (3)	Критичный (1) Высокий (0,8)
поврежденные в результате атаки системы	P		
общее число систем	p		
степень защиты после применения контрмер	W	$W = \frac{\sum t}{T}$ (4)	Средний (0,5) Низкий (0,2)
эффективные контрмеры	t		
общее число контрмер	T		

включает в себя только «режим земли». Для данного БАС характерны следующие угрозы:

- подмена сигнала GPS [22];
- подмена сообщения [23];
- глушение канала [24].

С помощью методики оценки угроз рассчитаем коэффициент опасности данных угроз, затем определим последствия, возникающие в результате угроз. На примере угрозы «Потеря контроля над БАС» рассмотрим предлагаемые контрмеры. Согласно методике снижения вероятности угрозы в данном случае стоит использовать следующие контрмеры:

- резервирование каналов связи,
- предопределенная процедура управления КФС для автономной работы или отключения,
- использование более чем одного типа датчиков для каждого критического процесса,
- шифрование каналов связи,
- использование систем обнаружения аномалий.

При угрозе подмены сигнала GPS вероятность наступления такого последствия, как «срыв задачи» будет равна:

$$K = \frac{4}{5} = 0{,}8.$$

В переводе на процентное соотношение – 80 %, для снижения риска с помощью схемы определим эффективные контрмеры и рассчитаем степень снижения риска:

$$W = \frac{7}{10} = 0{,}7.$$

После успешного применения контрмер вероятность возникновения снижается на 70%, в нашем случае K > W, значит вероятность наступления данного последствия после применения контрмер остается, но сводится к 10%, что позволяет сделать вывод об эффективности выбранных контрмер, в случае их успешного применения.

Вероятность наступления такого последствия как «Выход из строя» равна:

$$K = \frac{3}{5} = 0{,}6.$$

Что в процентном соотношении составляет 60%, рассчитаем степень снижения риска после применения контрмер:

$$W = \frac{5}{10} = 0{,}5.$$

После применения контрмер K > W, что означает если все контрмеры были успешно реализованы вероятность наступления последствия сводится к 10 %. В реальных условиях каждая успешно примененная контрмера снижает угрозу возникновения на 10 %.

Также при угрозе «подмена сигнала GPS» возможно такое последствие как «Частичное разрушение КФС», рассчитаем вероятность наступления для этого последствия:

$$K = \frac{4}{5} = 0{,}8.$$

В процентном соотношении – 80%, рассчитаем степень защиты после применения контрмер:

$$W = \frac{4}{10} = 0{,}4.$$

Применение контрмер в этом случае позволяет снизить риск возникновения последствия на 40 % и сводит вероятность возникновения к 40 %, вдвое меньше, чем до применения, что позволяет сделать выводы об эффективности контрмер в случае их успешного применения.

Заключение

Выбор эффективных контрмер для повышения отказоустойчивости КФС требует комплексного подхода. В результате работы был проведен анализ основных параметров КФС, и были выбраны те компоненты, которые имеют наибольшую вероятность наличия уязвимостей. Знания о наличии уязвимостей дают понимание о возможных векторах атак, которые может использовать злоумышленник для дестабилизации работы системы.

По результатам анализа литературы был составлен перечень контрмер в зависимости от вида кибератаки, которая может быть проведена на КФС. Перечень контрмер был разделен на три вида в зависимости

от функциональных возможностей системы. Приведенный перечень носит рекомендательный характер и может быть использован на усмотрение пользователей и операторов КФС.

Результатом методики является концептуальная модель, которая включает в себя перечень возможных кибератак на КФС, структурно-функциональные характеристики, на которые влияют приведенные кибератаки, и набор контрмер для минимизации рисков безопасности и повышения отказоустойчивости системы. Важно отметить, что эффективность контрмер может различаться в зависимости от конкретной системы и ситуации.

Данная методика показывает себя эффективней аналогов за счет возможностей расчета коэффициентов опасности, предсказаний вероятных последствий и предложения эффективных контрмер для снижения рисков. Простота расчетов и пошаговое использование делает методику более легкой в использовании и менее время затратной. Методика имеет возможность совершенствования и расширения за счет добавления новых атак и возможных угроз, а также добавления актуальных контрмер.

Разработанная методика была протестирована на экспериментальном стенде собранного БАС. Результат методики позволил авторам понять, что необходимо конкретизировать перечень СФХ системы, а также составить перечень вероятных рисков, которые могут наступить в результате реализации кибератак.

Работа выполнена при поддержке Совета по грантам Президента Российской Федерации. Стипендия Президента Российской Федерации молодым ученым и аспирантам (Конкурс СП-2022) № СП-858.2022.5 и Внутреннего гранта студенческим научным объединениям Южного федерального университета.

Литература

1. *I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, «Anatomy of Threats to the Internet of Things,» in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636–1675, Secondquarter 2019, doi: 10.1109/COMST.2018.2874978*
2. *Qaswar F., Rahmah M., Raza M. A., Noraziah A., Alkazemi B., Fauziah Z., Hassan M. K. A., Sharaf A. Applications of Ontology in the Internet of Things: A Systematic Analysis. Electronics. 2023; 12(1):111. https://doi.org/10.3390/electronics12010111*
3. *Jean-Paul Y., Hassan N., Ola S. Security analysis of drones systems: Attacks, limitations, and recommendations internet of things // Sensors. – 2020 Vol. 11, No. 100218 – P. 1–38.*
4. *Levshun, D., Kotenko, I. Intelligent Graph-Based Correlation of Security Events in Cyber-Physical Systems. In: Kovalev, S., Kotenko, I., Sukhanov, A. (eds) Proceedings of the Seventh International Scientific Conference «Intelligent Information Technologies for Industry» (IITI'23). IITI 2023. Lecture Notes in Networks and Systems, vol 777. Springer, Cham. https://doi.org/10.1007/978-3-031-43792-2_12*
5. *Lee I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet. 2020; 12(9):157. https://doi.org/10.3390/fi12090157*
6. *Ramanathan, L., Nandhini, R. S. (2022). Cyber-Physical System—An Architectural Review. In: Joshi, A., Mahmud, M., Ragel, R. G., Thakur, N. V. (eds) Information and Communication Technology for Competitive Strategies (ICTCS 2020). Lecture Notes in Networks and Systems, vol 191. Springer, Singapore. https://doi.org/10.1007/978-981-16-0739-4_13*
7. *A. Tantawy, S. Abdelwahed, A. Erradi, K. Shaban, Model-based risk assessment for cyber physical systems security, Computers & Security, Volume 96, 2020, 101864, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101864*
8. *Мельник Э. В., Сафроненкова И. Б., Таранов А. Ю. Онтологический подход к решению задачи перераспределения вычислительной нагрузки в распределенной системе мониторинга с мобильными компонентами на базе распределённого реестра // Известия ЮФУ. Технические науки. 2023.; N 5(2023).; С. 163–173.; DOI 10.18522/2311-3103-2023-5-163-173*
9. *Elias G. T., Tala T. K., Hamed T. G. A secure Blockchain-based communication approach for UAV networks // Proceedings of the IEEE International Conference on Electro Information Technology (EIT). – Chicago, 2020. – P. 411–415.*
10. *Ammar A., Muhammad M., Kashif M. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs // Sensors. 2021. Vol. 196, No. 4. P. 108–217.*
11. *Ghiasi M. et al. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future // Electric Power Systems Research. 2023. Vol. 215. p. 108975.*
12. *Wöhnert, Kai Hendrik & Wöhnert, Sven-Jannik & Thiel, Tobias & Weißbach, Rüdiger & Skwarek, Volker. Secure Cyber-Physical Object Identification in Industrial IoT-Systems. Procedia Manufacturing. 51. 1221–1228. 10.1016/j.promfg.2020.10.171*
13. *D. M., Thompson., Sean, B., Maynard., Atif, Ahmad, Ahmad. «Cyber-threat intelligence for security decision-making: A review and research agenda for practice». Computers & Security, 132 (2023).:103352–103352. doi: 10.1016/j.cose.2023.103352*
14. *Rakesh S., Atefeh O., Sajjad A. Machine-learning-enabled intrusion detection system for cellular connected UAV networks // Sensors. – 2021. – Vol. 10, No.1549. – P. 1–28.*
15. *Mihalache, S. F., Pricop, E., Fattahi, J. (2019). Resilience Enhancement of Cyber-Physical Systems: A Review. In: Mahdavi Tabatabaei, N., Najafi Ravadanegh, S., Bizon, N. (eds) Power Systems Resilience. Power Systems. Springer, Cham. https://doi.org/10.1007/978-3-319-94442-5_11*

16. *Thulasiraman P., Haakensen T., Callanan A. «Countering Passive Cyber Attacks Against Sink Nodes in Tactical Sensor Networks Using Reactive Route Obfuscation», Elsevier Journal of Network and Computer Applications, Vol. 132, pp. 10–21, April 2019. DOI: 10.1016/j.jnca.2019.01.028*
17. *Zhang, Dongdong & Li, Chunjiao & Goh, Hui Hwang & Ahmad, Tanveer & Zhu, Hongyu & Liu, Hui & Wu, Thomas. (2022). A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems. Renewable Energy. 189. 1383–1406. 10.1016/j.renene.2022.03.096*
18. *Zheng, Yu & Li, Zheng & Xu, Xiaolong & Qingzhan, Zhao. (2021). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks. 8, 422–435. DOI: 10.1016/j.jnca.2019.01.028*
19. *Li, Guangxia & Shen, Yulong & Zhao, Peilin & Lu, Xiao & Liu, Jia & Liu, Yangyang & Hoi, Steven. (2019). Detecting Cyberattacks in Industrial Control Systems Using Online Learning Algorithms. Neurocomputing. 364, 338–348. DOI: 10.1016/j.neucom.2019.07.031*
20. *J. Leško, M. Schreiner, D. Megyesi and L. Kovács, «Pixhawk PX-4 Autopilot in Control of a Small Unmanned Airplane», 2019 Modern Safety Technologies in Transportation (MOSATT), Kosice, Slovakia, 2019, pp. 90–93, doi: 10.1109/MOSATT48908.2019.8944101*
21. *Basan, E., Lapina, M., Lesnikov, A., Basyuk, A., Mogilny, A. Trust Monitoring in a Cyber-Physical System for Security Analysis Based on Distributed Computing. In: Alikhanov, A., Lyakhov, P., Samoylenko, I. (eds) Current Problems in Applied Mathematics and Computer Science and Systems. APAMCS 2022. Lecture Notes in Networks and Systems, vol 702. Springer, Cham. https://doi.org/10.1007/978-3-031-34127-4_42*
22. *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. https://doi.org/10.3390/drones6010008*
23. *Basan, E.; Basan, A.; Nekrasov, A. Method for Detecting Abnormal Activity in a Group of Mobile Robots. Sensors 2019, 19, 4007. https://doi.org/10.3390/s19184007*
24. *Basan, E.; Basan, A.; Mushenko, A.; Nekrasov, A.; Fidge, C.; Lesnikov, A. Analysis of Attack Intensity on Autonomous Mobile Robots. Robotics 2024, 13, 101. https://doi.org/10.3390/robotics13070101*

A METHODOLOGY FOR SELECTING EFFECTIVE COUNTERMEASURES TO INCREASE THE FAULT TOLERANCE OF CYBERPHYSICAL SYSTEMS

Basan E. S.[4], Silin O. I.[5], Firsova M. G.[6]

Keywords: *internet of things, sensors, cyberattack, threats, vulnerabilities, structural and functional characteristics, means of data transmission, countermeasures, incident.*

The aim of the work *is to develop a methodology for increasing the fault tolerance of a cyberphysical system through the use of countermeasures, depending on the identified threats when exposed to attacks on it.*

Research method: *the developed methodology is based on a conceptual model that describes the cyberphysical parameters and structural and functional characteristics of the system, and also allows you to identify current threats affecting the cyberphysical system. The methodology formally describes the threats that pose a danger to cyber-physical systems, assesses the risks of these threats and suggests effective countermeasures to reduce the risk of threats. An ontological approach is used to hierarchically represent knowledge about cyberphysical parameters and threats. The ontology allows us to describe the ratio of threats affecting the structural and functional characteristics, as well as to identify countermeasures that help minimize information security risks.*

Research results: *a methodology has been developed that, based on the analysis of the structural and functional characteristics of the system and their criticality, allows identifying current threats and selecting effective countermeasures to minimize them. An analysis of the main parameters of cyber-physical systems was conducted, a conceptual model was compiled that allows describing the structure of the cyber-physical system. As a result of the analysis of the main parameters of cyber-physical systems, those that are most susceptible to cyber-attacks were identified. A list of countermeasures was also created that minimize security risks, which increases the fault tolerance of the cyber-physical system. The result of the work is a list of attacks that are relevant for cyber-physical systems, as well as a number of countermeasures that minimize the identified cyber-attacks, while the countermeasures are divided into three categories.*

Scientific novelty: *the use of an ontological approach to describe the cyber-physical parameters and structural and functional characteristics of a cyber-physical system, which made it possible to identify those most susceptible to attacks and assess security risks.*

4 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

5 Oleg I. Silin, Assistant of the Department of Information Technology Security named after O. B. Makarevich, Institute of Computer Technology and Information Security, Southern Federal University «SFedU», Taganrog, Russia. E-mail: silin@sfedu.ru

6 Artyom Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, E-mail: Balyabinю.AA@ talantiuspeh.ru

References

1. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, «Anatomy of Threats to the Internet of Things,» in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636–1675, Secondquarter 2019, doi: 10.1109/COMST.2018.2874978
2. Qaswar F., Rahmah M., Raza M. A., Noraziah A., Alkazemi B., Fauziah Z, Hassan MKA, Sharaf A. Applications of Ontology in the Internet of Things: A Systematic Analysis. Electronics. 2023; 12(1):111. https://doi.org/10.3390/electronics12010111
3. Jean-Paul Y., Hassan N., Ola S. Security analysis of drones systems: Attacks, limitations, and recommendations internet of things // Sensors. – 2020 Vol. 11, No. 100218 – P. 1–38.
4. Levshun, D., Kotenko, I. Intelligent Graph-Based Correlation of Security Events in Cyber-Physical Systems. In: Kovalev, S., Kotenko, I., Sukhanov, A. (eds) Proceedings of the Seventh International Scientific Conference «Intelligent Information Technologies for Industry» (IITI'23). IITI 2023. Lecture Notes in Networks and Systems, vol 777. Springer, Cham. https://doi.org/10.1007/978-3-031-43792-2_12.
5. Lee I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet. 2020; 12(9):157. https://doi.org/10.3390/fi12090157
6. Ramanathan, L., Nandhini, R. S. (2022). Cyber-Physical System – An Architectural Review. In: Joshi, A., Mahmud, M., Ragel, R. G., Thakur, N. V. (eds) Information and Communication Technology for Competitive Strategies (ICTCS 2020). Lecture Notes in Networks and Systems, vol 191. Springer, Singapore. https://doi.org/10.1007/978-981-16-0739-4_13
7. A. Tantawy, S. Abdelwahed, A. Erradi, K. Shaban, Model-based risk assessment for cyber physical systems security, Computers & Security, Volume 96, 2020, 101864, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101864
8. Mel'nik Je. V., Safronenkova I. B., Taranov A. Ju. Ontologicheskij podhod k resheniju zadachi pererаspredelenija vychislitel'noj nagruzki v raspredelennoj sisteme monitoringa s mobil'nymi komponentami na baze raspredeljonnogo reestra // Izvestija JuFU. Tehnicheskie nauki.; 2023.; N 5 (2023).; S. 163–173.; DOI 10.18522/2311-3103-2023-5-163-173
9. Elias G. T., Tala T. K., Hamed T. G. A secure Blockchain-based communication approach for UAV networks // Proceedings of the IEEE International Conference on Electro Information Technology (EIT). – Chicago, 2020. – P. 411–415.
10. Ammar A., Muhammad M., Kashif M. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs // Sensors. – 2021. – Vol. 196, No. 4. – P. 108–217.
11. Ghiasi M. et al. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future // Electric Power Systems Research. 2023. Vol. 215. p. 108975.
12. Wöhnert, Kai Hendrik & Wöhnert, Sven-Jannik & Thiel, Tobias & Weißbach, Rüdiger & Skwarek, Volker. Secure Cyber-Physical Object Identification in Industrial IoT-Systems. Procedia Manufacturing. 51. 1221-1228. 10.1016/j.promfg.2020.10.171
13. D. M., Thompson., Sean, B., Maynard., Atif, Ahmad, Ahmad. «Cyber-threat intelligence for security decision-making: A review and research agenda for practice». Computers & Security, 132 (2023).:103352–103352. doi: 10.1016/j.cose.2023.103352
14. Rakesh S., Atefeh O., Sajjad A. Machine-learning-enabled intrusion detection system for cellular connected UAV networks // Sensors. – 2021. – Vol. 10, No.1549. – P. 1–28.
15. Mihalache, S. F., Pricop, E., Fattahi, J. (2019). Resilience Enhancement of Cyber-Physical Systems: A Review. In: Mahdavi Tabatabaei, N., Najafi Ravadanegh, S., Bizon, N. (eds) Power Systems Resilience. Power Systems. Springer, Cham. https://doi.org/10.1007/978-3-319-94442-5_11
16. Thulasiraman P., Haakensen T., Callanan A. «Countering Passive Cyber Attacks Against Sink Nodes in Tactical Sensor Networks Using Reactive Route Obfuscation», Elsevier Journal of Network and Computer Applications, Vol. 132, pp. 10–21, April 2019. DOI: 10.1016/j.jnca.2019.01.028
17. Zhang, Dongdong & Li, Chunjiao & Goh, Hui Hwang & Ahmad, Tanveer & Zhu, Hongyu & Liu, Hui & Wu, Thomas. (2022). A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems. Renewable Energy. 189. 1383–1406. 10.1016/j.renene.2022.03.096
18. Zheng, Yu & Li, Zheng & Xu, Xiaolong & Qingzhan, Zhao. (2021). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks. 8, 422–435. DOI: 10.1016/j.dcan.2021.07.006
19. Li, Guangxia & Shen, Yulong & Zhao, Peilin & Lu, Xiao & Liu, Jia & Liu, Yangyang & Hoi, Steven. (2019). Detecting Cyberattacks in Industrial Control Systems Using Online Learning Algorithms. Neurocomputing. 364, 338–348. DOI: 10.1016/j.neucom.2019.07.031
20. J. Leško, M. Schreiner, D. Megyesi and L. Kovács, «Pixhawk PX-4 Autopilot in Control of a Small Unmanned Airplane», 2019 Modern Safety Technologies in Transportation (MOSATT), Kosice, Slovakia, 2019, pp. 90–93, doi: 10.1109/MOSATT48908.2019.8944101
21. Basan, E., Lapina, M., Lesnikov, A., Basyuk, A., Mogilny, A. Trust Monitoring in a Cyber-Physical System for Security Analysis Based on Distributed Computing. In: Alikhanov, A., Lyakhov, P., Samoylenko, I. (eds) Current Problems in Applied Mathematics and Computer Science and Systems. APAMCS 2022. Lecture Notes in Networks and Systems, vol 702. Springer, Cham. https://doi.org/10.1007/978-3-031-34127-4_42
22. 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. https://doi.org/10.3390/drones6010008
23. Basan, E.; Basan, A.; Nekrasov, A. Method for Detecting Abnormal Activity in a Group of Mobile Robots. Sensors 2019, 19, 4007. https://doi.org/10.3390/s19184007
24. Basan, E.; Basan, A.; Mushenko, A.; Nekrasov, A.; Fidge, C.; Lesnikov, A. Analysis of Attack Intensity on Autonomous Mobile Robots. Robotics 2024, 13, 101. https://doi.org/10.3390/robotics13070101