УДК 004.056 **DOI** 10.15622/ia.2020.19.5.6

Д.С. Левшун, Д.А. Гайфулина, А.А. Чечулин, И.В. Котенко

ПРОБЛЕМНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Левшун Д.С., Гайфулина Д.А., Чечулин А.А., Котенко И.В. **Проблемные вопросы информационной безопасности киберфизических систем.**

Аннотация. Представляются анализ и систематизация современных исследований в области обеспечения информационной безопасности киберфизических систем. Рассматриваются проблемные вопросы, связанные с информационной безопасностью подобных систем: «Что атакуют?», «Кто атакует?», «Почему атакуют?», «Как атакуют?» и «Как защититься?». В качестве ответа на первый вопрос даются определение и классификация киберфизических систем по таким атрибутам этих систем, как сложность, связность, критичность и социальный аспект. В качестве ответа на второй и третий вопросы предлагается классификация атакующих по таким атрибутам, как тип доступа, способ доступа, намерения, знания и ресурсы. В качестве ответа на четвертый вопрос рассматривается классификация атакующих действий по таким атрибутам, как субъект и объект, способ воздействия, предпосылки и последствия. В качестве ответа на пятый вопрос предлагается классификация методов и средств защиты по таким атрибутам, как принцип работы, объект защиты и решаемая задача. Научная значимость статьи заключается в систематизации современного состояния исследований в предметной области. Практическая значимость статьи заключается в предоставлении информации о проблемных вопросах безопасности, которые характерны для киберфизических систем, что позволит учитывать их при разработке, администрировании и использовании таких систем.

Ключевые слова: информационная безопасность, киберфизическая система, цель атакующего, модель атакующего, модель атакующих действий, метод и средство защиты.

1. Введение.

Киберфизические системы стали неотъемлемой частью нашей жизни: от электроэнергетики, производства и транспорта, до медицины, торговли и личного пользования [1]. Таким образом, обеспечение защищенности таких систем представляет собой критически важную задачу, решить которую в полной мере, как показывает практика в России и за рубежом, пока не удалось [2]. Это подтверждается, например, тем, что все чаще появляются новости о ботнетах из умных микроволновок и холодильников, используемых для проведения DDoS-атак, а также о взломе изолированных сетей критически важных предприятий через умные датчики и камеры [3]. Этим же обусловлена высокая актуальность выбранной темы.

Предполагается, что данная работа станет отправной точкой для разработчиков, исследователей и системных администраторов в понимании различных аспектов информационной безопасности киберфизических систем. Научная значимость статьи заключается в систематизации современного состояния исследований в предметной области. Практическая значимость статьи заключается в том, что ознакомление с ней позволит лучше понять, какие проблемы информационной безопасности характерны для киберфизических систем с точки зрения объекта атаки, злоумышленника, цели и мотива атаки, способа атаки, а также методов и средств защиты, и учитывать их при разработке, администрировании и использовании таких систем. Даются ответы на следующие вопросы: (1) что является объектом атаки? («Что атакуют?»); (2) кто является субъектом атаки? («Кто атакует?»); (3) каковы намерения атакующих? («Почему атакуют?»); (4) каков способ реализации атаки? («Как атакуют?»); (5) какие методы и средства защиты могут быть применены? («Как защититься?»).

В качестве ответа на первый вопрос в разделе 2 предлагаются определение и классификация киберфизических систем. Данная классификация позволяет оценить критичность системы или ее элементов в соответствии с зависящими от них бизнес-процессами, сложность в соответствии с функциональными возможностями и связность в соответствии с используемыми интерфейсами и протоколами передачи данных. Кроме того, данная классификация позволяет учесть социальный аспект работы системы в соответствии с задействованным персоналом и возможными пользователями.

В качестве ответа на второй и третий вопросы в разделе 3 разрабатывается классификация атакующих. Данная классификация позволяет оценить возможности атакующих в соответствии с типом доступа к системе, уровнем знаний и доступных ресурсов. Кроме того, предложенная классификация позволяет учесть возможные намерения атакующих, в том числе связанные с нарушением конфиденциальности и целостности информации, а также нарушением доступности устройств и перехватом управления ими.

В качестве ответа на четвертый вопрос в разделе 4 формируется классификация атакующих действий. Данная классификация позволяет установить взаимосвязь между атакующим и атакующими действиями в соответствии со знаниями и ресурсами, необходимыми злоумышленнику для их реализации, а также целью, которой соответствует их применение. Кроме того, данная классификация устанавливает взаимосвязь между

атакующими действиями и элементами киберфизической системы, в соответствии с которыми они могут быть реализованы.

В качестве ответа на пятый вопрос в разделе 5 предлагается классификация методов и средств защиты. Данная классификация позволяет оценить возможность реализации атакующих действий в соответствии с используемыми методами и средствами защиты. В разделе 6 представляются основные выводы по каждому из вопросов.

При этом ответы на упомянутые выше вопросы, точно также как и классификации, предложенные в качестве ответа на них, связаны между собой (рис. 1).

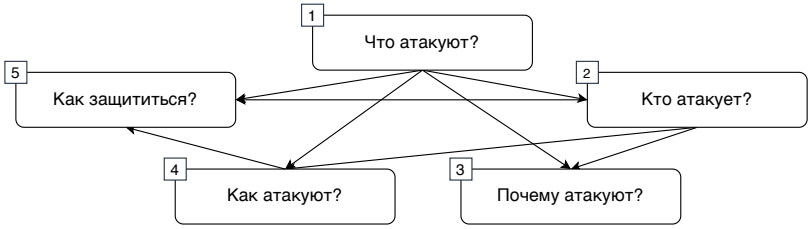

Рис. 1. Взаимосвязь между проблемными вопросами информационной безопасности

Взаимосвязь между вопросами показана направленными стрелками. При этом процесс выстраивания взаимосвязей изначально построен на двух основных понятиях информационной безопасности: злоумышленник («Кто атакует?») и объект атаки («Что атакуют?»). Затем, на основе информации об объекте атаки и злоумышленнике можно предположить цель атакующих («Почему атакуют?), а также используемые им инструменты и подходы («Как атакуют?»). Кроме того, при расширении информации об объекте атаки и злоумышленнике данными об используемых злоумышленником инструментах и подходах, становится возможным предположить эффективные способы противодействия («Как защититься?»). Отметим, что на рисунке показана прямая связь между вопросами, в то время как косвенные связи не отображены – в противном случае была бы связь все ко всем. Каждый из данных вопросов, точно также как и ответы на них, будут рассмотрены более подробно в последующих разделах.

2. Определение и классификация киберфизических систем. Применение киберфизических систем становится все более распространенным и востребованным, так как в этих системах реализована интеграция информационных технологий и устройств взаимодействия с

физическими процессами и объектами. Важно отметить, что в научной литературе пока не существует единого определения киберфизической системы, и в ряде работ присутствуют различные его описания. Термин киберфизическая система впервые был предложен в 2006 году для обозначения комплексов, состоящих из природных объектов, искусственных подсистем и контроллеров [4]. Кроме того, популяризация данного термина связана с проектом Индустрия 4.0 [5], в основе которого лежит внедрение данных систем в промышленность. Так в работе [6] представлен обзор различных типов систем и связанных с ними процессов перехода от мехатроники к облачным системам Интернета вещей или киберфизическим системам. Как правило, следующие системы относят к киберфизическим [7]: системы управления производством; Интернет вещей; «умный дом»; робототехнические системы; беспилотные летательные аппараты; беспилотные автомобили; системы военного назначения.

В исследовании [8] киберфизическая система определяется как новый тип системы, которая является результатом объединения встроенных программных систем, связанных, с одной стороны, с их физической средой с помощью датчиков и исполнительных механизмов, а с другой стороны, с глобальными сетями, такими как Интернет с его данными и услугами. Согласно [9] киберфизическая система представляет собой комплексную техническую систему, которая объединяет сенсорные технологии и технологии вычислений, связи и управления. Оборудование и программное обеспечение системы тесно связаны через сеть, формируя четыре процесса: сбор данных, анализ данных, принятие решений и их выполнение. В работе [10] используется понятие киберфизического пространства для обозначения условной среды, в которой в неразрывной связи существуют физические объекты и их информационные сущности. А в работе [7] понятие киберфизической системы представляется в качестве удобной концепции для представления технологических систем как результата интеграции физических процессов и информационной среды.

Резюмируя, можно выделить следующие характеристики, позволяющие отнести систему к киберфизической: (1) интеграция информационных технологий с физической средой; (2) наличие процессов сбора, хранения, анализа, обработки и предоставления данных; (3) наличие надежной среды передачи данных между элементами системы. Это означает, что киберфизическая система может быть определена как система, которая выполняет функции сбора, хранения, анализа, обработки и предоставления данных от устройств, взаимодействующих с физическими процессами и объектами, а также их тесную интеграцию с информационными технологиями в рамках надежной среды передачи данных. Под информационной безопас-

ностью киберфизической системы понимается обеспечение целостности, конфиденциальности и доступности обрабатываемых данных, а также инфраструктуры и связанных с ней физических процессов. Под информационной безопасностью киберфизической системы также можно понимать защищенность информации и информационных ресурсов этой системы от различного рода угроз (незаконного ознакомления, преобразования, уничтожения информации и нарушения работоспособности системы).

Точно также как при определении киберфизических систем, в научной литературе сложно обозначить единую их классификацию. В обобщенном виде основные атрибуты (признаки) классификации подобных систем можно представить следующим образом: *сложность* в соответствии с функциональными возможностями и используемыми компонентами; *связность* в соответствии с используемыми интерфейсами и протоколами передачи данных; *критичность* в соответствии с зависящими от системы бизнес-процессами; *социальный аспект* в соответствии с характером взаимодействия системы с пользователями и операторами. Понимание данных атрибутов позволяет получить представление о киберфизической системе, помогая определить, что является целью злоумышленника и какие возможности он использует при атаке на данную систему. Отметим, что учитывая множество способов оценки различных атрибутов киберфизических систем, в данном обзоре сделана попытка обобщить предлагаемые в научной и технической литературе решения и представить анализ в виде общего подхода. Рассмотрим каждый из представленных атрибутов более подробно.

Оценка сложности киберфизической системы может быть осуществлена в соответствии с функциональными возможностями данной системы и используемыми ей компонентами. Наиболее активно данные параметры киберфизических систем изучены в работах, связанных с их проектированием. При этом составляющие системы принято разделять на различные уровни в зависимости от функциональности элементов каждого слоя.

Например, авторы [11] предложили сервис-ориентированную архитектуру киберфизических систем, состоящую из таких уровней, как физический, сетевой и уровень сервисов. В исследовании [12] выделяют уровень восприятия, сетевой и прикладной. Задачей физического уровня, или уровня восприятия, является надежное считывание информации с датчиков. Сетевой уровень обеспечивает повсеместный доступ и передачу данных. На уровне сервисов, или прикладном уровне, выполняются функции по сбору, хранению, обработке и представлению данных.

В работах [13, 14] предложена архитектура киберфизической системы, состоящая из пяти уровней, которые содержат: *уровень соединения* – сбор всех видов данных от датчиков и контроллеров системы; *уровень преобразования данных* или *сетевой уровень* – анализ разнородных данных с целью определения значимой информации; *кибернетический уровень* или *уровень конвергенции* – центральный информационный узел в архитектуре, реализующий анализ данных и контроль работы системы; *уровень познания* – представление знаний пользователям, визуализация и принятие решений; *уровень конфигурации* – обратная связь между уровнями, выполнение функций центрального диспетчерского контроля.

Также распространенным представлением архитектуры киберфизических систем является структура из семи уровней модели ISO/OSI – от физического до прикладного уровня [15, 16]. Таким образом, элементы системы могут быть классифицированы по своей функциональности, то есть от места, занимаемого в общей архитектуре.

Киберфизические системы также могут быть классифицированы в зависимости от процессов, связанных с обработкой используемых ими данных. Например, в работе [17] предложен признак классификации данных систем по семантическому уровню используемых для работы данных: *уровень соединения* – использование данных, предоставляемых датчиками; *уровень преобразования* – использование данных от датчиков, после их предварительной обработки и агрегации; *уровень кибернетики* – использование данных от других систем; *уровень познания* – обработка данных датчиков на основе моделирования и дифференциального анализа для диагностики состояния системы; *уровень конфигурации* – использование поступающих данных для адаптации и реконфигурации.

Кроме того, согласно [18] оценку сложности можно также проводить на основе следующих структурных особенностей киберфизических систем: *количество контуров управления* – с одним контуром управления и множеством контуров управления; *структура контуров управления* – одноуровневые и иерархические; *количественный состав элементов* – фиксированный и переменный; *качественный состав элементов* – однородные и гетерогенные; *динамика поведения* – адаптивные и самоорганизующиеся. При этом под адаптацией и самоорганизацией подразумевается реакция на внешние воздействия, способность к прогнозированию предстоящих изменений во внешней среде, проведение внутреннего тестирования и совершенствование собственной организации не только под воздействием внешних факторов, но и в случае условно стабильной работы.

Отметим, что в области искусственных систем не существует четкой границы, разделяющей простые и сложные системы. При этом выделяют два основных способа оценки сложности систем [19]. Первый связан с количеством информации, необходимым для описания системы, и определяет ее дескриптивную сложность. Подобная оценка возможна на основе количественных параметров системы, например таких как число элементов, связей и иерархических уровней, а также непересекающихся системных функций [20]. Второй способ позволяет оценить сложность познания системы и связан с количеством информации, необходимым для уменьшения меры неопределенности системы. При этом дескриптивная сложность и сложность познания дополняют друг друга – возрастание одной сложности влечет за собой увеличение другой. Роль классификации киберфизических систем заключается в ограничении способов описания подобных систем, что задает основу для их оценки.

Оценка связности киберфизической системы может быть осуществлена в соответствии с используемыми в ней интерфейсами и протоколами передачи данных. Данная оценка затрагивает один из важнейших элементов любой системы – процесс организации надежного обмена данными между ее компонентами. При этом существующие телекоммуникационные технологии включают в себя как алгоритмы передачи данных, так и средства их реализации, вплоть до физических каналов связи.

В [18] для оценки связности киберфизических систем предлагается использовать такие признаки, как географическая распределенность и открытость системы. Относительно географической распределенности выделяют: централизованные системы, то есть системы, расположенные в границах одного физического объекта (предприятие, здание и т.п.), и распределенные системы, расположенные на нескольких связанных между собой объектах. Открытость системы определяет характер использования внутренних и внешних (глобальных) сетей и относит киберфизическую систему к системе закрытого типа, если для ее работы используется только внутренняя среда связи, и системе открытого типа, если для работы системы необходим доступ в глобальную сеть Интернет.

В исследовании [17] для оценки связности киберфизических систем предлагается использовать применяемые в них технологии и стандарты связи. При этом технологии характеризуют устройства, используемые системой для взаимодействия с физическими объектами или процессами, например датчики температуры и RFID-метки, в то время как стандарты характеризуют процесс взаимодействия элементов системы между собой, указывая на используемые протоколы и интерфейсы. Протоколы делят на высокоуровневые, низкоуровневые и межуровневые, а для классификации

интерфейсов предлагается использовать различные признаки, характеризующие топологию связи, формат и режим передачи данных, а также функциональное назначение сети.

Используемые протоколы и интерфейсы можно условно разделить на проводные и беспроводные. Беспроводные датчики и исполнительные механизмы играют центральную роль в разработке современных киберфизических систем. В таких сложных гетерогенных системах каналы связи должны отвечать строгим требованиям по пропускной способности, задержке и дальности, а также обладать низким энергопотреблением. В [21] рассматриваются наиболее актуальные стандарты беспроводной связи, такие как: NFC, UHF RFID, ZigBee, Z-Wave, EnOcean, Bluetooth, Wi-Fi, 3GPP, NB-IOT, LoRa и SigFox. При этом выделяют следующие топологии сети: звезда, древовидная, ячеистая и сотовая.

К наиболее распространенным проводным интерфейсам передачи данных между устройствами на основе микроконтроллеров относят UART, SPI, I2C, Ethernet, 1-Wire, Modbus и CAN [22, 23]. Каждый из перечисленных интерфейсов имеет ряд особенностей, влияющих на скорость передачи данных, потребление энергии и доступные дополнительные функции: например, функции адресации и идентификации подключаемых устройств. При этом для данных интерфейсов широко распространены их аппаратные реализации, что привело к их интеграции в большинство современных устройств на основе микроконтроллеров.

Отметим, что глобальная информатизация различных сфер жизнедеятельности человека способствует как развитию существующих спецификаций протоколов сетевого обмена, так и появлению новых протоколов. При этом для устройств киберфизических систем прослеживается тенденция к использованию проприетарных протоколов, то есть протоколов с нерегламентированными (по крайней мере, общедоступно) спецификациями. Подобная ситуация в основном связана со стремлением защитить интеллектуальную и коммерческую собственность компаний, а также усложнить условия анализа сетевых протоколов сторонними исследователями. Это означает, что зачастую трафик в киберфизических системах можно охарактеризовать как трафик большого объема, высокой гетерогенности и неопределенной структуры [24].

Оценка критичности киберфизической системы может быть осуществлена в соответствии с зависящими от нее бизнес-процессами. Для осуществления данной оценки зачастую используются модели бизнес-процессов, а также проводится анализ потенциальных угроз и уязвимостей для последующей оценки рисков и выбора контрмер. При этом риск определяется как способность конкретной угрозы использовать уязвимость

одного или нескольких активов для нанесения ущерба организации [25]. В свою очередь, активы могут представлять собой материальные активы, информацию, программное и аппаратное обеспечение, персонал и нематериальные ресурсы, имеющие ценность для организации.

По определению, критической информационной инфраструктурой является совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов, а также обеспечивающие их взаимодействие информационно-телекоммуникационные сети [26]. Таким образом, к данным объектам могут быть отнесены киберфизические системы, функционирующие в сферах здравоохранения, науки, транспорта, связи, энергетики, финансов, обороны и промышленности. Анализ области применения киберфизических систем представлен в работах [27–29]. Рассмотрим данные исследования более подробно.

В работе [27] выделяются следующие сферы применения киберфизических систем: общественная безопасность, розничная торговля, транспорт, промышленность, здравоохранение, «умный дом», строительство, энергетика. Для каждой сферы определяется конечный потребитель, и приводятся примеры устройств. Авторы [28] проводят обзор существующих решений в области проектирования киберфизических систем, что позволяет выделить следующие области применения: автомобильные системы и транспорт, медицинские системы, умные дома и здания, социальные сети и игровые системы, системы планирования, системы управления, системы питания, системы наблюдения, промышленные системы, авиационно-космические системы, поисковые системы, экологические системы, системы строительства, робототехнические системы и водораспределительные системы. В статье [29] рассматриваются основные составляющие современной интеллектуальной среды, а именно такие концепции как «умный дом», «умное здоровье», «умный город» и «умная фабрика». При этом данные концепции сопоставляются с текущими коммуникационными решениями в области киберфизических систем. Также в данной работе представлен обзор коммуникационных технологий и архитектур подобных систем, а в заключении обсуждаются проблемы, которые остаются открытыми для исследований.

Производственные киберфизические системы характеризуют как объединение автономных и согласованных элементов (от машин до логистических сетей), соединенных друг с другом в соответствии с поставленной целью на всех уровнях производства и способных принимать решения в режиме реального времени [30]. При этом преимущество от внедрения таких систем исследуются повсеместно. Так, в [31] показан процесс

внедрения принципов киберфизических систем в промышленный сектор путем организации работ предприятий в рамках таких технологий, как «умное производство» и «цифровая фабрика». В работах [32, 33] показаны преимущества взаимодействия человека и робототехнических систем в условиях опасной среды. Статья [34] описывает транспортные киберфизические системы, их основные принципы организации и функционирования. В работе [35] предложена парадигма киберфизической строительной системы, представляющая собой конечное множество функциональных компонентов, таких как строительные объекты и комплексы, а также вычислительные ресурсы, интегрированные во включенные физические процессы. В ряде работ [36, 37] приводятся исследования медицинских киберфизических систем для повышения эффективности и безопасности здравоохранения.

Отметим, что критичность киберфизической системы характеризуется последствиями полного или частичного отказа как всей системы, так и отдельных ее элементов. Данные последствия включают в себя как финансовый и репутационный ущерб, так и угрозу жизни и здоровью человека. Одним из способов представления критичности является вектор из следующих составляющих: надежность, последствия отказа, возможность уменьшения вероятности возникновения и тяжести последствий [38]. При этом ранжирование элементов киберфизической системы по степени критичности зависит от типа системы, выбранных частных показателей, а также доступной экспертной информации.

Критичность информации, обрабатываемой в киберфизических системах, как правило, определяется владельцем системы и может зависеть от различных параметров. Например, на критичность информации может влиять ее необходимость для корректного функционирования системы, а также ущерб от потери, модификации или утечки информации. Критичность может вычисляться как с использованием качественных, так и количественных показателей [39].

В исследовании [40] предложена классификация информационных активов в соответствии с требованиями к конфиденциальности, целостности и доступности. Относительно конфиденциальности авторы выделяют информацию, ограниченную к распространению согласно требованиям законодательства; информацию, ограниченную к распространению согласно требованиям организации; и открытую информацию, обеспечение конфиденциальности которой не требуется. Относительно целостности выделяют информацию, нарушение целостности которой может привести к значительному, умеренному или незначительному ущербу, а также информацию, обеспечение целостности которой не требуется. Относительно

доступности выделяют информацию, доступную в любое время, а также информацию, доступную с задержкой до нескольких часов / дней / недель.

На основе предложенной авторами [40] классификации, информация может быть разделена на *критически важную* – конфиденциальность должна быть обеспечена в соответствии с требованиями законодательства, нарушение целостности может привести к значительному ущербу, информация доступна в любое время; *важную* – конфиденциальность должна быть обеспечена в соответствии с требованиями организации, нарушение целостности может привести к умеренному ущербу, информация доступна с задержкой до нескольких часов; и *обычную* – обеспечение конфиденциальности и целостности не требуется.

Оценка социального аспекта киберфизической системы может быть осуществлена в соответствии с характером взаимодействия системы с пользователями и операторами. При этом развитие данного направления исследований дало начало такому термину как социо-киберфизическая система. Важно отметить, что эффективность функционирования киберфизической системы зависит не только от аппаратного и программного обеспечения, но и от взаимодействующего с ней персонала и потребителя. Это означает, что интересы различных социальных групп должны учитываться как на уровне формирования внешнего облика системы, так и при разработке технического задания.

Так, в работе [41] данный факт позволил ввести признак социализации элементов киберфизической системы, который характеризует следующие виды взаимодействия системы с социумом: проектирование, производство, купля/продажа, хранение, выполнение работы (оператор), техническое обслуживание и утилизация. А в исследовании [17] был введен признак человеческого фактора, который описывает следующие типы взаимодействия киберфизических систем с оператором: *автономия* – система принимает все необходимые решения без какого-либо вмешательства оператора; *автоматизация* – система направляет оператора во время выполнения задач, принимая большинство решений; *инструмент* – оператор управляет системой и отвечает за большинство решений; *руководство* – система только предоставляет данные оператору, принимающему все решения.

Зачастую киберфизические системы моделируют интеллектуальные возможности человека в задачах поиска, анализа и синтеза информации об окружающем мире для получения новых знаний и решения поставленных задач. Так, в работе [18] для подобных систем вводится понятие интеллектуализации, описывающее способность системы к обучению, накоплению опыта и принятию решений. Кроме того, в данной работе

вводится понятие динамики реагирования на внешний мир, которое делится на динамику высокого, среднего и низкого уровней. Предполагается, что данный признак может быть использован для оценки способности киберфизических систем к работе с неопределенными и динамическими данными, а также к извлечению знаний из накопленного опыта. Также в данной работе вводится понятие модели восприятия внешнего мира, описывающее как объекты киберфизической системы воспринимают окружающий мир: без модели внешнего мира, с заданной моделью внешнего мира или с моделью внешнего мира, которая генерируется в процессе работы системы.

На основе анализа и систематизации современного состояния исследований авторами были выбраны в качестве основных такие атрибуты классификации, как сложность, связность, критичность и социальный аспект киберфизических систем. С использованием этих атрибутов была построена классификация, представленная на рисунке 2.

Рис. 2. Классификация киберфизических систем

Данная классификация позволяет оценить критичность системы или ее элементов в соответствии с зависящими от них бизнес-процессами, сложность в соответствии с функциональными возможностями и связность в соответствии с используемыми интерфейсами и протоколами передачи данных. Кроме того, данная классификация позволяет учесть социальный аспект работы системы в соответствии с задействованным персоналом и возможным пользователями. Достаточность классификации подтверждается анализом существующих научных и практических

работ, в которых для определения типа системы используются именно вышеперечисленные атрибуты.

Например, относительно сложности можно выделить децентрализованную одноуровневую самоорганизующуюся систему с переменным количеством элементов. Относительно связности – географически распределенную систему с наличием выхода в сеть Интернет, построенную на основе беспроводных и проводных технологий с использованием низкоуровневых и высокоуровневых протоколов. Относительно критичности – систему, используемую в критически важной инфраструктуре с участием человека, обрабатывающую критически важную информацию, отказ которой может повлечь финансовый ущерб. Относительно социального аспекта – автономную систему, выступающую в качестве источника данных, не способную к самообучению и накоплению знаний, имеющую низкую динамику реагирования на внешний мир. Каждая из полученных классификаций позволяет ограничить способ описания исследуемых систем и задает основу для оценки их сложности, связности, критичности и социального аспекта.

3. Анализ и классификация атакующих. Важным этапом в процессе определения угроз безопасности киберфизической системы является идентификация лиц, действия которых могут привести к нарушению конфиденциальности, целостности или доступности системы и возникновению ущерба. Согласно определению в ГОСТ Р. 53114-2008 [42] нарушителем информационной безопасности считается физическое лицо или логический объект, случайно или преднамеренно совершивший действие, которое повлекло негативные последствия. Модель, или профиль, атакующего характеризует возможные пути взаимодействия между атакующим и целевой системой, в частности определяет ограничения для атакующего. Результатом анализа модели атакующего является предположение о видах и потенциале нарушителей, которые могут реализовать угрозы безопасности для киберфизической системы с заданными характеристиками и особенностями функционирования.

Предполагается, что классификация атакующих позволит оценить их возможности в соответствии с типом доступа к системе, уровнем знаний, возможных намерений и доступных ресурсов. *Тип доступа* позволяет различать внешнего и внутреннего нарушителя, рядового пользователя и администратора. *Уровень знаний* является характеристикой атакующего, которая указывает на его технические навыки для инициирования и проведения атаки. Также данная характеристика описывает осведомленность нарушителя об архитектуре целевой системы и существующих мерах защиты. *Намерения* злоумышленника указывают на цель проведения

атаки на систему. Этот параметр трудно поддается количественной оценке и очень динамичен. *Доступные ресурсы* атакующего включают в себя аппаратные и программные ресурсы, которые могут быть использованы для развертывания определенного типа атаки.

Основными нормативными документами, определяющими модель атакующего в Российской Федерации, являются: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [43], «Методика определения угроз безопасности информации в информационных системах» [44] и «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» [45].

В нормативном документе [43] нарушители подразделяются на два типа: внешние и внутренние. При этом к внешним нарушителям относятся нарушители, не имеющие доступа к киберфизической системе, реализующие угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена. При этом внешними нарушителями могут быть разведывательные службы государств, криминальные структуры, конкурирующие организации, недобросовестные партнеры и физические лица. А к внутренним нарушителям относятся нарушители, имеющие доступ к киберфизической системе, включая пользователей и операторов системы, реализующие угрозы непосредственно в системе. При этом возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны организационно-технических мер защиты, в том числе по допуску физических лиц к данным системы и контролю порядка проведения работ.

Более того, внутренние нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа: *категория 1* – лица, имеющие санкционированный доступ к системе и обеспечивающие нормальное ее функционирование; *категория 2* – зарегистрированные пользователи системы, осуществляющие ограниченный доступ к ее ресурсам с рабочего места; *категория 3* – зарегистрированные пользователи системы, осуществляющие удаленный доступ к ее ресурсам; *категория 4* – зарегистрированные пользователи системы с полномочиями администратора безопасности отдельного сегмента системы; *категория 5* – зарегистрированные пользователи с полномочиями системного администратора системы; *категория 6* – зарегистрированные пользователи с полномочиями администратора безопасности системы;

категория 7 – разработчики программного обеспечения системы и лица, обеспечивающие его сопровождение; *категория 8* – разработчики и лица, обеспечивающие поставку, сопровождение и ремонт оборудования системы.

В нормативном документе [44] вводится понятие потенциала нарушителя, который может быть низким, средним и высоким: *низкий потенциал* – нарушитель обладает информацией об уязвимостях отдельных элементов киберфизической системы, опубликованной в общедоступных источниках, при этом для проведения атак использует общедоступные инструменты или инструменты, созданные самостоятельно; *средний потенциал* – нарушитель обладает всеми возможностями нарушителей с низким потенциалом, а также имеет осведомленность о мерах защиты, применяемых в киберфизической системе; кроме того, нарушитель имеет информацию об уязвимостях отдельных элементов системы и применяет находящиеся в свободном доступе программные средства для проведения атак, а также имеет доступ к сведениям о характеристиках и особенностях функционирования киберфизической системы; *высокий потенциал* – нарушитель обладает всеми возможностями нарушителя со средним потенциалом, а также может получить несанкционированный доступ к киберфизической системе из выделенных сетей связи; кроме того, нарушитель данного типа имеет доступ к программному обеспечению и оборудованию системы, хорошо осведомлен о мерах защиты, применяемых в ней, а также обладает информацией об уязвимостях системы, проводит исследования атакуемой системы и использует узкоспециализированные инструменты для достижения своих целей.

В нормативном документе [45] приводятся обобщенные возможности нарушителей, при этом основное внимание уделяется возможностям нарушителя по атакам на средства защиты системы и среду их функционирования: возможность атаковать киберфизическую систему только за пределами контролируемой зоны; возможность атаковать киберфизическую систему в пределах контролируемой зоны, но без физического доступа к ней; возможность атаковать киберфизическую систему в пределах контролируемой зоны с физическим доступом к ней; возможность привлекать специалистов, имеющих опыт разработки и анализа средств защиты, типичных для киберфизических систем.

Важно отметить, что помимо основных нормативных документов, различные классификации атакующих приведены в ряде исследований в области анализа угроз информационной безопасности. Рассмотрим данные работы более подробно.

Например, в работе [46] представлен обзор исследований в области атак на киберфизические системы, а также профилированию атакующих. В результате данного обзора делается вывод, что существующие исследования можно сгруппировать в две основные категории: (1) использующие различные модели атакующих с различными свойствами (например, одна модель для описания внутреннего нарушителя, другая – для описания разведывательной службы государства); (2) определяющие ряд параметров типа знаний, уровня или потенциала нарушителя для различения нарушителей в рамках единой модели. Кроме того, в данной работе предлагается обобщенная классификация атакующих, включающая следующие их виды: *любитель* – использует общедоступные инструменты для атаки на систему и имеет стандартный доступ к оборудованию, программному обеспечению и подключению к интернету; *внутренний нарушитель* – обладает системными привилегиями (например, пользователь, супервайзер, администратор); *хактивист* – использует свои способности для проявления политической активности; *кибертеррорист* – политически мотивированный злоумышленник, который использует свои способности для совершения правонарушений; *киберпреступник* – атакующий с обширными знаниями и навыками в области безопасности, цели которого могут варьироваться от шантажа до шпионажа и саботажа; *группировка* – группа людей, иногда финансируемая государством, целью которой часто является разведка и атаки на критически важные системы общественной инфраструктуры. Авторы также отмечают, что границы между видами атакующих в приведенной классификации достаточно размыты, а потому определение реального злоумышленника в качестве одного конкретного вида может быть затруднительно. Касательно целей атакующих, авторы выделяют: личные, экономические, криминалистические, террористические и политические.

В работе [47] приводится классификация атакующих на киберфизическую систему на примере системы управления водоснабжением. При этом злоумышленник классифицируются по типу доступа к системе и возможностям. Авторы выделяют следующие типы доступа к системе: *тип 0* – злоумышленник не имеет прямого доступа к инфраструктуре и сервисам системы, к применению доступны только методы социальной инженерии; *тип 1* – злоумышленник взаимодействует с инфраструктурой и сервисами системы опосредованно, осуществляя непрямой доступ к ним; *тип 2* – злоумышленник воздействует на инфраструктуру системы или ее сервисы напрямую, находясь при этом на некотором расстоянии от контролируемого периметра; *тип 3* – злоумышленник имеет физический доступ к инфраструктуре системы, но не имеет возможности исследовать

и модифицировать внутренние электронные компоненты; *тип 4* – нарушитель имеет полный доступ к инфраструктуре системы и всем внутренним элементам и интерфейсам.

Авторы выделяют следующие уровни возможностей атакующих: *уровень 1* – использование общедоступных инструментов и эксплуатация известных уязвимостей системы; *уровень 2* – способность выявлять и эксплуатировать ранее неизвестные уязвимости и разрабатывать новые инструменты для воздействия на целевую систему; *уровень 3* – возможности *уровня 2* и наличие почти неограниченных ресурсов для осуществления атак. Таким образом, предложенная авторами классификация позволяет рассматривать атакующих с точки зрения типа доступа, ресурсов и знаний, необходимых для успешной реализации атакующих действий.

На основе анализа и систематизации современного состояния исследований по таким атрибутам классификации атакующих, как тип доступа, способ доступа, намерения, знания и ресурсы, была построена классификация, представленная на рисунке 3.

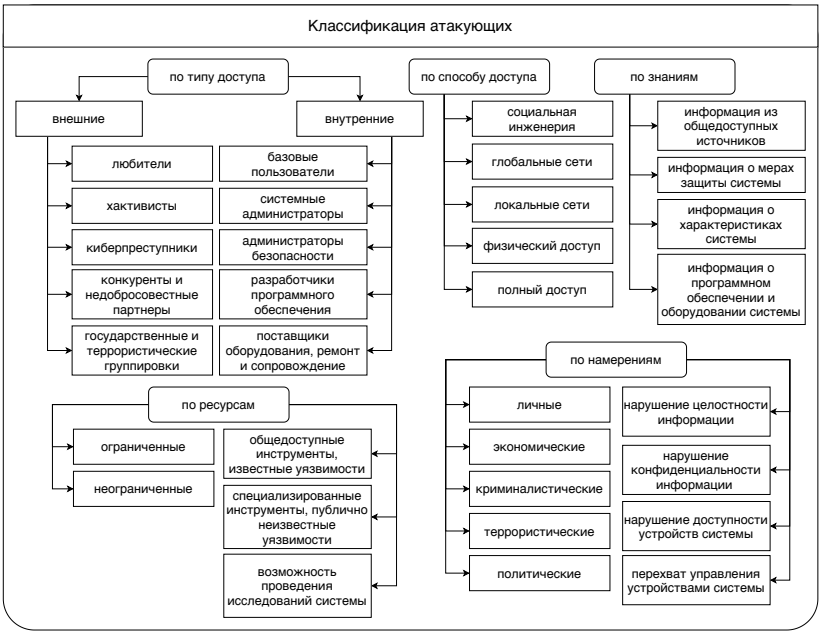

Рис. 3. Классификация атакующих

Данная классификация позволяет оценить возможности атакующих в соответствии с типом и способом доступа к системе, уровнем знаний и доступных ресурсов. Кроме того, данная классификация позволяет учесть возможные намерения атакующих, в том числе связанные с нарушением конфиденциальности и целостности информации, а также нарушением доступности устройств и перехватом управления ими.

4. Анализ и классификация атакующих действий. Не менее важным этапом в процессе определения угроз безопасности киберфизической системы является анализ действий, которые могут привести к нарушению конфиденциальности, целостности или доступности системы. Согласно определению в ГОСТ Р. ИСО/МЭК 27000–2012 [48] атакой является попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования. При этом атаки могут происходить на разных уровнях системы, включать в себя множество этапов, быть растянутыми по времени и затрагивать собой различные ее элементы. И хотя многообразие атакующих действий активно исследуется в научном сообществе, на данный момент не существует единой их классификации. Рассмотрим существующие работы в данном направлении более подробно.

В [49] при классификации сетевых атакующих действий выделяют признаки классификации на основе ресурсов, топологии и трафика: *по влиянию на ресурсы* – направленные (отказ в обслуживании, переполнение таблицы маршрутизации) и ненаправленные (повышение привилегий); *по влиянию на топологию* – снижающие производительность (подмена таблицы маршрутизации, «воронка», «червоточина») и изолирующие («черная дыра»); *по влиянию на трафик* – подслушивающие (сниффинг и анализ трафика) и перехватывающие (понижение привилегий, спуфинг).

В работе [50] при классификации атакующих действий на SCADA-системы выделяют следующие типы атак: ослабление сетевого периметра с помощью бекдоров, эксплуатация уязвимостей в используемых протоколах, перехват управления отдельными устройствами системы, нарушение работы базы данных, перехват и модификация сетевых сообщений, модификация системного времени для прекращения работы средств защиты. В исследовании также предлагается разделить атакующие действия на атаки, направленные на модификацию, перехват или внедрение входных данных от датчиков системы; атаки, направленные на изменение процесса работы системы за счет модификации, перехвата или внедрения данных на уровне взаимодействия между контроллерами системы; атаки, направленные на модификацию логов системы; атаки, направленные на перехват управления отдельными устройствами или прекращение их работы.

В [51] авторы предлагают представлять атакующие действия следующим кортежем данных: субъект, объект, намерения, вектор и последствия. При этом субъектом атаки может быть злоумышленник, природная катастрофа, человеческий фактор, ошибки системы и поддерживающей инфраструктуры. Объектом атаки может быть любой элемент системы, среда передачи данных между ними, а также система в целом. Намерения могут быть криминальными, разведывательными, террористическими или политическими. Векторы атак разделены на перехват, модификацию и подделку данных, а также прекращение их передачи. Последствия атаки включают в себя компрометацию конфиденциальности, целостности, доступности, приватности и надежности системы.

В работе [52] представлена классификация атакующих действий на киберфизические системы. Авторы выделяют атаки на датчики, вычислительные процессы, обратную связь, среду передачи данных и исполнительные механизмы. Рассмотрим примеры для каждого из перечисленных видов атакующих действий более подробно: *атаки на датчики* – выведение оборудования из строя, прекращение подачи питания, использование физических процессов для некорректной работы датчиков; *атаки на вычислительные процессы* – удаление, модификация, подмена или подделка данных, черви, вирусы, трояны; *атаки на обратную связь* – нарушение целостности данных, перехват управления; *атаки на среду передачи данных* – удаление, модификация, подмена или подделка данных, потеря данных, сниффинг; *атаки на исполнительные механизмы* – удаление, модификация, подмена или подделка данных, прекращение подачи питания, модификация аппаратного и программного обеспечения.

В [53] при анализе безопасности киберфизических систем предлагается выделять атакующие действия в соответствии с уровнем киберфизической системы, на котором происходит атака, элементом системы, на который атака направлена, и намерениями злоумышленника. При этом для каждого уровня киберфизической системы авторы представили основные проблемы безопасности и возможные контрмеры. Авторы [54] также предлагают классифицировать атакующие действия на киберфизические системы в соответствии с уровнем системы: физическим, сетевым или приложений. При этом для каждого уровня авторы выделяют соответствующие атакующие действия: *физический уровень* – выведение из строя оборудования, прекращение работы оборудования, прекращение подачи питания, перехват электромагнитных сигналов, внесение помех, отказ в обслуживании, перехват и модификация данных, прекращение передачи данных, перехват управления, несанкционированный доступ; *сетевой уровень* – распределенный отказ в обслуживании, вмешательство

в процесс маршрутизации, прекращение передачи, перенаправление или потеря данных, переполнение буфера; *уровень приложений* – неавторизованный доступ, утечка данных, внедрение вредоносного кода, перехват управления, внедрение вирусов и троянов, инъекции в базу данных.

В работе [55] авторы предлагают разделять атакующие действия на киберфизические системы в соответствии с областью их воздействия: от взаимодействия с физическими устройствами до различных аспектов сетевого взаимодействия (сегментация, топология, используемые технологии и структура). При этом авторы приводят следующую обобщенную их классификацию: перехват и анализ трафика; утечка персональных данных; выведение из строя оборудования; удаленное выполнение вредоносного кода; нарушение целостности исходного кода приложений;эксплуатация уязвимостей сетевых протоколов; отказ в обслуживании.

В [56] предлагается классифицировать атакующие действия на киберфизические системы в соответствии с их причиной, следствием и выполненным действием. Для каждого действия выделяют метод и предусловия, а для причины и следствия – затронутый элемент и влияние на него. В работе [57] предложено классифицировать атакующие действия на киберфизические системы в соответствии с объектом атаки, влиянием на систему и влиянием на человека. Рассмотрим предложенную классификацию более подробно: *по объекту атаки* – сбор данных, среда передачи данных, система управления; *по влиянию на систему* – физическое (некорректная работа, отказ в обслуживание, медленная обработка данных) и кибернетическое (конфиденциальность, целостность, доступность, неаппелируемость); *по влиянию на человека* – эмоциональное воздействие, влияние на приобретенный опыт, причинение физического вреда.

В [58] атакующие действия разделяют на основе способа воздействия на объекты информационной безопасности и по аспекту безопасности, на нарушение которого они направлены. При этом по способу воздействия выделяют: *информационные* – несанкционированный доступ, копирование и хищение информации, нарушение технологии обработки информации; *программные* – использование ошибок и уязвимостей в программном обеспечении, распространение вредоносных программ, установка закладок; *физические* – уничтожение устройств системы, хищение носителей информации, хищение ключей и средств криптографической защиты данных; *радиоэлектронные* – внедрение устройств перехвата информации, перехват, расшифровка, подмена и уничтожение данных в каналах связи; *организационно-правовые* – нарушение законодательства, закупка устаревших программ и устройств. По аспекту безопасности

выделяют атакующие действия, направленные на нарушение *конфиденциальности*, *целостности* и *доступности*.

На основе анализа и систематизации современного состояния исследований по таким атрибутам классификации атакующих действий, как субъект и объект, способ воздействия, предпосылки и последствия, была построена классификация, представленная на рисунке 4.

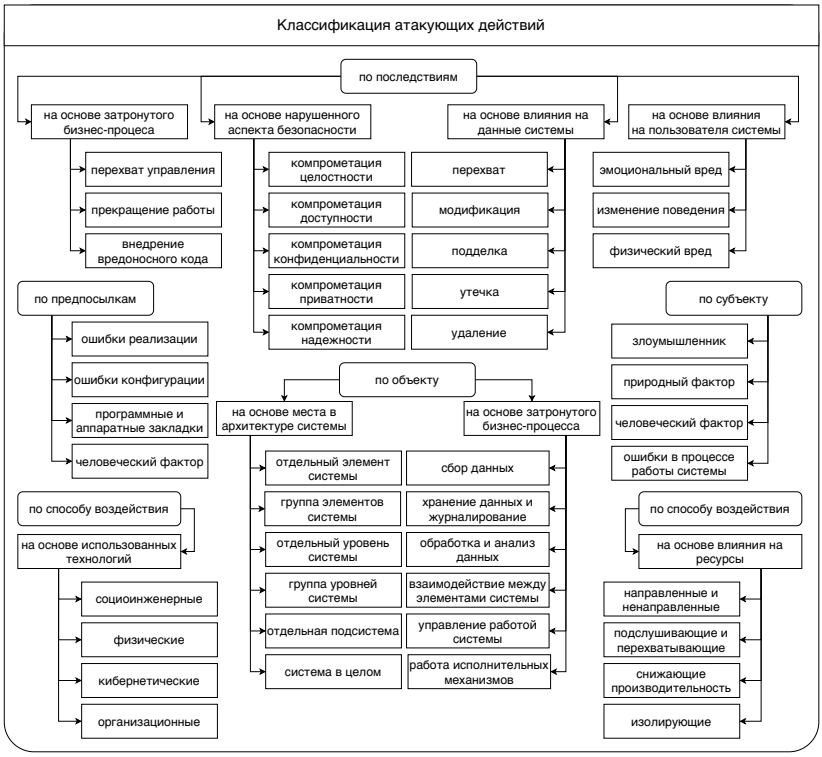

Рис. 4. Классификация атакующих действий

Данная классификация позволяет установить взаимосвязь между атакующим и атакующими действиями в соответствии со знаниями и ресурсами, необходимыми злоумышленнику для их реализации, а также целью, которой соответствует их применение. Кроме того, данная классификация устанавливает взаимосвязь между атакующими действиями и элементами киберфизической системы, в соответствии с которыми они могут быть реализованы.

5. Анализ и классификация методов и средств защиты. Поскольку одной из отличительных черт киберфизических систем является тесная интеграция физических процессов и информационных технологий, число проблем, которые необходимо учитывать при разработке механизмов безопасности для таких систем, значительно выше в сравнении с системами других типов. Кроме того, подобные системы часто обладают динамической инфраструктурой, гетерогенными источниками информации и разнородными хранилищами данных, что также увеличивает сложность требуемой защиты. При этом большинство исследований в данной области направлено на решение различных проблем безопасности на каждом отдельном уровне архитектуры киберфизической системы, а не системы в целом. Рассмотрим существующие работы в данном направлении более подробно.

В работах [12, 59] авторы предлагают определять необходимые методы и средства защиты на основе компонентного состава киберфизической системы. При этом в данных работах представлена классификация методов защиты в соответствии с уровнем системы, защиту которого они обеспечивают. Авторы выделяют следующие уровни: *уровень сбора данных* – сертификация, контроль доступа, аутентификация, легковесное шифрование данных, физическая безопасность устройств, мониторинг окружающей среды, доверительное управление; *уровень передачи данных* – надежная маршрутизация и шифрование данных, аутентификация и согласование ключей, контроль доступа к сети, механизм обнаружения атак; *уровень анализа и обработки данных* – сквозное шифрование, обнаружение вторжений, доверительное управление, аутентификация и авторизация, интеллектуальный анализ данных, форензика, защита персональных данных.

Отметим, что упомянутые выше методы и средства защиты в работе [12] авторы относят к информационному полю системы, помимо которого также выделяют управляющее поле и оценку рисков. Отмечается, что данные механизмы безопасности должны быть разработаны с учетом обеспечения безопасности системы в целом, а не только отдельного ее уровня. При этом данный процесс включает в себя разработку интегрированного межуровневого решения безопасности, которое способно к работе с различными методами и средствами защиты, а также надежно интегрирует данные из разных источников.

В работах [60, 61] представлена архитектура киберфизической системы, которая представляет собой комплексное решение по обеспечению безопасности подобных систем. Данное решение интегрирует в себе как решения по обеспечению физической, так и информационной

безопасности, и состоит из следующих основных частей: *источники данных* – включают в себя различные системы физической и кибернетической безопасности; *модуль сбора данных* – использует различные аппаратные и программные интерфейсы для подключения к источникам данных, при этом полученные данные подлежат процессам предобработки и нормализации; *модуль анализа данных* – включает в себя различные этапы процесса корреляции событий безопасности; *модуль представление данных* – включает в себя такие процессы, как оценка защищенности, выработка контрмер и генерация отчетов.

Отметим, что в соответствии с предложенной авторами архитектурой методы и средства защиты киберфизической системы могут быть классифицированы в соответствии с решаемой задачей.

В работах [7, 62] предлагается рассматривать методы и средства обеспечения безопасности киберфизических систем с точки зрения теории управления. При этом авторы выделяют следующие признаки, которые необходимо учитывать при проектировании защиты системы: наличие обратной связи, наличие контура адаптивного управления и возможность прогнозирования состояния системы. На основе данных признаков авторы предлагают следующую классификацию методов и средств защиты: *статические* – функция управления не изменяется со временем, выходное состояние объекта защиты зависит от постоянных значений управляющих воздействий; *активные* – результаты экспериментального тестирования объекта защиты используются для настройки параметров систем безопасности; *адаптивные* – параметры систем безопасности периодически изменяются для максимизации эффективности защиты на основе характеристик объекта в процессе мониторинга; *динамические* – присутствует динамическая компенсация нежелательных изменений состояния системы в процессе работы.

Отметим, что предложенный авторами подход позволяет сформулировать задачу обеспечения безопасности киберфизических систем как задачу автоматического управления в условиях целенаправленных киберугроз с целью обеспечения устойчивости функционирования.

Авторы [61] предлагают анализировать используемые в киберфизической системе сетевые интерфейсы и протоколы для определения необходимых средств и методов защиты среды передачи данных. При этом особое внимание уделяется процессу взаимодействия между контроллерами системы, где в приведенном эксперименте безопасность шины данных обеспечивается за счет взаимной аутентификация устройств и шифрования передаваемых данных, а надежность – за счет динамической адресации и мониторинга состояния подключаемых устройств, отсутствия

неконтролируемых потерь показаний датчиков и проверки целостности передаваемых данных.

В фреймворке безопасности, предложенном компанией «Cisco» [63] для киберфизических систем, выделяются четыре основных компонента: аутентификация и идентификация, контроль доступа, сетевая политика и аналитика безопасности. При этом базовое применение сетевой политики в первую очередь касается обеспечения соответствия поступающего в сеть трафика заданным правилам, в том числе допустимому диапазону IP-адресов и типам трафика. Пакеты трафика, не соответствующие заданным правилам, признаются в качестве аномальных и должны быть отброшены как можно ближе к границе сети, тем самым сводя к минимуму риск воздействия. Как правило, для обнаружения аномалий используются различные методы, обобщенная классификация которых может быть представлена следующим образом: поведенческие, статистические, интеллектуальный анализ данных, в том числе методы машинного обучения [64].

В работе [65] рассматриваются существующие методы оценки уязвимостей, их роль в процессе оценки рисков безопасности и способы применения. Выделяются три основные группы методов: количественные, качественные и качественно-количественные. Количественные методы оценки рисков позволяют оценить риск в денежных единицах и учитывают частоту нежелательных событий. Качественные методы ранжируют риски относительно друг друга на основе ценности активов, уязвимостей, угроз и защитных мер. При этом на практике в основном применяется качественно-количественный подход, в рамках которого любому качественному уровню сопоставляют определенные диапазоны количественных величин.

В работе [66] авторы рассматривают исследования по оценке уязвимостей киберфизических систем в академических и коммерческих сферах. При этом авторы отмечают, что для последней характерно многообразие подходов к выявлению уязвимостей, в то время как в академической среде подобного не наблюдается.

В [67] рассматриваются методики оценки рисков киберфизических систем с точки зрения экономического эффекта, который проявляет себя даже тогда, когда мотивация злоумышленника не является финансовой. Приводится анализ различных моделей и методик оценки рисков, а также систем оценки уязвимостей.

В работе [68] рассматриваются существующие подходы к оценке и управлению рисками с точки зрения безопасности, защиты и их интеграции. Методы оценки рисков безопасности для киберфизических систем включают в себя: *анализ дерева отказов* – представление, позво-

ляющее связать различные легитимные события и ошибки, возникновение которых может привести к нежелательному событию; *анализ отказов и их последствий* – структурированный метод анализа безопасности системы, позволяющий распознать ситуации, которые приводят к отказу системы или отдельных ее элементов, а также их последствия; *анализ критичности и надежности* – метод анализа безопасности системы, позволяющий оценить степень критичности и надежности процессов системы за счет изучения последствий возможных отклонений; *разработка в соответствии с моделью* – метод разработки имитационных моделей систем реального времени и анализа данных моделей для проверки соответствия требованиям безопасности; *анализ деревьев успеха и целей* – метод анализа безопасности системы, основанный на структурном анализе надежности и риска системы; *анализ аварийных процессов* – метод анализа безопасности, основанный на теоретико-множественной модели и анализе ситуаций, возникновение которых приводит к аварии.

Работа [69] посвящена исследованию основных подходов в области оценки рисков для потенциально опасных объектов. Методы оценки включают в себя количественную оценку с помощью применения математической статистики, экспертную оценку рисков, имитационное моделирование и их комбинации. При этом в исследовании уточняется, что оценка нарушения физической безопасности проводится для каждого конкретного объекта с использованием следующих методов: математическое моделирование распределения вероятности рискового события; экспертная оценка методами Дельфи и ранжирования; численное интегрирование функции риска во времени и пространстве. Это означает, что оценку безопасности киберфизической системы можно представить в виде процесса анализа накопленных данных, мнения экспертов или работы математического аппарата.

Социальный аспект киберфизических систем и, соответственно, возможные атаки социальной инженерии приводят к поиску методов и средств защиты от них. Например, в работе [70] изучаются явления агрессии в социо-киберфизической среде и их влияние на индивидуальное и групповое сознание пользователей. Полученные результаты предлагается использовать при разработке единой социо-киберфизической системы управления данными процессами. Авторы отмечают, что в социальной сети объединение источника с используемыми средствами и формами коммуникации позволяет учесть социальный эффект сообщения, который может быть использован для предсказания проявлений агрессии, давления и других деструктивных явлений.

В работе [71] авторами предложена классификация социоинженерных атак и возможный подход к оценке индекса защищенности корпоративных сетей с точки зрения поведения человека. Предлагаются следующие основные меры защиты от атак социальной инженерии: доступность политики информационной безопасности; проведение инструктажа; мониторинг соблюдения информационной безопасности; политика управления идентификацией; внедрение биометрических систем доступа.

На основе анализа и систематизации современного состояния исследований по таким атрибутам классификации методов и средств защиты, как принцип работы, объект защиты и решаемая задача, была построена классификация, представленная на рисунке 5.

Рис. 5. Классификация методов и средств защиты

Данная классификация позволяет оценить возможность реализации атакующих действий в соответствии с используемыми методами и средствами защиты. Это возможно благодаря тому, что классификация методов и средств защиты по объекту защиты совпадает с классификацией атакующих действий по аналогичному атрибуту. Следовательно, при дальнейшем анализе знаний, ресурсов и возможностей злоумышленника можно будет сделать вывод о реализуемости тех или иных атакующих действий. При этом, классификация методов и средств защиты позволяет установить взаимосвязь между используемой системой защиты и возможностью реализации атакующих действий (рис. 6).

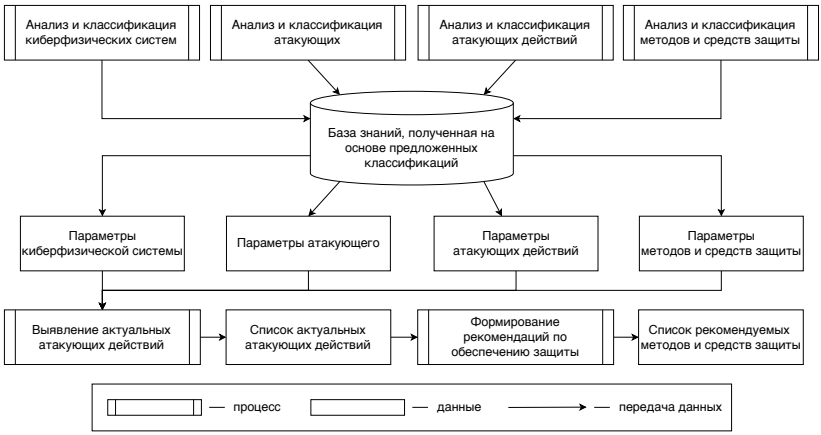

Рис. 6. Процесс выявления актуальных атакующих действий и рекомендации методов и средств защиты

Это означает, что имея информацию о компонентном составе киберфизической системы, можно определить перечень атакующих действий, которым данная система потенциально подвержена. Затем, имея представление об уровне знаний злоумышленника и доступных ему ресурсах, данный перечень атак может быть ограничен точно также как при наличии информации об используемых методах и средствах защиты. Все атакующие действия, оставшиеся после данных преобразований, представляют собой реальную угрозу и должны быть приняты во внимание.

6. Заключение. Проведены анализ и систематизация современных исследований в области обеспечения информационной безопасности киберфизических систем с точки зрения объекта атаки, злоумышленника, цели и мотива атаки, способа атаки, а также методов и средств защиты. Предложено определение киберфизических систем. Дана классификация киберфизических систем по таким атрибутам, как сложность, связность, критичность и социальный аспект. При этом по сложности киберфизические системы разделяют на централизованные и децентрализованные, иерархические и одноуровневые, с постоянным и переменным количеством элементов, адаптивные и неадаптивные, самоорганизующие и несамоорганизующиеся. По связности – географически распределенные и нераспределенные, с наличием и отсутствием выхода в Интернет, беспроводные, проводные и смешанные, с использованием низкоуровневых, высокоуровневых, межуровневых и проприетарных протоколов. По кри-

тичности – используемые в критической и некритической инфраструктуре, работающие с участием или без участия человека, с наличием или отсутствием потенциального ущерба финансам, репутации, пользователям и операторам при частичном и полном отказе, обрабатывающие данные, обладающие или не обладающие критической важностью. По социальному аспекту – автономные и автоматизированные, поддерживающие принятие решений и выступающие только в качестве источника данных, способные и не способные к самообучению и накоплению знаний, высокой, средней и низкой динамики реагирования на внешний мир.

Предложена классификация атакующих по таким атрибутам, как тип доступа, способ доступа, намерения, знания и ресурсы. При этом по типу доступа атакующих разделяют на внешних и внутренних. Внешние атакующие делятся на любителей, хактивистов, киберпреступников, конкурентов и недобросовестных партнеров, государственные и террористические группировки. Внутренние атакующие делятся на базовых пользователей, системных администраторов, администраторов безопасности, разработчиков программного обеспечения, поставщиков оборудования и сотрудников, осуществляющих ремонт и сопровождение системы. По способу доступа выделены – социальная инженерия, глобальные сети, локальные сети, физический и полный доступ. При этом такующий может обладать информацией как из общедоступных источников, так и о мерах защиты, характеристиках, программном обеспечении и оборудовании системы. Ресурсы атакующего могут быть ограничены и неограничены, а также задействованы на общедоступные и специализированные инструменты, известные и публично неизвестные уязвимости, проведение исследований системы. По намерениям выделены личные, экономические, криминалистические, террористические и политические. Кроме того, намерения связаны с нарушение целостности, конфиденциальности и доступности информации, перехватов управления устройствами системы.

Рассмотрена классификация атакующих действий по таким атрибутам, как субъект, объект, способ воздействия, предпосылки и последствия. Субъектом атакующего действия может быть злоумышленник, природный или человеческий фактор, ошибки в процессе работы системы. Объект атакующего действия может быть выделен на основе места в архитектуре системы и затронутого бизнес-процесса. На основе места в архитектуре системы – отдельный элемент, группа элементов, отдельный уровень, группа уровней, отдельная подсистема, система в целом. На основе затронутого бизнес-процесса – сбор данных, хранение данных и журналирование, обработка и анализ данных, взаимодействие между элементами системы, управление работой системы, работа исполнительных

механизмов. Способ воздействия может быть определен на основе использованных технологий и на основе влияния на ресурсы системы. На основе использованных технологий – социоинженерные, физические, кибернетические и организационно-правовые атакующие действия. На основе влияния на ресурсы – направленные и ненаправленные, подслушивающие и перехватывающие, снижающие производительность, изолирующие. По предпосылкам – ошибки реализации и конфигурации, программные и аппаратные закладки, человеческий фактор. Последствия атакующих действия могут быть определены на основе затронутого бизнес-процеса, нарушенного аспекта безопасности, влияния на данные и пользователя системы. На основе затронутого бизнес-процеса – перехват управления, прекращение работы, внедрение вредоносного кода. На основе нарушенного аспекта безопасности – компрометация целостности, доступности, конфиденциальности, приватности и надежности. На основе влияния на данные системы – перехват, модификация, подделка, утечка, удаление. На основе влияния на пользователя системы – эмоциональный вред, изменение поведения, физический вред.

Предложена классификация методов и средств защиты по таким атрибутам, как принцип работы, объект защиты и решаемая задача. По решаемой задаче методы и средства защиты разделяют на элементы сбора, обработки и хранения данных; анализа данных, обнаружения атак и аномалий; мониторинга безопасности и поддержки принятия решений; идентификации, аутентификации и контроля доступа; шифрования и предотвращения утечек данных; оценки рисков и расследования инцидентов; обучения персонала, подготовки инструкций и документов. Объект защиты определяется на основе места в архитектуре системы и затронутого бизнес-процесса. На основе места в архитектуре – отдельный элемент, группа элементов, отдельный уровень, группа уровней, отдельная подсистема и система в целом. На основе затронутого бизнес-процесса – сбор данных, хранение данных и журналирование, обработка и анализ данных, взаимодействие между элементами системы, управление работой системы, работа исполнительных механизмов. По принципу работы – статические, активные, адаптивные, динамические.

Предполагается, что данная статья будет полезна как разработчикам, позволяя ответить на ряд проблемных вопросов информационной безопасности киберфизических систем на этапе их проектирования и поддержки, так и системным администраторам, давая возможность получить представление о состоянии безопасности устройств, которые входят в зону их ответственности. Кроме того, работа будет полезна исследователям и студентам, изучающим проблемы информационной безопасности.

Литература

1. *Десницкий В.А. и др.* Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. Вып. 5. № 48. С. 5–31.
2. *Levshun D., Chechulin A., Kotenko I., Chevalier Y.* Design and Verification Methodology for Secure and Distributed Cyber-Physical Systems // 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). 2019. pp. 1–5.
3. *Pressley A.* Securing connections in the cloud and across IoT devices // Intelligent CIO Europe, 2020.
4. *Baheti R., Gill H.* Cyber-physical systems // The impact of control technology. 2011. vol. 12. no. 1. pp. 161–166.
5. *Schwab K.* The fourth industrial revolution // Currency. 2017.
6. *Hehenberger P. et al.* Design, modelling, simulation and integration of cyber-physical systems: Methods and applications // Computers in Industry. 2016. vol. 82. pp. 273–289.
7. *Зегжда Д.П.* Устойчивость как критерий информационной безопасности киберфизических систем // Проблемы информационной безопасности. Компьютерные системы, 2016. Т. 2. С. 13–18.
8. *Broy M.* Engineering cyber-physical systems: Challenges and foundations // Complex Systems Design & Management. 2013. pp. 1–13.
9. *Li Y., Li X., Wang L., Li Y.* Limestone-gypsum wet flue gas desulfurization based on Cyber-Physical System // 2019 Chinese Control And Decision Conference (CCDC). 2019. pp. 473–477.
10. *Рогозинский Г.Г.* Мультидоменный подход и модели объектов киберфизического пространства в задачах отображения информации // Труды учебных заведений связи. 2017. Т. 3. №. 4. С. 88–93.
11. *Xiao-Le W., Hong-Bin H., Su D., Li-Na C.* A service-oriented architecture framework for cyber-physical systems // Recent Advances in Computer Science and Information Engineering. 2012. pp. 671–676.
12. *Dong P., Han Y., Guo X., Xie F.* A systematic review of studies on cyber physical system security // International Journal of Security and Its Applications. 2015. vol. 9. no. 1. pp. 155–164.
13. *Xia X., Liu C., Wang H., Han Z.* A Design of Cyber-Physical System Architecture for Smart City // Recent Trends in Intelligent Computing, Communication and Devices. 2020. pp. 967–973.
14. *Lee J., Bagheri B., Kao H.A.* A cyber-physical systems architecture for Industry 4.0-based manufacturing systems // Manufacturing letters. 2015. vol. 3. pp. 18–23.
15. *Rojas R.A., Rauch E., Vidoni R., Matt D.T.* Enabling connectivity of cyber-physical production systems: a conceptual framework // Procedia Manufacturing. 2017. vol. 11. pp. 822–829
16. *Alguliyev R., Imamverdiyev Y., Sukhostat L.* Cyber-physical systems and their security issues // Computers in Industry. 2018. vol. 100. pp. 212–223.
17. *Cardin O.* Classification of cyber-physical production systems applications: Proposition of an analysis framework // Computers in Industry. 2019. vol. 104. pp. 11–21.
18. *Zegzhda D.P., Poltavtseva M.A., Lavrova D.S.* Systematization and security assessment of cyber-physical systems // Automatic control and computer sciences. 2017. vol. 51. no. 8. pp. 835–843.
19. *Романов В.Н.* Техника анализа сложных систем // СПб: СЗТУ. 2011. 287 с.
20. *Кохановский В.А., Сергеева М.Х., Комахидзе М.Г.* Оценка сложности систем // Вестник Донского государственного технического университета. 2012. № 4(65). С. 22–26.

21. *Burg A., Chattopadhyay A., Lam K.Y.* Wireless communication and security issues for cyber–physical systems and the Internet-of-Things // Proceedings of the IEEE. 2017. vol. 106. no. 1. pp. 38–60.
22. *Mikhaylov K., Tervonen J.* Evaluation of power efficiency for digital serial interfaces of microcontrollers // 2012 5th International Conference on New Technologies, Mobility and Security (NTMS). 2012. pp. 1–5.
23. *Avatefipour O., Hafeez A., Tayyab M., Malik H.* Linking received packet to the transmitter through physical-fingerprinting of controller area network // 2017 IEEE Workshop on Information Forensics and Security (WIFS). 2017. pp. 1–6.
24. *Гайфулина Д.А., Котенко И.В., Федорченко А.В.* Методика лексической разметки структурированных бинарных данных сетевого трафика для задач анализа протоколов в условиях неопределенности // Системы управления, связи и безопасности. 2019. № 4. С. 280–299.
25. *Дойникова Е.В.* Оценка защищенности и выбор защитных мер в компьютерных сетях на основе графов атак и зависимостей сервисов. // Диссертация на соискание ученой степени кандидата технических наук. 2017. 207 с.
26. Федеральный закон “О безопасности критической информационной инфраструктуры Российской Федерации” от 26.07.2017№ 187-ФЗ (последняя редакция) // АО «Консультант Плюс».
27. *Stallings W.* The internet of things: network and security architecture // Internet Protoc. J. 2015. vol. 18. no. 4. pp. 2–24.
28. *Khaitan S.K., McCalley J.D.* Design techniques and applications of cyberphysical systems: A survey // IEEE Systems Journal. 2014. vol. 9. no. 2. pp. 350–365.
29. *Gomez C. et al.* Internet of Things for enabling smart environments: A technology-centric perspective // Journal of Ambient Intelligence and Smart Environments. 2019. vol. 11. no. 1. pp. 23–43.
30. *Monostori L.* Cyber-physical production systems: Roots, expectations and R&D challenges // Procedia Cirp. 2014. vol. 17. pp. 9–13.
31. *Гурьянов А.В., Заколдаев Д.А., Жаринов И.О., Нечаев В.А.* Принципы организации цифровых проектных и производственных предприятий Индустрии 4.0 // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 3. С. 421–427.
32. *Nikolakis N., Maratos V., Makris S.* A cyber physical system (CPS) approach for safe human-robot collaboration in a shared workplace // Robotics and Computer-Integrated Manufacturing. 2019. vol. 56. pp. 233–243.
33. *Liu H., Wang L.* Remote human–robot collaboration: A cyber–physical system application for hazard manufacturing environment // Journal of Manufacturing Systems. 2020. vol. 54. pp. 24–34.
34. *Лёвин Б.А., Розенберг И.Н., Цветков В.Я.* Транспортные кибер-физические системы // Наука и технологии железных дорог. 2017. Т. 3. № 3. С. 3.
35. *Волков А.А.* Кибернетика строительных систем. Киберфизические строительные системы // Промышленное и гражданское строительство. 2017. №. 9. С. 4–7.
36. *Dey N. et al.* Medical cyber-physical systems: A survey // Journal of medical systems. 2018. vol. 42. no. 4. pp. 74.
37. *Shishvan O.R., Zois D.S., Soyata T.* Incorporating Artificial Intelligence into Medical Cyber-Physical Systems: A Survey // Connected Health in Smart Cities. Springer, Cham. 2020. pp. 153–178.
38. *Попов Д.С.* Информационное обеспечение технологической подготовки ремонтного производства на транспорте // Вестник Сибирского государственного университета путей сообщения. 2007. № 17. С. 163–168.

39. *Федорченко А.В., Дойникова Е.В., Котенко И.В.* Автоматизированное определение активов и оценка их критичности для анализа защищенности информационных систем // Труды СПИИРАН. 2019. Т. 18. № 5. С. 1182–1211.
40. *Коптенков М.М.* Категорирование информации –– первый шаг к обеспечению информационной безопасности организации // Безопасность информационных технологий. 2011. Т. 18. № 4. С. 117–119.
41. *Микони С.В.* Модель участников жизненного цикла социо-киберфизической системы // Технологическая перспектива в рамках евразийского пространства: новые рынки и точки экономического роста. 2019. С. 341–347.
42. ГОСТ Р. 53114-2008 Защита информации // Обеспечение информационной безопасности в организации. Основные термины и определения. 2008.
43. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // Федеральная служба по техническому и экспортному контролю (ФСТЭК России), 15 февраля 2008 г.
44. Методика определения угроз безопасности информации в информационных системах // Федеральная служба по техническому и экспортному контролю (ФСТЭК России), проект, 2015 г.
45. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности // Федеральная служба безопасности (ФСБ России), 31 марта 2015 года, № 149/7/2/6-432.
46. *Rocchetto M., Tippenhauer N.O.* On attacker models and profiles for cyber-physical systems // European Symposium on Research in Computer Security. 2016. pp. 427–449.
47. *Десницкий В. А.* Модель киберфизической системы управления водоснабжением для анализа инцидентов безопасности // Информационные технологии и телекоммуникации. 2017. Т. 5. № 3. С. 93–102.
48. ГОСТ Р. ИСО/МЭК 27000–2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология // М.: ФГУП «СТАНДАРТИНФОРМ». 2014.
49. *Mayzaud A., Badonnel R., Chrisment I.* A Taxonomy of Attacks in RPL-based Internet of Things. 2016.
50. *Zhu B., Joseph A., Sastry S.* A taxonomy of cyber attacks on SCADA systems // 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing. 2011. pp. 380–388.
51. *Humayed A., Lin J., Li F., Luo B.* Cyber-physical systems security – A survey // IEEE Internet of Things Journal. 2017. vol. 4. no. 6. pp. 1802–1831.
52. *Alguliyev R., Imamverdiyev Y., Sukhostat L.* Cyber-physical systems and their security issues // Computers in Industry. 2018. vol. 100. pp. 212–223.
53. *Ashibani Y., Mahmoud Q.H.* Cyber physical systems security: Analysis, challenges and solutions // Computers & Security. 2017. vol. 68. pp. 81–97.
54. *Gao Y. et al.* Analysis of security threats and vulnerability for cyber-physical systems // Proceedings of 2013 3rd International Conference on Computer Science and Network Technology. 2013. pp. 50–55.
55. *Makhdoom I. et al.* Anatomy of threats to the internet of things // IEEE Communications Surveys & Tutorials. 2018. vol. 21. no. 2. pp. 1636–1675.
56. *Yampolskiy M. et al.* A language for describing attacks on cyber-physical systems // International Journal of Critical Infrastructure Protection. 2015. vol. 8. pp. 40–52.
57. *Heartfield R. et al.* A taxonomy of cyber-physical threats and impact in the smart home // Computers & Security. 2018. vol. 78. pp. 398–428.

58. *Алексеев Д.М., Иваненко К.Н., Убирайло В.Н.* Классификация угроз информационной безопасности // Символ науки. 2016. № 9-1. С. 18–20.
59. *Ashibani Y., Mahmoud Q. H.* Cyber-physical systems security: Analysis, challenges and solutions // Computers & Security. 2017. vol. 68. pp. 81–97.
60. *Desnitsky V., Levshun D., Chechulin A., Kotenko I.* Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System // JoWUA. 2016. vol. 7. no. 2. pp. 60–80.
61. *Котенко И. В. и др.* Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3(27). С. 29–38.
62. *Зегжда Д.П. и др.* Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасностию 2018. № 2(26). С. 2–14.
63. *Frahim J.* Securing the Internet of Things: A Proposed Framework // Cisco White Paper, March 2015.
64. *Гайфулина Д.А.* Аналитический обзор методов обнаружения аномалий сетевого уровня киберфизических систем // Альманах научных работ молодых ученых Уни-верситета ИТМО. 2018. Т. 1. С. 4–5.
65. *Котенко И.В., Дойникова Е.В.* Методы оценивания уязвимостей: использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. 2011. № 4. С. 74–81.
66. *Desmit Z., Elhabashy A.E., Wells L.J., Camelio J.A.* An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems // Journal of Manufacturing Systems. 2017. vol. 43. pp. 339–351.
67. *Radanliev P. et al.* Future developments in cyber risk assessment for the internet of things // Computers in Industry. 2018. vol. 102. pp. 14–22.
68. *Lyu X., Ding Y., Yang S.H.* Safety and security risk assessment in cyber-physical systems // IET Cyber-Physical Systems: Theory & Applications. 2019. vol. 4. no. 3. pp. 221–232.
69. *Телегина М.В., Янников И.М., Куделькин В.А., Ушаков И.С.* Модели и методы оценки безопасности критически важных и потенциально опасных объектов // Интеллектуальные системы в производстве. 2017. Т. 15. № 1. С. 118–121.
70. *Кулагина И.В., Исхакова А.О., Галин Р.Р.* Моделирование практик агрессии в социо-киберфизической среде // Вестник Томского государственного университета. Философия. Социология. Политология. 2019. № 52. С. 147–161.
71. *Гарате В.Г.* Анализ уровня защищенности корпоративных компьютерных сетей в контексте социоинженерных атак // Известия СПбГЭТУ «ЛЭТИ». 2017. Т. 3. С. 12–15.

Левшун Дмитрий Сергеевич — младший научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: безопасность в соответствии с проектом, проектирование, моделирование и верификация киберфизических систем. Число научных публикаций – 47. levshun@comsec.spb.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-26-42; факс: +7(812)328-44-50.

Гайфулина Диана Альбертовна — младший научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПб ФИЦ РАН). Область научных интересов: неструктурированных данных, обнаружение

атак и аномалий. Число научных публикаций – 19. gaifulina@comsec.spb.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-26-42; факс: +7(812)328-44-50.

Чечулин Андрей Алексеевич — канд. техн. наук, доцент, ведущий научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: безопас-ность компьютерных сетей, обнаружение вторжений, анализ уязвимостей, визуализация, безопасность встроенных устройств, анализ социальных сетей. Число научных публикаций – 100. chechulin@comsec.spb.ru; 14 линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-71-81; факс: +7(812)328-44-50.

Котенко Игорь Витальевич — д-р техн. наук, профессор, главный научный сотрудник, лаборатория проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН). Область научных интересов: информационная безопасность, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, ложные информационные системы, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибертерроризму; искусственный интеллект, в том числе многоагентные системы, мягкие и эволюционные вычисления, машинное обучение, извлечение знаний, анализ и объединение данных, интеллектуальные системы поддержки принятия решений; телекоммуникационные системы, в том числе поддержка принятия решений и планирование для систем связи. Число научных публикаций – 450. ivkote@comsec.spb.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-71-81; факс: +7(812)328-44-50.

Поддержка исследований. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-17-50205.

DOI 10.15622/ia.2020.19.5.6

D. Levshun, D. Gaifulina, A. Chechulin, I. Kotenko

PROBLEMATIC ISSUES OF INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEMS

Levshun D., Gaifulina D., Chechulin A., Kotenko I. **Problematic Issues of Information Security of Cyber-Physical Systems.**

Abstract. This paper is an analysis and systematization of modern research in the field of cyber-physical system information security. The problematic issues of information security of such systems are considered: «What is being attacked?», «Who is attacking?», «Why is someone attacking?», «How is someone attacking?» and «How to protect the system?». As an answer to the first question, the paper proposes a definition and classification of cyber-physical systems according to such criteria as complexity, connectivity, criticality and social aspect. As an answer to the second and the third questions, the paper describes a classification of attacker according to such criteria as type of access, method of access, intentions, knowledge and resources. As an answer to the fourth question, the paper contains a classification of attack actions according to such criteria as subject and object, method of influence, prerequisites and consequences. As an answer to the fifth question, the paper proposes a classification of protection methods and security tools according to such criteria as principle of operation, object of protection and task to be solved. The scientific significance of the paper is systematization of a current state of the art in the subject area. The practical value of the paper is providing information about security issues that are specific to cyber-physical systems, which will allow one to develop, manage and use such systems in a more secure way.

Keywords: information security, cyber-physical system, target of the attacker, model of the attacker, model of attack actions, protection method, security tool.

Levshun Dmitry — Junior Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: security by design, design, modeling and verification of cyber-physical systems. The number of publications – 47. levshun@comsec.spb.ru; 39, 14-th Line V.O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-26-42; fax: +7(812)328-44-50.

Gaifulina Diana — Junior Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: data mining, analysis of unstructured data, detection of attacks and anomalies. The number of publications – 19. gaifulina@comsec.spb.ru; 39, 14-th Line V.O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-26-42; fax: +7(812)328-44-50.

Chechulin Andrey — Ph.D., Associate Professor, Leading Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: computer network security, intrusion detection, vulnerability analysis, visualization, IoT security, social networks analysis. The number of publications – 100. chechulin@comsec.spb.ru; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-71-81; fax: +7(812)328-44-50.

Kotenko Igor — Ph.D., Dr.Sci., Professor, Chief Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). Research interests: : information security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism; artificial intelligence, including

multi-agent frameworks and systems, agent-based modeling and simulation, soft and evolutionary computing, machine learning, data mining, data and information fusion; telecommunications, including decision making and planning for telecommunication systems. The number of publications – 450. ivkote@comsec.spb.ru; 39, 14-th Line V.O., 199178, Saint-Petersburg, Russia; office phone: +7(812)328-71-81; fax: +7(812)328-44-50.

Acknowledgements. The reported study was funded by RFBR, project number 19-17-50205.

References

1. Desnitsky V.A. et al. [Combined Design Technique for Secure Embedded Devices Exemplified by a Perimeter Protection System]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2016. vol. 5. no. 48. pp. 5–31. (In Russ.).
2. Levshun D., Chechulin A., Kotenko I., Chevalier Y. Design and Verification Methodology for Secure and Distributed Cyber-Physical Systems. 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). 2019. pp. 1–5.
3. Pressley A. Securing connections in the cloud and across IoT devices // Intelligent CIO Europe, 2020.
4. Baheti R., Gill H. Cyber-physical systems. *The impact of control technology*. 2011. vol. 12. no. 1. pp. 161–166.
5. Schwab K. The fourth industrial revolution. Currency. 2017.
6. Hehenberger P. et al. Design, modelling, simulation and integration of cyber-physical systems: Methods and applications. *Computers in Industry*. 2016. vol. 82. pp. 273–289.
7. Zegzhda D.P. [Stability as information security criteria for cyber-physical systems]. *Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy — Information Security Problems. Computer Systems*. 2016. Issue 2. pp. 13–18. (In Russ.).
8. Broy M. Engineering cyber-physical systems: Challenges and foundations. Complex Systems Design & Management. 2013. pp. 1–13.
9. Li Y., Li X., Wang L., Li Y. Limestone-gypsum wet flue gas desulfurization based on Cyber-Physical System. 2019 Chinese Control And Decision Conference (CCDC). 2019. pp. 473–477.
10. Rogozinsky G.G. [Multi-domain approach and models of cyber-physical objects in information representation systems]. *Trudy uchebnyh zavedenij svyazi –- Proceedings of Telecommunication Universities*. 2017. Issue 3. vol. 4. pp. 88–93. (In Russ.).
11. Xiao-Le W., Hong-Bin H., Su D., Li-Na C. A service-oriented architecture framework for cyber-physical systems. Recent Advances in Computer Science and Information Engineering. 2012. pp. 671–676.
12. Dong P., Han Y., Guo X., Xie F. A systematic review of studies on cyber physical system security. *International Journal of Security and Its Applications*. 2015. vol. 9. no. 1. pp. 155–164.
13. Xia X., Liu C., Wang H., Han Z. A Design of Cyber-Physical System Architecture for Smart City. Recent Trends in Intelligent Computing, Communication and Devices. 2020. pp. 967–973.
14. Lee J., Bagheri B., Kao H.A. A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing letters*. 2015. vol. 3. pp. 18–23.
15. Rojas R. A., Rauch E., Vidoni R., Matt D.T. Enabling connectivity of cyber-physical production systems: a conceptual framework. *Procedia Manufacturing*. 2017. vol. 11. pp. 822–829.
16. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues. *Computers in Industry*. 2018. vol. 100. pp. 212–223.
17. Cardin O. Classification of cyber-physical production systems applications: Proposition of an analysis framework. *Computers in Industry*. 2019. vol. 104. pp. 11–21.

18. Zegzhda D.P., Poltavtseva M.A., Lavrova D.S. Systematization and security assessment of cyber-physical systems. *Automatic control and computer sciences*. 2017. vol. 51. no. 8. pp. 835–843.
19. Romanov V.N. [Approach for complex systems analysis]. SPb: SZTU. 2011. 287 p. (In Russ.).
20. Kohanovskiy V.A., Sergeyeva M.H., Komakhidze M.G. [System complexity index]. *Vestnik Donskogo gosudarstvennogo tekhnicheskogo universiteta – Advanced Engineering Research*. 2012. vol. 4(65). pp. 22–26. (In Russ.).
21. Burg A., Chattopadhyay A., Lam K.Y. Wireless communication and security issues for cyber–physical systems and the Internet-of-Things. *Proceedings of the IEEE*. 2017. vol. 106. no. 1. pp. 38–60.
22. Mikhaylov K., Tervonen J. Evaluation of power efficiency for digital serial interfaces of microcontrollers. 2012 5th International Conference on New Technologies, Mobility and Security (NTMS). 2012. pp. 1–5.
23. Avatefipour O., Hafeez A., Tayyab M., Malik H. Linking received packet to the transmitter through physical-fingerprinting of controller area network. 2017 IEEE Workshop on Information Forensics and Security (WIFS). 2017. pp. 1–6.
24. Gaifulina D.A., Kotenko I.V., Fedorchenko A.V. [A Technique for Lexical Markup of Structured Binary Data for Problems of Protocols Analysis in Uncertainty Conditions]. *Sistemy upravleniya, svyazi i bezopasnosti -– Systems of Control, Communication and Security*. 2019. vol. 4. pp. 280–299. (In Russ.).
25. Doynikova E.V. [Security assessment and selection of protective measures in computer networks based on attack graphs and service dependencies]. *Dissertaciya na soiskanie uchenoj stepeni kandidata tekhnicheskih nauk – Dissertation for the degree of candidate of technical sciences*. 2017. 207 p. (In Russ.).
26. Federal'nyj zakon «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii» ot 26.07.2017 № 187-FZ (poslednyaya redakciya) – Federal Law «On the Security of the Critical Information Infrastructure of the Russian Federation» dated July 26, 2017 No. 187-FZ (last edition)]. Consultant Plus. (In Russ.).
27. Stallings W. The internet of things: network and security architecture. *Internet Protoc. J*. 2015. vol. 18. no. 4. pp. 2–24.
28. Khaitan S.K., McCalley J.D. Design techniques and applications of cyberphysical systems: A survey. *IEEE Systems Journal*. 2014. vol. 9. no. 2. pp. 350–365.
29. Gomez C. et al. Internet of Things for enabling smart environments: A technology-centric perspective. *Journal of Ambient Intelligence and Smart Environments*. 2019. vol. 11. no. 1. pp. 23–43.
30. Monostori L. Cyber-physical production systems: Roots, expectations and R&D challenges. *Procedia Cirp*. 2014. vol. 17. pp. 9–13.
31. Gurjanov A.V., Zakoldaev D.A., Zharinov I.O., Nechaev V.A. [Design concepts for digital project and production companies of Industry 4.0 standard]. *Nauchno-tekhnicheskij vestnik informacionnyh tekhnologij, mekhaniki i optiki -– Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2018. Issue 18. vol. 3. pp. 421-427. (In Russ.).
32. Nikolakis N., Maratos V., Makris S. A cyber physical system (CPS) approach for safe human-robot collaboration in a shared workplace. *Robotics and Computer-Integrated Manufacturing*. 2019. vol. 56. pp. 233–243.
33. Liu H., Wang L. Remote human–robot collaboration: A cyber–physical system application for hazard manufacturing environment. *Journal of Manufacturing Systems*. 2020. vol. 54. pp. 24–34.
34. Levin B.A., Rosenberg I.N., Tsvetkov V.Y. [Transport cyber-physical systems]. *Nauka i tekhnologii zheleznyh dorog — Science and technology of railways*. 2017. Issue 3. vol. 3. pp. 3. (In Russ.).

35. Volkov A A. [Cybernetics of construction systems]. *Promyshlennoe i grazhdanskoe stroitel'stvo — Cyber-physical construction systems*. 2017. vol. 9. pp. 4–7. (In Russ.).
36. Dey N. et al. Medical cyber-physical systems: A survey. *Journal of medical systems*. 2018. vol. 42. no. 4. pp. 74.
37. Shishvan O.R., Zois D.S., Soyata T. Incorporating Artificial Intelligence into Medical Cyber-Physical Systems: A Survey. *Connected Health in Smart Cities*. 2020. pp. 153–178.
38. Popov D.S. [Information support for technological preparation of repair production in transport]. *Vestnik Sibirskogo gosudarstvennogo universiteta putej soobshcheniya -– Journal of the Siberian State Transport University*. 2007. vol. 17. pp. 163–168. (In Russ.).
39. Fedorchenko A.V., Doynikova E.V., Kotenko I.V. [Automated detection of assets and calculation of their criticality for the analysis of information system security]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2019. Issue 18(5). pp. 1182–1211. (In Russ.).
40. Koptenkov M.M. [Information categorization is the first step to ensuring the information security of an organization]. *Bezopasnost Informatsionnykh Tekhnologiy — IT Security*. 2011. Issue 18. vol. 4. pp. 117–119.
41. Mikoni S.V. [Model of the participants in the life cycle of a socio-cyber-physical system]. *Tekhnologicheskaya perspektiva v ramkah evrazijskogo prostranstva: novye rynki i tochki ekonomicheskogo rosta – Technological perspective within the Eurasian space: new markets and points of economic growth*. 2019. pp. 341–347. (In Russ.).
42. GOST R. 53114-2008 Information security. Ensuring information security in the organization. Basic terms and definitions. 2008. (In Russ.).
43. The basic model of threats to the security of personal data during their processing in personal data information systems. Federal Service for Technical and Export Control (FSTEC of Russia), February 15, 2008. (In Russ.).
44. Metodika opredeleniya ugroz bezopasnosti informacii v informacionnyh sistemah [Methodology for determining threats to information security in information systems]. Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSTEK Rossii), proekt, 2015. (In Russ.).
45. Methodological recommendations for the development of regulatory legal acts that determine threats to the security of personal data, relevant when processing personal data in information systems of personal data used in the implementation of relevant activities. Federal Security Service (FSB of Russia), March 31, 2015, No. 149/7/2/6-432. (In Russ.).
46. Rocchetto M., Tippenhauer N.O. On attacker models and profiles for cyber-physical systems. European Symposium on Research in Computer Security. 2016. pp. 427–449.
47. Desnitsky V.A. [A Modeling and Analysis of Security Incidents in a Cyber-Physical System for Water Supply Management]. *Informacionnye tekhnologii i telekommunikacii – Telecom IT*. 2017. vol. 5. no. 3. pp. 93–102. (In Russ.).
48. GOST R. ISO/IEC 27000–2012 Information technology. Security methods and means. Information security management systems. General overview and terminology. Moscow: FGUP STANDARTINFORM. 2014. (In Russ.).
49. Mayzaud A., Badonnel R., Chrisment I. A Taxonomy of Attacks in RPL-based Internet of Things. 2016.
50. Zhu B., Joseph A., Sastry S. . A taxonomy of cyber attacks on SCADA systems. 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing. 2011. pp. 380–388.
51. Humayed A., Lin J., Li F., Luo B. Cyber-physical systems security – A survey. *IEEE Internet of Things Journal*. 2017. vol. 4. no. 6. pp. 1802–1831.
52. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues. *Computers in Industry*. 2018. vol. 100. pp. 212–223.
53. Ashibani Y., Mahmoud Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*. 2017. vol. 68. pp. 81–97.

54. Gao Y. et al. Analysis of security threats and vulnerability for cyber-physical systems. Proceedings of 2013 3rd International Conference on Computer Science and Network Technology. 2013. pp. 50–55.
55. Makhdoom et al. Anatomy of threats to the internet of things. *IEEE Communications Surveys & Tutorials*. 2018. vol. 21. no. 2. pp. 1636–1675.
56. Yampolskiy et al. A language for describing attacks on cyber-physical systems. *International Journal of Critical Infrastructure Protection*. 2015. vol. 8. pp. 40–52.
57. Heartfield et al. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*. 2018. vol. 78. pp. 398–428.
58. Alekseev D.M., Ivanenko K.N., Ubirailo V.N. [Classification of threats to information security]. *Simvol nauki -– Science symbol*. 2016. vol. 9-1. pp. 18–20. (In Russ.).
59. Ashibani Y., Mahmoud Q.H. Cyber-physical systems security: Analysis, challenges and solutions. *Computers & Security*. 2017. vol. 68. pp. 81–97.
60. Desnitsky V., Levshun D., Chechulin A., Kotenko I.V. Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System. *JoWUA*. 2016. vol. 7. no. 2. pp. 60–80.
61. Kotenko I.V. et al. [Integrated approach to provide security of cyber-physical systems based on microcontrollers]. *Voprosy Kiberbezopasnosti -– Voprosy Kiberbezopasnosti*. 2018. vol. 3(27). pp. 29-38. (In Russ.).
62. Zegzhda D.P. et al. [Advanced production technologies security in the era of digital transformation]. *Voprosy Kiberbezopasnosti – Voprosy Kiberbezopasnosti*. 2018. vol. 2(26). pp. 2–14. (In Russ.).
63. Frahim J. Securing the Internet of Things: A Proposed Framework. Cisco White Paper, March 2015.
64. Gaifulina D.A. [Analytical review of methods for detecting network layer anomalies in cyber-physical systems]. *Al'manah nauchnyh rabot molodyh uchenyh Universiteta ITMO — Almanac of scientific works of young scientists of ITMO University*. 2018. Issue 1. pp. 4–5. (In Russ.).
65. Kotenko I.V., Doynikova E.V. [Vulnerabilities assessment techniques: use for the computer systems security analysis]. *Zashchita informacii. Insajd -– Information Security*. Inside. 2011. vol. 4. pp. 74–81. (In Russ.).
66. Desmit Z., Elhabashy A.E., Wells L.J., Camelio J.A. An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. *Journal of Manufacturing Systems*. 2017. vol. 43. pp. 339–351.
67. Radanliev P. et al. Future developments in cyber risk assessment for the internet of things. *Computers in Industry*. 2018. vol. 102. pp. 14–22.
68. Lyu X., Ding Y., Yang S.H. Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*. 2019. vol. 4. no. 3. pp. 221–232.
69. Telegina M.V., Yannikov I.M., Kudelkin V.A., Ushakov I.S. [Models and methods for safety assessment of potentially dangerous objects]. *Intellektual'nye sistemy v proizvodstve — Intelligent systems in production*. 2017. Issue 15. vol. 1. pp. 118–121. (In Russ.).
70. Kulagina I.V., Iskhakova A.O., Galin R.R. [Modeling the practice of aggression in the socio-cyber-physical environment]. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya — Tomsk State University Journal of Philosophy, Sociology and Political Science*. 2019. vol. 52. pp. 147–161. (In Russ.).
71. Garate V.G. Analysis of security level of corporate networks in the context of socioengineering attacks. *Izvestiya SPbGETU «LETI» – Izvestiya ETU LETI*. 2017. Issue 3. pp. 12–15. (In Russ.).