УДК 004.065 **DOI** 10.15622/ia.2020.19.5.7

Р.В. Мещеряков, А.Ю. Исхаков, О.О. Евсютин

СОВРЕМЕННЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ В ПРОТОКОЛАХ УПРАВЛЕНИЯ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Мещеряков Р.В., Исхаков А.Ю., Евсютин О.О. **Современные методы обеспечения целостности данных в протоколах управления киберфизических систем.**

Аннотация. В настоящее время остро стоит проблема создания методологического обеспечения безопасности киберфизических систем, в частности проектирования и реализации подсистем информационной безопасности. При этом ландшафт угроз и уязвимостей, характерных для применяемого в киберфизических системах широкого спектра аппаратных и программных технологий, чрезвычайно широк и сложен. В этом контексте безопасность протоколов прикладного уровня имеет первостепенное значение, поскольку эти протоколы лежат в основе взаимодействия между приложениями и службами, работающими на различных устройствах, а также в облачных инфраструктурах. В условиях постоянного взаимодействия исследуемых систем с реальной физической инфраструктурой актуальна проблема определения эффективных мер по обеспечению целостности передаваемых команд управления, поскольку нарушение выполняемых критически важных процессов может затрагивать жизнь и здоровье людей. Представлен обзор основных методов обеспечения целостности данных в протоколах управления киберфизических систем, а также обзор уязвимостей протоколов прикладного уровня, широко используемых в различных киберфизических системах. Рассмотрены классические методы обеспечения целостности и новые методы, в частности блокчейн, а также основные направления повышения эффективности протоколов обеспечения целостности данных в киберфизических системах. Анализ уязвимостей прикладного уровня проведен на примере наиболее популярных спецификаций MQTT, CoAP, AMQP, DDS, XMPP, а также их реализаций. Установлено, что несмотря на наличие во всех перечисленных протоколах базовых механизмов обеспечения безопасности, исследователи продолжают регулярно выявлять уязвимости в популярных реализациях, что зачастую ставит под угрозу сервисы критической инфраструктуры. В ходе подготовки обзора существующих методов обеспечения целостности данных для исследуемого класса систем были определены ключевые проблемы интеграции этих методов и способы их решения.

Ключевые слова: киберфизическая система, интернет вещей, протокол, блокчейн, цифровые водяные знаки, аутентификация

1. Введение. Исследование методов и подходов к обеспечению информационной безопасности в киберфизических системах является важной задачей на пути формирования единой методологии развития средств автоматизации и управления в сложных гетерогенных системах, переход к которым позволит человечеству выйти на более высокий уровень индустриализации, снизить количество и уровень последствий техногенных производственных катастроф и повысить качество жизни.

Актуальность задач обеспечения комплексной безопасности киберфизических систем за счет специализированных научно обоснован-

ных методов организации защищенного взаимодействия компонентов обусловлена стремительным ростом кибератак по всему миру – сложных, многошаговых и зачастую адаптированных под целевую инфраструктуру. Так, после нашумевшей Mirai [1] двумя другими крупными ботнет-атаками стали Hajime и Reaper, которые направлены на большое количество умных устройств. В апреле 2020 года исследователи в области кибербезопасности зафиксировали множественные атаки ботнета «Dark Nexus», использующего уязвимые гаджеты Интернета вещей для выполнения распределенных атак «отказ в обслуживании». На данный момент атака включает более 1400 ботов, функционирующих в режиме обратного прокси-сервера, и направлена на критически важные объекты Китая, Таиланда, Бразилии, Южной Кореи и России [2].

Подобные вторжения в киберфизические системы производственных процессов, запущенных в критической инфраструктуре, недопустимы. Именно поэтому обсуждению данной проблемы и выдвижению собственных подходов и методов посвящено множество публикаций российских и зарубежных авторов, а также материалов докладов профильных конференций. Такая активность показывает заинтересованность мирового научного сообщества в создании комплексных решений в данной области.

К числу отличительных особенностей подавляющего большинства решений для киберфизических систем являются высокие требования к уровню функционирования, безопасности и надежности протоколов управления, а также необходимость сочетания многопрофильных задач в рамках одного производственного процесса, ведения непрерывного мониторинга и анализа состояния системы. Наряду с этим не менее важной отличительной особенностью является проблема применимости современных средств и методов обеспечения безопасности. Перспективные направления адаптации методов и алгоритмов защиты информации для их использования в киберфизических системах зачастую обусловлено низкой вычислительной способностью компонентов таких комплексов.

Результаты исследований [3-5] говорят о том, что наибольшей популярностью у злоумышленников пользуются именно протоколы прикладного уровня (Application layer), в рамках которых разработчики реализуют проприетарные правила и механизмы (форматы запросов и ответов, программные интерфейсы приложений (application programming interface, API), запросы к уровню представления, обработчики ошибок и т.д.). Это связано с высокой вероятностью наличия уязвимостей нулевого дня, что обусловлено низкой степенью защиты применяемых методов вследствие игнорирования разработчиками не-

обходимого анализа со стороны научного сообщества и исследователей в сфере информационной и кибернетической безопасности. В [6] представлено исследование типовых протоколов безопасности DTLS и IPSec, применяемых в контексте защиты рассматриваемых инфраструктур. Приведенный в вышеуказанной работе анализ подчеркивает, что эти протоколы не отвечают некоторым требованиям безопасности, кроме того, существует проблема высокой нагрузки и масштабирования, когда речь заходит о применении протоколов DTLS и IPSec в устройствах инфраструктуры Интернета вещей (Internet of Things, IoT) с низкими вычислительными способностями. Указанные обстоятельства вынуждают разработчиков еще раз задуматься об обеспечении безопасности непосредственно на уровне приложений. В этой связи в рамках данной статьи обзор будет ориентирован на методы защиты, предназначенные для применения на прикладном уровне модели OSI (The Open Systems Interconnection model). В качестве перспективных мер по нейтрализации угроз нарушения целостности данных приводится анализ мирового опыта по применению технологии блокчейн и цифровых водяных знаков в качестве механизмов обеспечения информационной безопасности киберфизических систем.

Статья организована следующим образом. В разделе 2 представлена общая характеристика рассматриваемых протоколов прикладного уровня, которые применяются для управления объектами киберфизических систем и элементами инфраструктуры Интернета вещей. В разделе 3 рассматриваются потенциальные риски безопасности, основанные на консолидации записей из баз данных Common Vulnerabilities and Exposures (CVE) и банка данных угроз ФСТЭК России, характерных для исследуемых протоколов, а также мировых практик и научных исследований. В разделе 4 представлен обзор современных научных публикаций в контексте обеспечения целостности данных для выбранной предметной области, в том числе приводится обзор научных публикаций, рассматривающих интеграцию технологии блокчейн в киберфизические системы, а также обзор методов встраивания цифровых водяных знаков в качестве механизма обеспечения целостности и аутентификации данных. В разделе 5 обсуждаются основные результаты анализа актуальных методов противодействия угрозам обеспечения целостности данных, передаваемых в протоколах управления киберфизических систем.

2. Краткий обзор исследуемых протоколов. Необходимо отметить, что рассматриваемые в статье протоколы зачастую относят и к протоколам Интернета вещей. Это связано с тем, что в научной среде инфраструктуры IoT и киберфизических систем имеют схожие опре-

деления. Оба понятия соответствуют тенденции интеграции цифровых возможностей, подразумевающей тесное взаимодействие между физическими и вычислительными процессами, в том числе с применением соответствующих систем и сетевой инфраструктуры. При этом в ходе анализа публикаций по соответствующей тематике у разных исследователей прослеживаются разногласия в архитектуре представления данных концепций. Так различные эксперты используют противоречивые определения о разного рода перекрытии понятий «Интернет вещей» и «киберфизические системы» – частичное или полное включение одного множества в другое, обратные включения, эквивалентность. Тем не менее наблюдается тенденция сближения этих терминов [7] – несмотря на различие в происхождении, современные системы, рассматриваемые с точки зрения функциональности, попадают под формальное определение обоих понятий.

Исследования, направленные на систематизацию различных категорий киберфизических систем [8, 9], применяют разнообразные подходы к их классификации:

– по уровням интеграции (connection, conversion, cyber и т.д.);

– по доменам применения (энергетика, робототехника, транспортные задачи, военные объекты, системы здравоохранения и т.д.);

– по степени взаимодействия с человеком.

Очевидно, что многообразие и гетерогенность используемого оборудования в той или иной области применения, а также различные архитектурные модели киберфизических и социокиберфизических систем требуют дифференцированного подхода в подборе оптимального перечня методов и средств обеспечения информационной безопасности. В данной статье обзор протоколов ограничивается наиболее популярными стандартами и реализациями [10], применяемыми при разработке киберфизических систем и IoT-решений:

– CoAP;
– MQTT;
– DTLS;
– Eddystone;
– HTTP2;
– iBeacon;
– PJON;
– STOMP;
– Websocket;
– XMPP.

Как было отмечено ранее, протоколы связи на прикладном уровне являются фундаментальным элементом киберфизической эко-

системы, поскольку они лежат в основе всех взаимодействий между элементами IoT, а также между устройствами и облачной инфраструктурой [11-12]. Типичные функции, реализованные этими протоколами, связаны с обменом сообщениями и обнаружением сервисов. В частности, обмен сообщениями относится к передаче информации (данных и управляющих воздействий) между устройствами, а обнаружение – к детектированию предлагаемых устройств и сервисов. В таблице 1 приведены основные характеристики наиболее популярных протоколов обмена сообщениями, а именно: MQTT, CoAP, AMQP, DDS и XMPP. Протоколы обнаружения служб (такие как mDNS и SSDP) не предоставляют функционал передачи команд управления, поэтому не являются предметом настоящего исследования.

Таблица 1. Основные характеристики протоколов прикладного уровня

Протокол	MQTT	CoAP	AMQP	DDS	XMPP
Стандарт	OASIS	IETF	OASIS	OMG	IETF
Архитектура	Централизованная	Централизованная	Централизованная	Децентрализованная	Централизованная
Модель взаимодействия	Pub/Sub	Req/Resp	Pub/Sub	Pub/Sub	Pub/Sub, Req/Resp
Транспорт	TCP	UDP	TCP	TCP / UDP	TCP
Обеспечение конфиденциальности	TLS	DTLS	TLS	TLS/ DTLS	TLS
Аутентификация	Проприетарная	Проприетарная	SASL	Проприетарная	SASL
Авторизация	-	-	-	Проприетарная	Проприетарная

Содержимое таблицы 1 демонстрирует, что протоколы различаются по многим аспектам, таким как архитектурные модели и модели взаимодействия, режимы транспорта данных и встроенные механизмы обеспечения безопасности. Некоторые протоколы используют централизованные, то есть клиент-серверные архитектуры, в то время как другие основаны на полностью распределенных архитектурах. Например, для таких протоколов, как MQTT и AMQP, брокер играет роль сервера и взаимодействует с клиентами, получая и пересылая сообщения. Обмен сообщениями, как правило, осуществляется в соответствии с моделями публикации/подписки или запроса/ответа. Несмотря на то, что все рассмотренные протоколы предназначены для

подключения устройств в распределенной сети, выбор того или иного протокола определяется исходя из необходимости выполнения конкретных операционных сценариев и архитектуры внедрения, особенно когда приняты во внимание ключевые системные требования, такие как производительность, качество обслуживания, интероперабельность, обеспечение отказоустойчивости и безопасности [13].

3. Анализ уязвимостей. Несмотря на то, что во всех перечисленных протоколах в той или иной степени предусмотрены базовые механизмы обеспечения безопасности, исследователи регулярно находят уязвимости, которые ставят под угрозы сервисы критической инфраструктуры. На рисунке 1 представлена статистика национальной базы данных уязвимостей США (National vulnerability database, NVD) за последние 2,5 года по указанным протоколам.

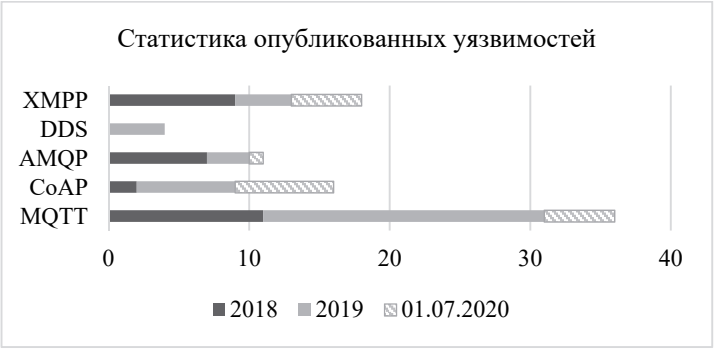

Рис. 1. Статистика по количеству уязвимостей протоколов (реализаций), опубликованных в базе NVD с 2018 года

Проведенный авторами анализ CVE, связанных с сервисами и системами, которые используют протокол MQTT, позволяет судить не только о характере выявленных угроз безопасности [14] в конкретных инфраструктурах, но и выявить общую тенденцию уязвимых точек данного стандарта. Так, в ходе анализа поисковой выдачи специализированной системы vulners.com было найдено более 70 записей (в том числе эксплойты, бюллетени безопасности и другие публикации), прямо или косвенно связанные с исследуемым протоколом. Поиск по NVD показал, что из более 36 тематических записей, опубликованных начиная с 2018 года, большинство уязвимостей связано с недостаточной проверкой сообщений сервисами и службами. Например, «ошибка неучтенной единицы» (CVE-2020-10070) в декодере длины пакета MQTT проекта Zephyr может привести к повреждению памяти и возможному удаленному выполнению кода. Уязвимость (CVE-2019-

11779) характеризует возможность вредоносного клиента MQTT вызвать переполнение стека, просто отправив *subscribe*-пакет, содержащий тему из не менее 65400 «/» символов. Аналогично пакет *connect* в сочетании с вредоносным пакетом запроса *unsubscribe* может быть использован для того, чтобы вызвать атаку типа «отказ в обслуживании» (DoS) на брокера (CVE-2019-6241). Другие вопросы безопасности относятся к категориям аутентификации и авторизации. Широко известен яркий пример (CVE-2017-7650), когда клиенты, определяющие имя пользователя как «#», полностью игнорируют механизмы контроля доступа и подписываются на все темы MQTT. В публикации [15] обсуждается несколько причин того, почему существует множество систем IoT на основе MQTT, в которых не реализованы адекватные механизмы безопасности, а также представлены демонстрационные сценарии типовых атак. Интерес представляет исследование [16], в рамках которого авторы провели оценку атак отказа в обслуживании, нацеленных на брокеров различных реализаций данного протокола, а также представили консолидированную модель угроз MQTT. Стоит отметить обзор популярной среди злоумышленников схемы DoS-атаки посредством отправки брокеру сообщений с высоким уровнем QoS.

Обзор публикаций, обобщающих уязвимости CoAP [17-19], а также БДУ ФСТЭК (BDU:2019-00925, BDU:2020-02424) и NVD (CVE-2020-12884, CVE-2020-10063, CVE-2019-17212, CVE-2018-12679, CVE-2018-12680) позволяет утверждать, что наиболее частая проблема безопасности в реализациях связана с некорректной проверкой объема подаваемых данных и содержимого сообщений. Использование этих уязвимостей может привести к таким последствиям, как утечка памяти и удаленное выполнение кода, что ставит под угрозу работоспособность всей киберфизической системы, использующей CoAP. Также известны уязвимости популярных библиотек CoAP, позволяющие в результате подмены адреса источника и некорректной обработки ответных сообщений (CVE-2019-9750) выполнять распределенную атаку типа «отказ в обслуживании».

Согласно базе данных NVD и научного сообщества [5, 20] сервисы киберфизических систем, использующие AMQP, неоднократно подвергались критике со стороны исследователей в области информационной безопасности. Так в ходе изучения практических исследований безопасности протокола AMQP было выявлено множество фактов некорректной настройки брокера, что зачастую приводит к серьезным угрозам для объекта. Кроме того, сам пользовательский веб-интерфейс управления зачастую становится источником критических

угроз (например, CVE-2015-0862, CVE-2016-0734, CVE-2017-4965). Безусловно, в отличие от MQTT и CoAP такие защитные механизмы, как TLS и SASL, как правило, включены по умолчанию, что снижает потенциальные риски безопасности. Тем не менее последствия уязвимостей (в большинстве случаев, связанных с компонентом брокера) позволяют злоумышленникам использовать повышение привилегий, выполнять перехват трафика в обход аутентификации и выполнять атаки типа «отказ в обслуживании» (CVE-2015-7559, CVE-2017-15699, CVE-2015-0224, CVE-2015-1499) и MiTM. В частности, некоторые уязвимости (CVE-2018-11087, CVE-2018-8119, CVE-2016-4467, CVE-2019-3845), связанные с отсутствием процедур проверки имени хоста и сертификатов, а также контролем доступа в очередях сообщений, позволяют злоумышленникам подделывать идентификационные данные и перехватывать команды управления.

DDS протокол поддерживает TLS, DTLS и другие механизмы безопасности. Последняя спецификация безопасности DDS OMG определяет архитектуру, основанную на наборе встроенных плагинов. Так плагины предлагают механизмы аутентификации и авторизации DataWriters и DataReaders, что позволяет избежать несанкционированной публикации и подписки. Тем не менее как спецификация, так и плагины подвержены уязвимостям. В частности, протокол рукопожатия, используемый для авторизации, как представлено в [21], может позволить злоумышленникам обнаружить потенциально конфиденциальную информацию о доступности в сети DDS (CVE-2019-15135). На практике [22] далеко не все продукты и сервисы DDS соответствуют спецификации безопасности, и даже совместимые реализации могут быть подвержены уязвимостям.

Протокол XMPP включает поддержку TLS для обеспечения конфиденциальности и целостности данных, а также обеспечивает поддержку SASL для процесса аутентификации. Подобные механизмы встроены в основные спецификации протокола и включены по умолчанию. Тем не менее отсутствие сквозной поддержки шифрования делает протокол уязвимым для различных типов угроз. В дополнение к этому за последние 5 лет было обнаружено более 90 CVE, которые в основном относятся к процессам аутентификации и проверки сообщений в тех или иных сервисах (например, CVE-2019-1845, CVE-2019-12855, CVE-2014-3451, CVE-2018-15720, CVE-2016-1307). В [23] рассматриваются уязвимости, связанные не с XMPP напрямую, а с пользовательскими функциями, встраиваемыми разработчиками поверх протокола, а также проведено моделирование атак типа «отказ в обслуживании» на сервер XMPP.

4. Методы защиты данных в протоколах киберфизических систем.

4.1. Классические методы обеспечения контроля целостности данных. Существует два больших научных направления, занимающихся целостностью данных в телекоммуникационных системах: теория кодирования и криптография. Одной из ключевых задач теории кодирования является обнаружение и исправление ошибок в передаваемых и хранимых данных. Обнаружение ошибок обеспечивает контроль целостности данных, в то время как исправление ошибок обеспечивает саму целостность. Во втором случае речь идет о так называемом помехоустойчивом кодировании.

Помехоустойчивое кодирование представляет собой метод, вводящий избыточность в передаваемую информацию для последующего восстановления ее целостности [24]. Кроме того, идеи, лежащие в основе помехоустойчивого кодирования, позволяют строить на его основе криптографические системы, устойчивые к атакам с использованием квантового компьютера [25]. Помехоустойчивые коды можно разделить на две основные группы: блоковые (блочные) коды [26] и сверточные коды [27]. Основное отличие блочных кодов от сверточных заключается в том, что блочные коды оперируют информационными последовательностями конечной длины, в то время как длина информационной последовательности для сверточного кода не ограничена. На практике широко используют следующие классы блочных кодов: коды Галлагера с малой плотностью проверок на четность (англ. LDPC), основным свойством которых является разреженная структура их порождающей матрицы, что оптимизирует процедуру их декодирования [28]; турбо-коды, объединяющие в себе идеи сверточного и блочного кодирования [29]; полярные коды, предложенные Ариканом в 2008 году и достигающие пропускной способности двоичного канала без памяти [30]. Также известны каскадные коды, позволяющие комбинировать различные методы конструирования блочных кодов с целью построения мощных кодов с хорошей корректирующей способностью [31].

Криптография представляет собой науку, занимающуюся поиском и исследованием математических методов преобразования информации с целью ее защиты. В отличие от теории кодирования криптография не позволяет обеспечивать целостности данных, а позволяет лишь ее контролировать. Другим отличием криптографических методов от методов теории кодирования является ориентированность на защиту от целенаправленных вредоносных действий, в то время как помехоустойчивое кодирование предназначено для защиты от естественных помех, присущих каналам передачи данных.

Выделяют три группы методов, предназначенных для обеспечения контроля целостности:

– хеширование;

– коды аутентичности сообщений (MAC);

– электронная подпись.

Поскольку область криптографических методов защиты информации на практике достаточно жестко ограничивается немногочисленным перечнем государственных стандартов, дадим определения перечисленным методам и приведем соответствующие стандарты.

Хешированием называется преобразование входной битовой строки произвольной длины в выходную битовую строку фиксированной длины. Функция, реализующая данное преобразование, называется хеш-функцией. Значение хеш-функции называют хеш-значением, хеш-кодом. Хеш-код является своего рода характеристическим признаком входной последовательности данных, по которому эти данные можно впоследствии идентифицировать, а также установить факт их изменения. Для этого хеш-код добавляется к передаваемым или хранимым данным и при необходимости рассчитывается повторно. Действующим отечественным стандартом хеширования является ГОСТ Р 34.11–2012 [32].

Кодом аутентичности сообщения (имитовставкой) называется контрольная комбинация, зависящая от открытого текста и секретного ключа, и использующаяся для обнаружения всех случайных или преднамеренных изменений в открытом тексте. Отличие от хеш-кода заключается в том, что в выработке имитовставки участвует секретный ключ. Поэтому рассчитать имитовставку может лишь законный пользователь, знающий этот ключ. Основные современные схемы выработки имитовставки строятся на основе симметричных блочных шифров при использовании последних в специальном режиме. Такой режим описан в отечественном стандарте ГОСТ Р 34.13–2015 [33].

Наконец, электронной подписью сообщения называется некоторая битовая строка, зависящая от самого сообщения и секретного ключа, известного только автору подписи. При возникновении спорной ситуации, связанной с отказом подписывающего от факта подписи им некоторого сообщения либо с попыткой подделки подписи, третья сторона (арбитр) должна иметь возможность разрешить спор. Существуют две основные схемы построения электронной цифровой подписи: на основе симметричных криптосистем и на основе криптографии с открытым ключом. На практике обычно используется вторая схема. Отечественный стандарт электронной подписи ГОСТ Р 34.10–2012 построен на математическом аппарате эллиптических кривых [34].

4.2. Основные направления развития и оптимизации методов защиты данных в M2M протоколах. Можно выделить большое количество исследований, посвященных различным вариантам модернизациям TLS и разработке решений, адаптированных для интеграции в ресурсы киберфизических систем с поддержкой MQTT [35-41]. Например, в [38] предлагают подход, основанный на алгоритме Blake2 [42], который позволяет обеспечить целостность и конфиденциальность передаваемых сообщений. Этот подход очень перспективный с точки зрения производительности на устройствах с ограниченными возможностями, особенно подходит для промышленных условий, в которых датчики и контроллеры обмениваются заранее определенными объемами данных. Авторы [37] предлагают безопасную версию MQTT, которая использует новый пакет управления, называемый Spublish, для публикации зашифрованных данных с помощью легковесной криптографии на основе эллиптических кривых [43, 44]. Для внедрения усовершенствованного механизма контроля доступа на устройствах с ограниченным доступом, где применение TLS ограничено, авторы [35] разработали облегченный механизм аутентификации. Аналогичным образом в [39] предлагают архитектуру MQTT, основанную на модифицированной версии OAuth framework [45], в которой два набора учетных данных используются устройствами для доступа к брокеру. С целью внедрения правил политик безопасности в работе [46] предлагается реализация специального коннектора, который перехватывает сообщения от брокера. Это позволяет не только генерировать соответствующие уведомления безопасности, но и способствует выполнению определенных контрмер. В основе коннектора лежит применение технологии прокси-сервера, отслеживающего обмен данными между клиентами и серверами.

Исследование [47] посвящено вопросам аутентификации, целостности, конфиденциальности, неотказуемости и контроля доступа для применения протокола XMPP в рамках передачи данных по сенсорным сетям. Связь на основе XMPP в сенсорных сетях ISO/IEC/IEEE 21451 использует маркер безопасности имени пользователя и пароля, а также интегрированные технологии публикации/подписки (pub/sub) и управления доступом на основе ролей. С использованием предложенного механизма обмен сообщениями ISO/IEC/IEEE 21451 осуществляется на основе модели pub/sub с использованием расширенного протокола доступа к простому объекту безопасности через XMPP.

Интерес вызывает работа [48], где авторы сравнивают библиотеки DTLS, поддерживаемые реализациями CoAP, которые наиболее часто встречаются в промышленных средах IoT. В работе [49] сравнивают сервисы безопасности, предоставляемые IPSec, TLS и DTLS.

Данное исследование показывает, что несмотря на популярность и признание мировым сообществом алгоритмов, заложенных в IPSEC и TLS, их реализации в киберфизических системах зачастую приводят к существенным нагрузкам, что может значительно снизить вычислительные ресурсы устройств. В нескольких работах эти проблемы были решены путем сосредоточения внимания на разработке легких решений для обеспечения безопасности канала связи между клиентами и серверами. В частности, в [50] представлена архитектура FDTLS, которая сочетает в себе безопасность на уровне хранилища и сети/связи для устройств с ограниченными ресурсами при использовании DTLS. Отмечено, что применяемая схема FDTLS решает проблемы избыточных операций за счет использования генерации асимметричных ключей, виртуального однорангового узла и оптимизации хранения на основе сокращения заголовков. Полученные авторами результаты с использованием реализации на основе Contiki на платформах OpenMote показывают, что по сравнению с использованием хранилища и сетевой безопасности отдельно FDTLS может уменьшить задержку ответов при передаче пакетов, а также способствовать экономии энергии. Усовершенствование протокола DTLS с точки зрения модернизации непосредственно криптографических алгоритмов является актуальной научной задачей. В частности, в работе [51] предлагается схема уменьшения числа рукопожатий для DTLS. Как показано в [52, 53], интеграция DTLS поверх CoAP на основе криптографии эллиптических кривых помогает свести к минимуму нагрузку на вычислительные ресурсы при преобразованиях данных. Задачи оптимизации протокола коснулись и вопросов энергоэффективности вычислительных аппаратных устройств [54]. По заявлению авторов, их аппаратная реализация протокола DTLS 1.3 повышает энергоэффективность в 438 раз по сравнению с программным обеспечением, наряду с размером кода и использованием памяти данных всего 8 КБ и 3 КБ соответственно. Криптографические ускорители соединены с процессором RISC-V с низким энергопотреблением на кристалле для тестирования приложений, выходящих за рамки DTLS, с экономией энергии до двух порядков. Тестовый чип, изготовленный на 65-нм CMOS, демонстрирует сеансы DTLS с аппаратным ускорением при потреблении 44,08 мкДж на квитирование и 0,89 нДж на байт зашифрованных данных при 16 МГц и 0,8 В.

4.3. Применение технологии блокчейн для подтверждения достоверности транзакций в киберфизических системах. Относительно новым направлением в кибербезопасности является направление, связанное с созданием механизмов и систем защиты на основе технологии блокчейн.

Блокчейн представляет собой децентрализованную технологию, которая обеспечивает целостность транзакций без участия доверенного центра. Под транзакциями понимаются некоторые действия из заранее определенного перечня, производимые над материальными или нематериальными активами, которыми владеют пользователи системы. Информация о произведенных транзакциях объединяется в блоки, которые, в свою очередь, связываются друг с другом через хеширование. Для распространения одинаковых копий блоков между всеми участниками системы используется некоторый специальный алгоритм, называемый алгоритмом достижения консенсуса и направленный на то, чтобы компрометация цепочек блоков была сложной для потенциального злоумышленника задачей.

Основное преимущество блокчейна, которое делает технологию привлекательной для разнообразных приложений защиты данных, состоит в сложности нарушения целостности сохраненных транзакций. Целенаправленное изменение блока скомпрометирует все другие блоки в цепочке, после чего всю цепочку нужно будет построить заново. Однако вычислительная сложность данной задачи минимизирует вероятность взлома блокчейна [55].

В настоящее время технология блокчейн стала активно применяться в киберфизических системах различного назначения. Как уже было отмечено, главная ценность данной технологии заключается в том, что она позволяет обеспечить подтверждение разного рода транзакций, производимых в недоверенной среде. Многочисленные исследования обосновывают важность технологии блокчейн для четвертой промышленной революции (Industry 4.0), например [56, 57].

Кроме того, в рамках Индустрии 4.0 блокчейн продвигается совместно с иными перспективными технологиями нашего времени [58]. К ним относятся Интернет вещей [59], большие данные [60], туманные вычисления [61], дополненная реальность [56]. В целом блокчейн рассматривается как одна из ключевых технологий индустриального Интернета вещей, способствующая модернизации традиционных фабрик в современные интеллектуальные фабрики, использующие последние достижения в области цифровых технологий.

Отметим некоторые примеры современных исследований, предлагающих конкретные научно-технические решения, связанные с применением технологии блокчейн для решения задач безопасности в киберфизических системах.

Существенная часть известных работ связана с проблемой безопасного управления различными активами, в том числе в киберфизических системах. Это следует из того факта, что первое применение

технологии блокчейн было связано с криптовалютой биткоин. Дальнейшее развитие технологии блокчейна также шло в этом направлении, сформировался рынок криптовалют, который сейчас играет заметную роль в жизни общества.

С течением времени количество приложений технологии блокчейн значительно расширилось. Так недавняя работа [62] анализирует полезность блокчейна в решении проблем безопасности «умного города», который является примером масштабной киберфизической системы. Авторы рассматривают такие составляющие функционирования «умного города», как здравоохранение, транспорт, интеллектуальные сети, управление цепочками поставок, финансовые системы и сети центров обработки данных, обсуждают возможности технологии блокчейн применительно к каждой из перечисленных составляющих и выделяют направления будущих исследований.

В целом исследования, посвященные приложениям технологии блокчейн, можно разделить на несколько обширных групп.

Первая группа исследований связана с управлением цепочками поставок с использованием технологии блокчейн. К данной группе, прежде всего, относятся исследования общего характера, которые не выделяют какую-то конкретную область или конкретный класс киберфизических систем, а предлагают общее решение по безопасному управлению поставками с использованием блокчейна и обсуждают некоторые аспекты данной проблемы. В некоторых случаях предлагаемые решения рассчитаны на применение в киберфизических системах различного назначения, в некоторых – явно не оговариваются такой сферой использования.

Так, в работе [63] представлена классификация барьеров, ограничивающих внедрение технологии блокчейн в управление цепочками поставок. Некоторые вопросы преодоления таких барьеров представлены в [64]. В обоих случаях конкретный актив не уточняется. К этой же группе можно отнести исследования, в которых рассматривается очень широкий перечень услуг и товаров в цепочках поставок. Статья [65] описывает реальные случаи применения блокчейна для отслеживания сырьевых ресурсов, ингредиентов или запасных комплектующих в различных отраслях промышленности. Акцент делается на использовании технологии блокчейн совместно с технологиями Интернета вещей, лежащими в основе многих киберфизических систем.

К первой группе, если не вводить более подробную классификацию, можно отнести исследования, посвященные смежным задачам, возникающим в сфере организации и управления производством. В качестве примера отметим работу [66], в которой представ-

лено архитектурное решение по защите целостности данных в киберфизических производственных системах, используемых в сфере совместного производства.

Вторая группа исследований направлена на решение задачи безопасного управления конкретной разновидностью активов или видом услуг, в том числе управление соответствующими цепочками поставок. В настоящее время перечень подобных приложений стал весьма широк. Блокчейн применяют для контроля за продажами или распределением электроэнергии [67, 68], топлива [69, 70], вычислительных ресурсов [71], программного обеспечения [72].

Все перечисленные исследования объединяет то, что в них присутствует товарно-денежный обмен. Поэтому предлагаемые блокчейн-решения во многом наследуют идеи криптовалют.

К следующей группе можно отнести исследования, посвященные проблеме организации доверенного взаимодействия между множеством некоторых устройств. Конкретные задачи, связанные с обеспечением целостности тех или иных данных, которыми оперируют такие устройства, могут различаться.

Во многих работах идет речь о взаимодействии произвольных устройств Интернета вещей без привязки к конкретным типам киберфизических систем. В качестве некоторых примеров последних работ в данном направлении можно отметить [73-76].

В большинстве таких работ делается акцент на энергоэффективности архитектурных решений, предназначенных для использования в системах Интернета вещей, и предлагаются различные способы достижения этого свойства.

В части решаемых задач рассматриваемые работы можно разделить на те, в которых речь идет только об обеспечении целостности транзакций, и те, в которых помимо этого обеспечивается конфиденциальность данных, содержащихся в транзакциях. Так, в исследовании [77] в качестве объекта защиты рассматриваются данные о местоположении устройств Интернета вещей. Авторы указывают на необходимость обеспечения конфиденциальности этих данных, поэтому в предлагаемой ими схеме блокчейн объединяется с шифрованием.

Переходя от общих решений по применению технологии блокчейн для защиты данных в киберфизических системах, которые построены на основе технологии Интернета вещей, к частным случаям, необходимо отметить такой класс киберфизических систем, как подключенные транспортные средства, в том числе беспилотные [78-80]. В 2019–2020 годах наблюдается «взрывной» рост числа журнальных публикаций, посвященных соответствующим исследованиям, поэто-

му можно сказать, что обеспечение безопасности данного класса киберфизических систем с помощью технологии блокчейн представляет собой пример перспективного направления в рассматриваемой проблемной области.

4.4. Аутентификация данных в киберфизических системах с помощью цифровых водяных знаков. Эксплуатация киберфизических систем, включающих в себя автономные устройства интернета вещей, сопряжена с необходимостью экономии расхода энергии, в том числе при выборе защитных механизмов. В частности, это является одной из основных причин существования так называемой «легковесной криптографии».

Альтернативой криптографии являются методы цифровой стеганографии и цифровых водяных знаков. Указанные методы позволяют скрывать дополнительную информацию различного назначения в цифровых объектах. Обычно целью применения стеганографического сокрытия является обеспечение конфиденциальности данных, а внедрение цифровых водяных знаков в цифровые объекты в большинстве случаев применяется с целью их аутентификации.

Целесообразность использования методов встраивания информации в киберфизических системах, требовательных к энергопотреблению, объясняется следующими особенностями этих методов: низкой вычислительной сложностью в общем случае и направленностью на работу с избыточными данными.

Применение методов встраивания информации в цифровые данные в киберфизических системах является предметом исследований многих ученых, что подчеркивает актуальность данного направления. Соответствующие работы можно разделить на два больших класса:

– встраивание информации в мультимедиа-данные (цифровые изображения, аудио- и видеопоследовательности), вырабатываемые и передаваемые в киберфизических системах;

– встраивание информации в данные иной природы, не относящиеся к мультимедиа (сенсорные данные, информационные и управляющие сигналы в киберфизических системах).

Очевидно, что первый случай применим не ко всем киберфизическим системам, а только к тем, которые оперируют информацией подобного типа. Тем не менее такие системы не являются редкостью и подобные исследования представлены в достаточно большом количестве. Во многом это обусловлено тем фактом, что область сокрытия информации в мультимедиа имеет достаточно богатую историю и дает хорошую базу для новых направлений исследований.

В свою очередь, встраивание информации в произвольные данные в киберфизических системах представляет собой более широкий

случай, однако это направление представлено существенно меньшим количеством исследований.

В [81] приводится обзор методов встраивания информации в цифровые данные в Интернете вещей, актуальный на конец 2018 года. Поэтому в настоящем обзоре сосредоточимся на новых исследованиях, появившихся за последние несколько лет. При этом отметим, что в рамках настоящего обзора будут рассмотрены только методы встраивания цифровых водяных знаков, поскольку методы цифровой стеганографии в общем случае не связаны с задачей обеспечения целостности данных.

Прежде всего, следует выделить достаточно широкий класс исследований, которые посвящены разработке методов и алгоритмов сокрытия информации в цифровых изображениях (и иных цифровых объектах), предназначенных для защиты данных в киберфизических системах, но не обладающих какими-либо специфическими особенностями, которые связаны с заявленной областью применения. К данному классу относятся, например, работы [82-84]. Их авторы утверждают, что предлагаемые ими решения предназначены для защиты данных в Интернете вещей, однако не указывают какие-либо специфичные для данной области сценарии использования своих алгоритмов. Многие работы, которые можно отнести к данной группе, посвящены вопросам безопасности в телемедицинских системах.

Поскольку такие исследования представлены достаточно широко, их следует отметить как отдельный класс. Однако работы указанного класса фактически не выходят за пределы классического встраивания в мультимедиа-данные и далее рассматриваться не будут.

Следующая группа работ также охватывает классическое встраивание данных в мультимедиа-объекты. Отличие заключается в том, что авторы, заявляя применимость своих решений в киберфизических системах, определяют некоторые специфические сценарии передачи данных, характерные для таких систем, и указывают связанные с ними ограничения.

Работы указанной группы представлены не столь широко, но тем не менее их следует отделить от работ, составляющих первую группу.

В [85] также предлагается схема защищенной передачи изображений в телемедицинских системах. Зашифрованные конфиденциальные изображения встраиваются в изображения, содержимое которых не является конфиденциальным. Дополнительно в изображение-контейнер встраивается отпечаток (перцептивный хеш) конфиденциального изображения с целью его последующей аутентификации. Отличительной особенностью данной схемы является отслеживание порядка передачи изображений. Для этого авторы вводят понятие цепоч-

ки отпечатков изображений (image fingerprint) по аналогии с понятием цепочек блоков, лежащих в основе технологии блокчейн.

Исследование [86] носит несколько специфичный характер, поскольку в нем идет речь о встраивании скрытых вложений в изображения, используемые в печатной продукции. Однако в этой работе достаточно ясно определены приложения предлагаемого подхода в системах Интернета вещей и соответствующие сценарии применения, в частности для обеспечения аутентификации данных с целью защиты продукции от подделки, поэтому она соответствует теме настоящего обзора. Здесь также нужно отметить, что авторы работы говорят о стеганографическом встраивании, однако делают акцент на свойстве робастности, что характерно для встраивания цифровых водяных знаков.

Следующая группа работ посвящена встраиванию цифровых водяных знаков в данные, вырабатываемых и передаваемых в киберфизических системах и не относящихся к мультимедиа. В существенной части работ, относящихся к этой группе, речь идет о встраивании цифровых водяных знаков в данные беспроводных сенсорных сетей для обеспечения контроля целостности.

Подобный алгоритм предлагается в том числе и в одной из работ авторов настоящего обзора [87]. Отличительной особенностью данного алгоритма является возможность управлять уровнем искажений, вносимых в результате встраивания. Это делает его применимым к сенсорным данным различной физической природы.

В [88] представлен алгоритм встраивания цифровых водяных знаков в данные беспроводных сенсорных сетей, основное назначение которого заключается в обеспечении защиты от атаки, направленной на клонирование сенсорных узлов. Встраивание основано на преобразовании, схожем с гаммированием над двоичным алфавитом. В качестве преимущества алгоритма заявлена легковесность.

Алгоритмы встраивают элементы цифрового водяного знака в сенсорные данные последовательным и независимым образом, поскольку он не зависит от значений этих сенсорных данных или некоторых их характеристик. Идея формировать цифровой водяной знак в зависимости от самих защищаемых данных является достаточно распространенной как для классических методов и алгоритмов цифровых водяных знаков, так и для рассматриваемой проблемной области защиты данных беспроводных сенсорных сетей и интернета вещей.

В более простом случае элементы цифрового водяного знака вырабатываются только на основании значений элементов сенсорных данных. Примером является схема встраивания, представленная в [89]. В соответствии с данной схемой бит цифрового водяного знака, встра-

иваемый в очередное сенсорное значение, вырабатывается на основе нескольких предыдущих сенсорных значений.

Такой подход обладает определенными преимуществами по сравнению с независимым встраиванием элементов цифрового водяного знака, однако приводит к появлению проблемы синхронизации. Если при получении сообщения порядок элементов данных будет нарушен, это приведет к ошибкам при извлечении цифрового водяного знака даже при отсутствии на канале связи активного злоумышленника. Некоторый способ решения данной проблемы представлен в [90]. Авторы предлагают схему цифровых водяных знаков с двумя цепочками, в соответствии с которой сенсорные данные разделяются на группы переменной длины, зависящей от ключа. Выработка и встраивание цепочек цифровых водяных знаков осуществляется для пар смежных групп. Одна цепочка цифровых водяных знаков служит для аутентификации самих сенсорных данных. Вторая цепочка цифровых водяных знаков кодирует разделители между группами и обеспечивает синхронизацию между отправителем и получателем данных.

В более сложном случае в формировании цифрового водяного знака участвуют не только значения сенсорных величин, но и некоторые их характеристики. Так работа [91] посвящена проблеме аутентификации данных, поступающих от устройств Интернета вещей. Для этого предлагается извлекать стохастические характеристики потоков данных и формировать на их основе цифровые водяные знаки. В качестве метода встраивания цифровых водяных знаков в поток данных используется метод расширения спектра. В работе [92] также идет речь о том, чтобы использовать при формировании цифрового водяного знака различные характеристики захваченных данных: длину данных, частоту появления и время захвата. В [93] цифровой водяной знак формируется на основе информации о коллизиях протокола CSMA/CA и служит для отражения атаки клонирования сенсорных узлов. Кроме того, отличительной особенностью работы является способ представления сенсорных данных. Из них формируется матрица, подобная цифровому изображению. В общем случае такое решение позволяет использовать при работе с сенсорными данными подходы, которые успешно зарекомендовали себя применительно к цифровым изображениям.

Алгоритмы, представленные во всех отмеченных исследованиях, работают с цифровыми водяными знаками, представляющими собой двоичные последовательности. Кроме того, существует класс работ, посвященных встраиванию водяных знаков в аналоговые сигналы (в частности, в модулированные сигналы) для решения задач

аутентификации сигналов или их источника. Решения, которые можно найти в данных работах, идейно схожи с решениями по встраиванию цифровых водяных знаков. Отличие заключается лишь в форме представления сигнала и, как следствие, в способах его обработки.

Исследование [94] посвящено задаче аутентификации отправителя в системах, соответствующих стандарту NB-IoT (Narrow Band Internet of Things). В исследовании используется понятие радиочастотного водяного знака. Изначально водяной знак формируется как цифровой, однако далее встраивание осуществляется не уровне двоичных последовательностей, а на уровне модулированных сигналов. Основным преимуществом предлагаемой схемы называется повышенная надежность за счет устранения взаимной помехи между полезным сигналом и сигналом водяного знака.

В определенных случаях водяные знаки служат для отражения конкретных видов атак. Работа [95] посвящена идентификации кибератак воспроизведения, направленных на сетевые промышленные системы управления (networked control industrial systems). Под этим подразумевается попытка злоумышленника вмешаться в управление системой посредством воспроизведения ранее перехваченных последовательностей данных. Основным вкладом данной работы является не алгоритм встраивания, который взят из предшествующих работ, а стратегия применения данного алгоритма для защиты от злоумышленника.

В работе [96] представлен алгоритм встраивания обратимых водяных знаков в сигналы, передаваемые в промышленных системах управления с «жестким» реальным временем. В качестве приоритетной области применения авторы указывают судовые системы управления. Встраивание является аддитивным и осуществляется под управлением секретного ключа, который предварительно должен быть передан по защищенному каналу связи. Предлагаемый алгоритм позволяет выявлять атаки, направленные на задержку и искажение сигнала.

В завершение отметим, что стали появляться исследования, объединяющие рассмотренную в предыдущей секции технологию блокчейн и технологию цифровых водяных знаков. Блокчейн и цифровые водяные знаки направлены на решение разных задач безопасности в киберфизических системах. Их совместное использование потенциально позволит добиться большего уровня безопасности, чем при использовании данных технологий по отдельности. Эта идея уже нашла отражение в предшествующих исследованиях, однако преимущественно только в одном направлении, связанном с проблемой управления цифровыми правами [97-99]. Совместное применение данных технологий в иных приложениях [100-103] является перспективным

направлением исследований, развитие которого позволит внести вклад в область кибербезопасности.

5. Заключение. Стремительный прогресс в области вычислительных и коммуникационных технологий обуславливает интерес научного сообщества и промышленности к киберфизическим системам [100-103]. Используя сенсорные, вычислительные и сетевые возможности, киберфизические системы способствуют становлению нового поколения научно-технических решений, обеспечивающих автоматические процессы принятия решений в различных областях – от автоматизации мелких бытовых процессов до транспортировки материалов, фабрик будущего и критически важных производств. Интеграция методов информационных технологий с физической системой, такой как электросеть, транспортная система и цепочка поставок, для формирования «умной» инфраструктуры – это залог большей эффективности, надежности и устойчивости.

Представлен обзор основных методов обеспечения целостности данных в протоколах управления киберфизических систем, а также обзор уязвимостей протоколов прикладного уровня, широко используемых в киберфизических системах различной природы. Рассмотрены классические методы обеспечения целостности, новые методы, в частности блокчейн, а также направления развития и оптимизации методов защиты в M2M протоколах. Масштаб представленных сведений об уязвимостях и угрозах безопасности для протоколов киберфизических систем наилучшим образом подчеркивает потребность в новых методах и механизмах обеспечения безопасности, адаптированных для предотвращения таких угроз без препятствий в работе подобных инфраструктур.

Дальнейшие направления исследований будут связаны с повышением эффективности методов обеспечения целостности данных в киберфизических системах. В частности, интерес представляет гибридизация технологий блокчейн и цифровых водяных знаков для построения эффективных методов аутентификации данных и источников данных в мультимедиа-системах.

Литература

1. *Suastegui Jaramillo L.E.* Malware Detection and Mitigation Techniques: Lessons Learned from Mirai DDOS Attack // Journal of Information Systems Engineering & Management. 2018. vol. 3(3). no. 19. pp. 1–6.
2. *Mahbub M.* Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics // Journal of Network and Computer Applications. 2020. vol. 168. no. 102761. pp. 1–26.
3. *Luo J.-Z., Shan C., Cai J., Liu Y.* IoT Application-Layer Protocol Vulnerability Detection using Reverse Engineering // Symmetry. 2018. vol. 10. no. 561. pp. 1–13.
4. *Johnson D., Ketel M.* IoT: Application Protocols and Security // International Journal of Computer Network and Information Security. 2019. vol. no. 11. pp. 1–8.

5. *Nebbione G. Calzarossa M.C.* Security of IoT Application Layer Protocols: Challenges and Findings // Future Internet. 2020. vol. 12. no. 55. pp. 1–20.
6. *Alghamdi T., Lasebae A., Aiash M.* Security Analysis of the Constrained Application Protocol in the Internet of Things // Second International Conference on Future Generation Communication Technologies (FGCT 2013). 2013. pp. 163–168.
7. *Ватаманюк И.В., Яковлев Р.Н.* Обобщенные теоретические модели киберфизических систем // Известия Юго-Западного государственного университета. 2019. № 23(6). С. 161–175.
8. *Korzun D. et al.* Ambient Intelligence Services in IoT Environments: Emerging Research and Opportunities // IGI Global. 2019.
9. *Zavyalova Y.V., Korzun D.G., Meigal A.Y., Borodin A.V.* Towards the Development of Smart Spaces-Based Socio-Cyber-Medicine Systems // International Journal of Embedded and Real-Time Communication Systems (IJERTCS). 2017. pp. 45–63
10. *Kayal P. Perros H.* A comparison of IoT application layer protocols through a smart parking implementation // 2017 20th Conference on Innovations in Clouds, Internet and Networks. 2017. pp. 331–336.
11. *Dizdarevic J., Carpio F., Jukan A., Masip X.* A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration // ACM Computing Surveys. 2019. vol. 51. no. 6. pp. 1–29.
12. *Naik N.* Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP // Proceedings of the 2017 IEEE International Systems Engineering Symposium. 2017. pp. 1–7.
13. *Селезнёв С.П., Яковлев В.В.* Архитектура промышленных приложений IoT и протоколы AMQP, MQTT, JMS, REST, COAP, XMPP, DDS // International Journal of Open Information Technologies. 2019. № 5. С. 17–28.
14. *Dinculean D.* Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices // Applied Sciences. 2019. vol. 9. no. 848. pp. 1–10.
15. *Andy S., Rahardjo B., Hanindhito B.* Attack scenarios and security analysis of MQTT communication protocol in IoT system // 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics. 2017. pp. 1–6.
16. *Firdous S.N., Baig Z., Valli C., Ibrahim A.* Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol // Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). 2017. pp. 748–755.
17. *Jarvinen I., Raitahila I., Cao Z., Kojo M.* Is CoAP Congestion Safe? // ANRW '18: Proceedings of the Applied Networking Research Workshop. 2018. pp. 43–49.
18. *Roselin A.G. et al.* Exploiting the Remote Server Access Support of CoAP Protocol // IEEE Internet of Things Journal. 2019. pp. 9338–9349.
19. *Park C.* Security Architecture for Secure Multicast CoAP Applications // IEEE Internet of Things Journal. 2020. vol. 7. no. 4. pp. 3441–3452.
20. *Wani S.Y.* Internet of Things(IoT) Security and Vulnerability // Research proposal. 2018. pp. 1–9.
21. *White R. et al.* Network Reconnaissance and Vulnerability Excavation of Secure DDS Systems // Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops. 2019. pp. 57–66.
22. *Michaud M., Dean T., Leblanc S.* Attacking OMG Data Distribution Service (DDS) Based Real-Time Mission Critical Distributed Systems // Proceedings of the 2018 13th International Conference on Malicious and Unwanted Software. 2018. pp. 68–77.
23. *Malik I. et al.* XMPP architecture and security challenges in an IoT ecosystem // Proceedings of the 16th Australian Information Security Management Conference. 2019. pp. 62–73.

24. *Blahut R.E.* Principles and practice of information theory. Part 1 // Addison-Wesley. 1987. 458 p.
25. *Ivanov F., Kabatiansky G., Krouk E., Rumenko N.* A New Code-Based Cryptosystem // Code-Based Cryptography Workshop. 2020. pp. 41–49.
26. *Bahl L., Cocke J., Jelinek F., Raviv J.* Optimal decoding of linear codes for minimizing symbol error rate (Corresp.) // IEEE Transactions on Information Theory. 1974. vol. 20. no. 2. pp. 284–287.
27. *Ivanov F., Kreshchuk A., Zyablov V.* On the Local Erasure Correction Capacity of Convolutional Codes // 2018 International Symposium on Information Theory and Its Applications. 2018. pp. 296–300.
28. *Zyablov V.V., Ivanov F.I., Potapov V.G.* Comparison of various constructions of binary LDPC codes based on permutation matrices // Journal of Communications Technology and Electronics. 2012. vol. 57. pp. 932–945.
29. *Berrou C. et al.* An overview of turbo codes and their applications // The European Conference on Wireless Technology. 2005. pp. 1–9.
30. *Arikan E.* Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels // IEEE Transactions on Information Theory. vol. 55. no. 7. pp. 3051–3073.
31. *Zhilin I., Ivanov F., Zyablov V.* Generalized Error Locating Codes with Soft Decoding of Inner Codes // Proceedings of European Wireless 2015; 21th European Wireless Conference. 2015. pp. 1–5.
32. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хэширования // М.: Госстандарт России. 2012.
33. ГОСТ Р 34.13–2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров // М.: Госстандарт России. 2015.
34. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи // М.: Госстандарт России. 2012.
35. *Bali R.S., Jaafar F., Zavarasky P.* Lightweight Authentication for MQTT to Improve the Security of IoT Communication // Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. 2019. pp. 6–12.
36. *Malina L. et al.* A Secure Publish/Subscribe Protocol for Internet of Things // Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019. pp. 1–10.
37. *Singh M., Rajan M.A., Shivraj V.L., Balamuralidhar P.* Secure MQTT for Internet of Things (IoT) // Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies. 2015. pp. 746–751.
38. *Dinculeana D., Cheng X.* Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices // Applied Sciences. 2019. vol. 9. no. 848. pp. 1–10.
39. *Niruntasukrat A. et al.* Authorization mechanism for MQTT-based Internet of Things // Proceedings of the 2016 IEEE International Conference on Communications Workshops. 2016. pp. 290–295.
40. *Calabretta M., Pecori R., Veltri L.* A Token-based Protocol for Securing MQTT Communications // Proceedings of the 2018 26th International Conference on Software, Telecommunications and Computer Networks. 2018. pp. 1–6.
41. *Bisne L., Parmar M.* Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES // Proceedings of the 2017 Innovations in Power and Advanced Computing Technologies. 2017. pp. 1–5.
42. *Aumasson J.P., Neves S., Wilcox-O'Hearn Z., Winnerlein C.* BLAKE2: Simpler, Smaller, Fast as MD5 // Proceedings of the Applied Cryptography and Network Security. 2013. pp. 119–135.
43. *Kuchta V., Sharma G.* Lattice - Based Cryptography and Internet of Things // IoT Security: Advances in Authentication. 2020. pp. 101–118.

44. *Porambage P., Braeken A., Schmitt C.* Public Key Based Protocols – EC Crypto // IoT Security: Advances in Authentication. 2020. pp. 85–99.
45. *Hardt D.* The OAuth 2.0 Authorization Framework. URL: https://tools.ietf.org/html/rfc6749 (дата обращения: 15.03.2020).
46. *Colombo P., Ferrari E.* Access Control Enforcement Within MQTT-based Internet of Things Ecosystems // Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies. 2018. pp. 223–234.
47. *Guo L., Wu J., Xia Z., Li J.* Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks // IEEE Sensors Journal. vol. 15. no. 5. pp. 2577–2586.
48. *Iglesias-Urkia M., Orive A., Urbieta A., Casado-Mansilla D.* Analysis of CoAP implementations for industrial Internet of Things: A survey // Procedia Computer Science. 2017. vol. 109. pp. 188–195.
49. *Hussein A. Elhajj I., Chehab A., Kayssi A.* Securing Diameter: Comparing TLS, DTLS, and IPSec // 2016 IEEE International Multidisciplinary Conference on Engineering Technology. 2016. pp. 1–8.
50. *Boo E., Raza S, Höglund J., Ko J.* Towards Supporting IoT Device Storage and Network Security Using DTLS // MobiSys '19: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services. 2019. pp. 570–571.
51. *Shah V.* Exploit DTLS Vulnerabilities & Provide a Novel approach to Protect DTLS in CoAP based IoT // International Journal for Research in Applied Science and Engineering Technology. 2020. vol. 8. pp. 216–221.
52. *Albalas F., Al-Soud M., Almomani O., Almomani A.* Security-aware CoAP Application Layer Protocol for the Internet of Things using Elliptic-Curve Cryptography // International Arab Journal of Information Technology. 2018. vol. 15. no. 3A. pp. 550–558.
53. *Capossele A., Cervo V., Cicco G.D., Petrioli C.* Security as a CoAP resource: An optimized DTLS implementation for the IoT // Proceedings of the 2015 IEEE International Conference on Communications. 2015. pp. 549–554.
54. *Banerjee U. et al.* An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for Securing Internet-of-Things Applications // IEEE Journal of Solid-State Circuits. 2019. vol. 54. no. 8. pp. 2339–2352.
55. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 15.05.2020).
56. *Fernández-Caramés T.M., Fraga-Lamas P.* A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories // IEEE Access. 2019. vol. 7. pp. 45201–45218.
57. *Alladi T., Chamola V., Parizi R.M., Choo K.-K.R.* Blockchain Applications for Industry 4.0 and Industrial IoT: A Review // IEEE Access. 2019. vol. 7. pp. 176935–176951.
58. *Aceto G., Persico V., Pescapé A.* A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges // IEEE Communications Surveys & Tutorials. 2019. vol. 21. no. 4. pp. 3467–3501.
59. *Fernández-Caramés T.M., Fraga-Lamas P.* A Review on the Use of Blockchain for the Internet of Things // IEEE Access. 2018. vol. 6. pp. 32979–33001.
60. *Zhaofeng M. et al.* Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data // IEEE Internet of Things Journal. 2020. vol. 7. no. 5. pp. 4000–4015.
61. *Baniata H., Kertesz A.* A Survey on Blockchain-Fog Integration Approaches // IEEE Access. 2020. vol. 8. pp. 102657–102668.
62. *Bhushan B. et al.* Blockchain for smart cities: A review of architectures, integration trends and future research directions // Sustainable Cities and Society. 2020. vol. 61. pp. 1–27.
63. *Saberi S., Kouhizadeh M., Sarkis J., Shen L.* Blockchain technology and its relationships to sustainable supply chain management // International Journal of Production Research. 2019. vol. 57. no. 7. pp. 2117–2135.

64. *Fu Y., Zhu J.* Big production enterprise supply chain endogenous risk management based on blockchain // IEEE Access. 2019. vol. 7. pp. 15310–15319.
65. *Kshetri N.* 1 Blockchain's roles in meeting key supply chain management objectives // International Journal of Information Management. 2018. vol. 39. pp. 80–89.
66. *Yu C., Jiang X., Yu S., Yang C.* Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation // Robotics and Computer-Integrated Manufacturing. 2020. vol. 64. pp. 1–15.
67. *Li M. et al.* Blockchain-enabled Secure Energy Trading with Verifiable Fairness in Industrial Internet of Things // IEEE Transactions on Industrial Informatics. 2020. vol. 16. no. 10. pp. 6564–6574.
68. *Han D., Zhang C., Ping J., Yan Z.* Smart contract architecture for decentralized energy trading and management based on blockchains // Energy. 2020. vol. 199. pp. 1–14.
69. *Lu H., Huang K., Azimi M., Guo L.* Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks // IEEE Access. 2019. vol. 7. pp. 41426–41444.
70. *Anwar H., Arasu M., Ahmed Q.* Ensuring fuel economy performance of commercial vehicle fleets using blockchain technology // Proceedings of SAE World Congress Experience (WCX 2019). 2019. pp. 1510–1516.
71. *Pan J. et al.* EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts // IEEE Internet of Things Journal. 2018. vol. 6. no. 3. pp. 4719–4732.
72. *Seitz A. et al.* Fog computing as enabler for blockchain-based IIoT app marketplaces-A case study // Proceedings of the 2018 Fifth international conference on internet of things: systems, management and security. 2018. pp. 182–188.
73. *Koshy P., Babu S., Manoj B.S.* Sliding Window Blockchain Architecture for Internet of Things // IEEE Internet of Things Journal. 2020. vol. 7. no. 4. pp. 3338–3348.
74. *Luo J., Chen Q., Yu F.R., Tang L.* Blockchain-enabled software-defined industrial internet of things with deep reinforcement learning // IEEE Internet of Things Journal. 2020. vol. 7. no. 6. pp. 5466–5480.
75. *Ge C., Liu Z., Fang L.* A blockchain based decentralized data security mechanism for the Internet of Things // Journal of Parallel and Distributed Computing. 2020. vol. 141. pp. 1–9.
76. *Chi J. et al.* A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things // Journal of Network and Computer Applications. 2020. vol. 167. pp. 1–10.
77. *Li D., Hu Y., Lan M.* IoT device location information storage system based on blockchain // Future Generation Computer Systems. 2020. vol. 109. pp. 95–102.
78. *Cebe M. et al.* Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles // IEEE Communications Magazine. 2018. vol. 56. no. 10. pp. 50–57.
79. *Rathee G. et al.* A blockchain framework for securing connected and autonomous vehicles // Sensors. 2019. vol. 19. no. 14. pp. 1–15.
80. *Qian Y. et al.* Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles // IEEE Network. 2020. vol. 34. no. 2. pp. 46–51.
81. *Евсютин О.О., Кокурина А.С., Мещеряков Р.В.* Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей» // Компьютерная оптика. 2019. Т. 43. № 1. С. 137–154.
82. *Al-Shayea T.K., Mavromoustakis C.X., Batalla J.M., Mastorakis G.* A hybridized methodology of different wavelet transformations targeting medical images in IoT infrastructure // Measurement. 2019. vol. 148. pp. 1–14.
83. *Prasetyo H., Hsia C.-H., Liu C.-H.* Vulnerability attacks of SVD-based video watermarking scheme in an IoT environment // IEEE Access. 2020. vol. 8. pp. 69919–69936.

84. *Liu J. et al.* Robust Watermarking Algorithm for Medical Volume Data in Internet of Medical Things // IEEE Access. 2020. vol. 8. pp. 93939–93961.
85. *Peng H., Yang B., Li L., Yang Y.* Secure and Traceable Image Transmission Scheme Based on Semitensor Product Compressed Sensing in Telemedicine System // IEEE Internet of Things Journal. 2020. vol. 7. no. 3. pp. 2432–2451.
86. *Pu Y.-F., Zhang N., Wang H.* Fractional-Order Spatial Steganography and Blind Steganalysis for Printed Matter: Anti-Counterfeiting for Product External Packing in Internet-of-Things // IEEE Internet of Things Journal. 2019. vol. 6. no. 4. pp. 6368–6383.
87. *Evsutin O. et al.* Algorithm for Embedding Digital Watermarks in Wireless Sensor Networks Data with Control of Embedding Distortions // Proceedings of the 2nd International Conference on Distributed and Computer and Communication Networks (DCCN 2019). 2019. pp. 574–585.
88. *Hoang T.-M., Bui V.-H., Vu N.-L., Hoang D.-H.* A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks // Proceedings of the 34th International Conference on Information Networking (ICOIN 2020). 2020. pp. 649–653.
89. *Xiao X., Gao G.* Digital Watermark-Based Independent Individual Certification Scheme in WSNs // EEE Access. 2019. vol. 7. pp. 145516–145523.
90. *Wang B., Kong W., Li W., Xiong N.N.* A dual-chaining watermark scheme for data integrity protection in internet of things // Computers, Materials and Continua. 2019. vol. 58. no. 3. pp. 679–695.
91. *Ferdowsi A., Saad W.* Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems // IEEE Transactions on Communications. 2018. vol. 67. no. 2. pp. 1371–1387.
92. *Hameed K. et al.* Towards a for-mally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks // Future Generation Computer Systems. 2018. vol. 82. pp. 274–289.
93. *Nguyen V.-T. et al.* A lightweight watermark scheme utilizing MAC layer behaviors for wireless sensor networks // Proceedings of the 3rd International Conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom 2019). 2019. pp. 176–180.
94. *Huang H., Zhang L.* Reliable and Secure Constellation Shifting Aided Differential Radio Frequency Watermark Design for NB-IoT Systems // IEEE Communications Letters. 2019. vol. 23. no. 12. pp. 2262–2265.
95. *Rubio-Hernan J., De Cicco L., Garcia-Alfaro J.* Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems // Transactions on Emerging Telecommunications Technologies. 2018. vol. 29. no. 7. pp. 1–17.
96. *Song Z., Skuric A., Ji K.* A Recursive Watermark Method for Hard Real-Time Industrial Control System Cyber-Resilience Enhancement // IEEE Transactions on Automation Science and Engineering. 2020. vol. 17. no. 2. pp. 1030–1043.
97. *Zhao B. et al.* Y-DWMS: A Digital Watermark Management System Based on Smart Contracts // Sensors. 2019. vol. 19. no. 14. pp. 1–17.
98. *Qian Y. et al.* Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles // IEEE Network. 2020. vol. 34. no. 2. pp. 46–51.
99. *Zhang C. et al.* Blockchain-Enabled Accountability Mechanism Against Information Leakage in Vertical Industry Services // IEEE Transactions on Network Science and Engineering. 2020.
100. *Chen J., Gupta V., Quevedo D., Tesi P.* Privacy and security of cyberphysical systems // International Journal of Robust and Nonlinear Control. 2020. vol. 30. pp. 4165–4167.
101. *Lin H., Alemzadeh H., Iyer R.* Challenges and Opportunities in the Detection of Safety-Critical Cyberphysical Attacks // Computer. 2020. vol. 53. no. 3. pp. 26–37.

102. *Iskhakov A., Meshcheryakov R.* Intelligent System of Environment Monitoring on the Basis of a Set of IOT-Sensors // 2019 International Siberian Conference on Control and Communications. 2019. pp. 1–5.
103. *Iskhakov A., Iskhakova A., Meshcheryakov R.* Dynamic Container Virtualization as a Method of IoT Infrastructure Security Provision. Cyber-Physical Systems and Control. Lecture Notes in Networks and Systems. 2020. vol. 95. pp. 482–490.

Мещеряков Роман Валерьевич – д-р техн. наук, доцент, заведующий лабораторией, лаборатория киберфизических систем, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук (ИПУ РАН). Область научных интересов: информационная безопасность, системный анализ, робототехника. Число научных публикаций – 500. mrv@ieee.org; ул. Профсоюзная, 65, 117997, Москва, Россия; р.т.: +7(495)334-89-10.

Исхаков Андрей Юнусович – канд. техн. наук, старший научный сотрудник, лаборатория киберфизических систем, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук (ИПУ РАН). Область научных интересов: информационная безопасность, аутентификация, вычислительные сети. Число научных публикаций – 55. iskhakovandrey@gmail.com; ул. Профсоюзная, 65, 117997, Москва, Россия; р.т.: +7(923)421-58-28.

Евсютин Олег Олегович – канд. техн. наук, доцент, заведующий кафедрой, кафедра информационной безопасности киберфизических систем, Московский институт электроники и математики (МИЭМ НИУ ВШЭ); старший научный сотрудник, лаборатория киберфизических систем, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук (ИПУ РАН). Область научных интересов: информационная безопасность, цифровая обработка изображений, цифровая стеганография, цифровые водяные знаки. Число научных публикаций – 70. evsutin.oo@gmail.com; ул. Таллинская, 34, 123458, Москва, Россия; р.т.: +7(495)772-9590*12675.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проект № 19-17-50248).

DOI 10.15622/ia.2020.19.5.7

R. MESHCHERYAKOV, A. ISKHAKOV, O. EVSUTIN

ANALYSIS OF MODERN METHODS TO ENSURE DATA INTEGRITY IN CYBER-PHYSICAL SYSTEM MANAGEMENT PROTOCOLS

Meshcheryakov R., Iskhakov A., Evsutin O. **Analysis of Modern Methods to Ensure Data Integrity in Cyber-Physical System Management Protocols.**

Abstract. At present, the problem of creating methodological security of cyberphysical systems, in particular, the design and implementation of information security subsystems is acute. At the same time, the landscape of threats and vulnerabilities typical for a wide range of hardware and software technologies used in cyberphysical systems is extremely wide and complex. In this context, the security of application layer protocols is of paramount importance, as these protocols are the basis for interaction between applications and services running on different devices, as well as in cloud infrastructures. With the constant interaction of the systems under study with the real physical infrastructure, the challenge is to determine effective measures to ensure the integrity of the transferred control commands, as disruption of the performed critical processes can affect human life and health. The paper provides an analytical review of the main methods of data integrity assurance in management protocol of cyberphysical systems, as well as an overview of application layer protocols vulnerabilities widely used in cyberphysical systems of different types. Classical methods of data integrity assurance, new methods, in particular, blockchain, as well as the main directions of increasing the efficiency of data integrity protocols in cyberphysical systems are considered. Analysis of application layer vulnerabilities is carried out on the example of the most popular MQTT, CoAP, AMQP, DDS, XMPP specifications and their implementations. It is established that despite the presence of basic security mechanisms in all these protocols, researchers continue to regularly identify vulnerabilities in popular implementations, that often endangers critical infrastructure services. In the course of preparing the review of the existing methods of data integrity assurance for the examined class of systems, the key problems of these methods integration and ways of their solution were defined.

Keywords: Cyberphysical System, Internet of Things, Protocol, Blockchain, Watermarking, Authentication

Meshcheryakov Roman – Ph.D., Dr.Sci., Associate Professor, Head of Laboratory, Laboratory of Cyberphysical Systems, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences (ICS RAS). Research interests: information security, system analysis, robotics. The number of publications – 500. mrv@ieee.org; 65, Profsoyuznaya str., 117997, Moscow, Russia; office phone: +7(495)334-89-10.

Iskhakov Andrey – Ph.D., Senior Researcher, Laboratory of Cyberphysical Systems, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences (ICS RAS). Research interests: information security, authentication, computer networks. The number of publications – 55. iskhakovandrey@gmail.com; 65, Profsoyuznaya str., 117997, Moscow, Russia; office phone: +7 923 421-58-28.

Evsutin Oleg – Ph.D., Associate Professor, Head of Department, Department of Cyber-Physical Systems Information Security, Moscow Institute of Electronics and Mathematics (MIEM HSE); Senior Researcher, Laboratory of Cyberphysical Systems, V.A. Trapeznikov

Institute of Control Sciences of Russian Academy of Sciences (ICS RAS). Research interests: information security, digital image processing, digital steganography, digital watermarking. The number of publications – 70. evsutin.oo@gmail.com; 34, Tallinskaya str., 123458, Moscow, Russia; office phone: +7(495)772-9590*12675.

Acknowledgements. This research is supported by RFBR (19-17-50248).

References

1. Suastegui Jaramillo L.E. Malware Detection and Mitigation Techniques: Lessons Learned from Mirai DDOS Attack. *Journal of Information Systems Engineering & Management*. 2018. vol. 3(3). no. 19. pp. 1–6.
2. Mahbub M. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *Journal of Network and Computer Applications*. 2020. vol. 168. no. 102761. pp. 1–26.
3. Luo J.-Z., Shan C., Cai J., Liu Y. IoT Application-Layer Protocol Vulnerability Detection using Reverse Engineering. *Symmetry.* 2018. vol. 10. no. 561. pp. 1–13.
4. Johnson D., Ketel M. IoT: Application Protocols and Security. *International Journal of Computer Network and Information Security.* 2019. vol. no. 11. pp. 1–8.
5. Nebbione G. Calzarossa M.C. Security of IoT Application Layer Protocols: Challenges and Findings. *Future Internet.* 2020. vol. 12. no. 55. pp. 1–20.
6. Alghamdi T., Lasebae A., Aiash M. Security Analysis of the Constrained Application Protocol in the Internet of Things. Second International Conference on Future Generation Communication Technologies (FGCT 2013). 2013. pp. 163–168.
7. Vatamaniuk I.V., Iakovlev R.N. [Generalized Theoretical Models of Cyberphysical Systems]. *Izvestija Jugo-Zapadnogo gosudarstvennogo universiteta – Proceedings of the Southwest State University*. 2019. vol. 23(6). pp. 161–175. (In Russ.).
8. Korzun D. et al. Ambient Intelligence Services in IoT Environments: Emerging Research and Opportunities. IGI Global. 2019.
9. Zavyalova Y.V., Korzun D.G., Meigal A.Y., Borodin A.V. Towards the Development of Smart Spaces-Based Socio-Cyber-Medicine Systems. *International Journal of Embedded and Real-Time Communication Systems (IJERTCS)*. 2017. pp. 45–63
10. Kayal P. Perros H. A comparison of IoT application layer protocols through a smart parking implementation. 2017 20th Conference on Innovations in Clouds, Internet and Networks. 2017. pp. 331–336.
11. Dizdarevic J., Carpio F., Jukan A., Masip X. A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. *ACM Computing Surveys.* 2019. vol. 51. no. 6. pp. 1–29.
12. Naik N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. Proceedings of the 2017 IEEE International Systems Engineering Symposium. 2017. pp. 1–7.
13. Seleznev S., Yakovlev V. [Industrial Application Architecture IoT and protocols AMQP, MQTT, JMS, REST, CoAP, XMPP, DDS]. *International Journal of Open Information Technologies*. 2019. vol. 7. no. 5. pp. 17–28. (In Russ.).
14. Dinculean D. Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. *Applied Sciences.* 2019. vol. 9. no. 848. pp. 1–10.
15. Andy S., Rahardjo B., Hanindhito B. Attack scenarios and security analysis of MQTT communication protocol in IoT system. 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics. 2017. pp. 1–6.
16. Firdous S.N., Baig Z., Valli C., Ibrahim A. Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol. Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Commu-

nications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). 2017. pp. 748–755.
17. Jarvinen I., Raitahila I., Cao Z., Kojo M. Is CoAP Congestion Safe?. ANRW '18: Proceedings of the Applied Networking Research Workshop. 2018. pp. 43–49.
18. Roselin A.G. et al. Exploiting the Remote Server Access Support of CoAP Protocol. *IEEE Internet of Things Journal.* 2019. pp. 9338–9349.
19. Park C. Security Architecture for Secure Multicast CoAP Applications. *IEEE Internet of Things Journal.* 2020. vol. 7. no. 4. pp. 3441–3452.
20. Wani S.Y. Internet of Things(IoT) Security and Vulnerability // Research proposal. 2018. pp. 1–9.
21. White R. et al. Network Reconnaissance and Vulnerability Excavation of Secure DDS Systems. Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops. 2019. pp. 57–66.
22. Michaud M., Dean T., Leblanc S. Attacking OMG Data Distribution Service (DDS) Based Real-Time Mission Critical Distributed Systems. Proceedings of the 2018 13th International Conference on Malicious and Unwanted Software. 2018. pp. 68–77.
23. Malik I. et al. XMPP architecture and security challenges in an IoT ecosystem. Proceedings of the 16th Australian Information Security Management Conference. 2019. pp. 62–73.
24. Blahut R.E. Principles and practice of information theory. Part 1. Addison-Wesley. 1987. 458 p.
25. Ivanov F., Kabatiansky G., Krouk E., Rumenko N. A New Code-Based Cryptosystem. Code-Based Cryptography Workshop. 2020. pp. 41–49.
26. Bahl L., Cocke J., Jelinek F., Raviv J. Optimal decoding of linear codes for minimizing symbol error rate (Corresp.). *IEEE Transactions on Information Theory.* 1974. vol. 20. no. 2. pp. 284–287.
27. Ivanov F., Kreshchuk A., Zyablov V. On the Local Erasure Correction Capacity of Convolutional Codes. 2018 International Symposium on Information Theory and Its Applications. 2018. pp. 296–300.
28. Zyablov V.V., Ivanov F.I., Potapov V.G. Comparison of various constructions of binary LDPC codes based on permutation matrices. *Journal of Communications Technology and Electronics.* 2012. vol. 57. pp. 932–945.
29. Berrou C. et al. An overview of turbo codes and their applications. The European Conference on Wireless Technology. 2005. pp. 1–9.
30. Arikan E. Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels. *IEEE Transactions on Information Theory.* vol. 55. no. 7. pp. 3051–3073.
31. Zhilin I., Ivanov F., Zyablov V. Generalized Error Locating Codes with Soft Decoding of Inner Codes. Proceedings of European Wireless 2015; 21th European Wireless Conference. 2015. pp. 1–5.
32. GOST R 34.11–2012. [Information technology. Cryptographic data security. Hash function]. M.: Gosstandart Rossii. 2012. (In Russ.).
33. GOST R 34.13–2015. [Information technology. Cryptographic data security. Block ciphers operation modes]. M.: Gosstandart Rossii. 2015.
34. GOST R 34.10–2012. [Information technology. Cryptographic data security. Signature and verification processes of (electronic) digital signature]. M.: Gosstandart Rossii. 2012.
35. Bali R.S., Jaafar F., Zavarasky P. Lightweight Authentication for MQTT to Improve the Security of IoT Communication. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. 2019. pp. 6–12.
36. Malina L. et al. A Secure Publish/Subscribe Protocol for Internet of Things. Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019. pp. 1–10.

37. Singh M., Rajan M.A., Shivraj V.L., Balamuralidhar P. Secure MQTT for Internet of Things (IoT). Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies. 2015. pp. 746–751.
38. Dinculeana D., Cheng X. Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. *Applied Sciences.* 2019. vol. 9. no. 848. pp. 1–10.
39. Niruntasukrat A. et al. Authorization mechanism for MQTT-based Internet of Things. Proceedings of the 2016 IEEE International Conference on Communications Workshops. 2016. pp. 290–295.
40. Calabretta M., Pecori R., Veltri L. A Token-based Protocol for Securing MQTT Communications. Proceedings of the 2018 26th International Conference on Software, Telecommunications and Computer Networks. 2018. pp. 1–6.
41. Bisne L., Parmar M. Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES. Proceedings of the 2017 Innovations in Power and Advanced Computing Technologies. 2017. pp. 1–5.
42. Aumasson J.P., Neves S., Wilcox-O'Hearn Z., Winnerlein C. BLAKE2: Simpler, Smaller, Fast as MD5. Proceedings of the Applied Cryptography and Network Security. 2013. pp. 119–135.
43. Kuchta V., Sharma G. Lattice ‑ Based Cryptography and Internet of Things. IoT Security: Advances in Authentication. 2020. pp. 101–118.
44. Porambage P., Braeken A., Schmitt C. Public Key Based Protocols – EC Crypto. IoT Security: Advances in Authentication. 2020. pp. 85–99.
45. Hardt D. The OAuth 2.0 Authorization Framework. Available at: https://tools.ietf.org/html/rfc6749 (accessed: 15.03.2020).
46. Colombo P., Ferrari E. Access Control Enforcement Within MQTT-based Internet of Things Ecosystems. Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies. 2018. pp. 223–234.
47. Guo L., Wu J., Xia Z., Li J. Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks. *IEEE Sensors Journal.* vol. 15. no. 5. pp. 2577–2586.
48. Iglesias-Urkia M., Orive A., Urbieta A., Casado-Mansilla D. Analysis of CoAP implementations for industrial Internet of Things: A survey. *Procedia Computer Science.* 2017. vol. 109. pp. 188–195.
49. Hussein A. Elhajj I., Chehab A., Kayssi A. Securing Diameter: Comparing TLS, DTLS, and IPSec. 2016 IEEE International Multidisciplinary Conference on Engineering Technology. 2016. pp. 1–8.
50. Boo E., Raza S, Höglund J., Ko J. Towards Supporting IoT Device Storage and Network Security Using DTLS. MobiSys '19: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services. 2019. pp. 570–571.
51. Shah V. Exploit DTLS Vulnerabilities & Provide a Novel approach to Protect DTLS in CoAP based IoT. *International Journal for Research in Applied Science and Engineering Technology.* 2020. vol. 8. pp. 216–221.
52. Albalas F., Al-Soud M., Almomani O., Almomani A. Security-aware CoAP Application Layer Protocol for the Internet of Things using Elliptic-Curve Cryptography. *International Arab Journal of Information Technology.* 2018. vol. 15. no. 3A. pp. 550–558.
53. Capossele A., Cervo V., Cicco G.D., Petrioli C. Security as a CoAP resource: An optimized DTLS implementation for the IoT. Proceedings of the 2015 IEEE International Conference on Communications. 2015. pp. 549–554.
54. Banerjee U. et al. An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for Securing Internet-of-Things Applications. *IEEE Journal of Solid-State Circuits.* 2019. vol. 54. no. 8. pp. 2339–2352.
55. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf (accessed: 15.05.2020).

56. Fernández-Caramés T.M., Fraga-Lamas P. A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access*. 2019. vol. 7. pp. 45201–45218.
57. Alladi T., Chamola V., Parizi R.M., Choo K.-K.R. Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. *IEEE Access*. 2019. vol. 7. pp. 176935–176951.
58. Aceto G., Persico V., Pescapé A. A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges. *IEEE Communications Surveys & Tutorials*. 2019. vol. 21. no. 4. pp. 3467–3501.
59. Fernández-Caramés T.M., Fraga-Lamas P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*. 2018. vol. 6. pp. 32979–33001.
60. Zhaofeng M. et al. Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. *IEEE Internet of Things Journal*. 2020. vol. 7. no. 5. pp. 4000–4015.
61. Baniata H., Kertesz A. A Survey on Blockchain-Fog Integration Approaches. *IEEE Access*. 2020. vol. 8. pp. 102657–102668.
62. Bhushan B. et al. Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*. 2020. vol. 61. pp. 1–27.
63. Saberi S., Kouhizadeh M., Sarkis J., Shen L. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*. 2019. vol. 57. no. 7. pp. 2117–2135.
64. Fu Y., Zhu J. Big production enterprise supply chain endogenous risk management based on blockchain. *IEEE Access*. 2019. vol. 7. pp. 15310–15319.
65. Kshetri N. 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*. 2018. vol. 39. pp. 80–89.
66. Yu C., Jiang X., Yu S., Yang C. Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation. *Robotics and Computer-Integrated Manufacturing*. 2020. vol. 64. pp. 1–15.
67. Li M. et al. Blockchain-enabled Secure Energy Trading with Verifiable Fairness in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*. 2020. vol. 16. no. 10. pp. 6564–6574.
68. Han D., Zhang C., Ping J., Yan Z. Smart contract architecture for decentralized energy trading and management based on blockchains. *Energy*. 2020. vol. 199. pp. 1–14.
69. Lu H., Huang K., Azimi M., Guo L. Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks. *IEEE Access*. 2019. vol. 7. pp. 41426–41444.
70. Anwar H., Arasu M., Ahmed Q. Ensuring fuel economy performance of commercial vehicle fleets using blockchain technology. Proceedings of SAE World Congress Experience (WCX 2019). 2019. pp. 1510–1516.
71. Pan J. et al. EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts. *IEEE Internet of Things Journal*. 2018. vol. 6. no. 3. pp. 4719–4732.
72. Seitz, A.; Henze, D.; Miehle, D.; Bruegge, B.; Nickles, J.; Sauer, M. Fog computing as enabler for blockchain-based IIoT app marketplaces-A case study. Proceedings of the 2018 Fifth international conference on internet of things: systems, management and security. 2018. pp. 182–188.
73. Koshy P., Babu S., Manoj B.S. Sliding Window Blockchain Architecture for Internet of Things. *IEEE Internet of Things Journal*. 2020. vol. 7. no. 4. pp. 3338–3348.
74. Luo J., Chen Q., Yu F.R., Tang L. Blockchain-enabled software-defined industrial internet of things with deep reinforcement learning. *IEEE Internet of Things Journal*. 2020. vol. 7. no. 6. pp. 5466-=–5480.
75. Ge C., Liu Z., Fang L. A blockchain based decentralized data security mechanism for the Internet of Things. *Journal of Parallel and Distributed Computing*. 2020. vol. 141. pp. 1–9.

76. Chi J. et al. A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things. *Journal of Network and Computer Applications*. 2020. vol. 167. pp. 1–10.
77. Li D., Hu Y., Lan M. IoT device location information storage system based on blockchain. *Future Generation Computer Systems*. 2020. vol. 109. pp. 95–102.
78. Cebe M., Erdin E., Akkaya K., Aksu H., Uluagac S. Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. *IEEE Communications Magazine*. 2018. vol. 56. no. 10. pp. 50–57.
79. Rathee G. et al. A blockchain framework for securing connected and autonomous vehicles. *Sensors*. 2019. vol. 19. no. 14. pp. 1–15.
80. Qian Y. et al. Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles. *IEEE Network*. 2020. vol. 34. no. 2. pp. 46–51.
81. Evsutin O.O., Kokurina A.S., Meshcheryakov R.V. A review of methods of embedding information in digital objects for security in the internet of things. *Computer optics*. 2019. vol. 43. no. 1. pp. 137–154.
82. Al-Shayea T.K., Mavromoustakis C.X., Batalla J.M., Mastorakis G. A hybridized methodology of different wavelet transformations targeting medical images in IoT infrastructure. *Measurement*. 2019. vol. 148. pp. 1–14.
83. Prasetyo H., Hsia C.-H., Liu C.-H. Vulnerability attacks of SVD-based video watermarking scheme in an IoT environment. *IEEE Access*. 2020. vol. 8. pp. 69919–69936.
84. Liu J. et al. Robust Watermarking Algorithm for Medical Volume Data in Internet of Medical Things. *IEEE Access*. 2020. vol. 8. pp. 93939–93961.
85. Peng H., Yang B., Li L., Yang Y. Secure and Traceable Image Transmission Scheme Based on Semitensor Product Compressed Sensing in Telemedicine System. *IEEE Internet of Things Journal*. 2020. vol. 7. no. 3. pp. 2432–2451.
86. Pu Y.-F., Zhang N., Wang H. Fractional-Order Spatial Steganography and Blind Steganalysis for Printed Matter: Anti-Counterfeiting for Product External Packing in Internet-of-Things. *IEEE Internet of Things Journal*. 2019. vol. 6. no. 4. pp. 6368–6383.
87. Evsutin O. et al. Algorithm for Embedding Digital Watermarks in Wireless Sensor Networks Data with Control of Embedding Distortions. Proceedings of the 2nd International Conference on Distributed and Computer and Communication Networks (DCCN 2019). 2019. pp. 574–585.
88. Hoang T.-M., Bui V.-H., Vu N.-L., Hoang D.-H. A Lightweight Mixed Secure Scheme based on the Watermarking Technique for Hierarchy Wireless Sensor Networks. Proceedings of the 34th International Conference on Information Networking (ICOIN 2020). 2020. pp. 649–653.
89. Xiao X., Gao G. Digital Watermark-Based Independent Individual Certification Scheme in WSNs. *EEE Access*. 2019. vol. 7. pp. 145516–145523.
90. Wang B., Kong W., Li W., Xiong N.N. A dual-chaining watermark scheme for data in-tegrity protection in internet of things. *Computers, Materials and Continua*. 2019. vol. 58. no. 3. pp. 679–695.
91. Ferdowsi A., Saad W. Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems. *IEEE Transactions on Communications*. 2018. vol. 67. no. 2. pp. 1371–1387.
92. Hameed K. et al. Towards a for-mally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks. *Future Generation Computer Systems*. 2018. vol. 82. pp. 274–289.
93. Nguyen V.-T. et al. A lightweight watermark scheme utilizing MAC layer behaviors for wireless sensor networks. Proceedings of the 3rd International Conference on Recent Advances in Signal Processing, Telecommunications and Computing (SigTelCom 2019). 2019. pp. 176–180.
94. Huang H., Zhang L. Reliable and Secure Constellation Shifting Aided Differential Radio Frequency Watermark Design for NB-IoT Systems. *IEEE Communications Letters*. 2019. vol. 23. no. 12. pp. 2262–2265.

95. Rubio-Hernan J., De Cicco L., Garcia-Alfaro J. Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems. *Transactions on Emerging Telecommunications Technologies*. 2018. vol. 29. no. 7. pp. 1–17.
96. Song Z., Skuric A., Ji K. A Recursive Watermark Method for Hard Real-Time Industrial Control System Cyber-Resilience Enhancement. *IEEE Transactions on Automation Science and Engineering*. 2020. vol. 17. no. 2. pp. 1030–1043.
97. Zhao B. et al. Y-DWMS: A Digital Watermark Management System Based on Smart Contracts. *Sensors*. 2019. vol. 19. no. 14. pp. 1–17.
98. Qian Y. et al. Blockchain-Based Privacy-Aware Content Caching in Cognitive Internet of Vehicles. *IEEE Network*. 2020. vol. 34. no. 2. pp. 46–51.
99. Zhang C. et al. Blockchain-Enabled Accountability Mechanism Against Information Leakage in Vertical Industry Services. *IEEE Transactions on Network Science and Engineering*. 2020.
100. Chen J., Gupta V., Quevedo D., Tesi P. Privacy and security of cyberphysical systems. *International Journal of Robust and Nonlinear Control.* 2020. vol. 30. pp. 4165–4167.
101. Lin H., Alemzadeh H., Iyer R. Challenges and Opportunities in the Detection of Safety-Critical Cyberphysical Attacks. *Computer.* 2020. vol. 53. no. 3. pp. 26–37.
102. Iskhakov A., Meshcheryakov R. Intelligent System of Environment Monitoring on the Basis of a Set of IOT-Sensors. 2019 International Siberian Conference on Control and Communications. 2019. pp. 1–5.
103. Iskhakov A., Iskhakova A., Meshcheryakov R. Dynamic Container Virtualization as a Method of IoT Infrastructure Security Provision. Cyber-Physical Systems and Control. Lecture Notes in Networks and Systems. 2020. vol. 95. pp. 482–490.