Иван Б. Гетманюк[1], Иван Р. Федоров[2], Равиль С. Енгалычев[3,4]
[1,2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Кронверкский пр., 49, лит. А, Санкт-Петербург, 197101, Россия
[3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, Москва, 115409, Россия
[4]ПАО «Газпромнефть», Киевская,5 к. 4, Санкт-Петербург, Россия, 190013
[1]e-mail: ibgetmaniuk@itmo.ru, https://orcid.org/0000-0002-9075-998X
[2]e-mail: Ivanfedorov@itmo.ru, https://orcid.org/0000-0003-2422-4714
[3,4]e-mail: rsengalychev@gmail.com, https://orcid.org/0000-0001-9230-819X

ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ

DOI: http://dx.doi.org/10.26583/bit.2023.1.03

Аннотация. Одной из критичных и ключевых проблем в области безопасности промышленного Интернета вещей является аутентификация. Основной целью данной работы является выявление возможных методов решения вопросов аутентификации. Актуальность исследования подтверждается «Доктриной информационной безопасности Российской Федерации», и возникающими рисками, вызванными информационно-техническим воздействием на промышленные объекты в текущей геополитической обстановке. На основании представленного обзора литературы приведены архитектура промышленного Интернета вещей, варианты защиты протоколов аутентификации от известных атак, а также варианты защиты с применением технологии блокчейн. При анализе сетевых моделей выявлено, что варианты защиты информации никак не зависят от самой модели, а зависят от архитектурного уровня, на котором выстраивается защита конкретной модели. В статье рассмотрены достоинства и недостатки вариантов защиты, которые следует учитывать при внедрении. Полученные результаты могут быть использованы для выбора метода защиты протокола аутентификации при построении информационной системы в области Интернета вещей.

Ключевые слова: интернет вещей, промышленный интернет вещей, безопасность, аутентификация, блокчейн.
Для цитирования: ГЕТМАНЮК Иван Б.; ФЕДОРОВ Иван Р.; ЕНГАЛЫЧЕВ Равиль С. ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ. Безопасность информационных технологий, [S.l.], т. 30, № 1, с. 40–57, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1477. DOI: http://dx.doi.org/10.26583/bit.2023.1.03.

Ivan B. Getmanyuk[1], Ivan R. Fedorov[2], Ravil S. Engalychev[3]
[1,2]Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, Kronverkskij pr., 49, lit. A, 197101, Saint Petersburg, Russia
[3]National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute), Kashirskoe shosse, 31, Moscow, 115409, Russia
[4]PAO Gazpromneft, Kievskaya,5 k. 4, Saint Petersburg, Russia, 190013
[1]e-mail: ibgetmaniuk@itmo.ru, https://orcid.org/0000-0002-9075-998X
[2]e-mail: Ivanfedorov@itmo.ru, https://orcid.org/0000-0003-2422-4714
[3,4]e-mail: rsengalychev@gmail.com, https://orcid.org/0000-0001-9230-819X

Research of authentication methods in the industrial internet of things

DOI: http://dx.doi.org/10.26583/bit.2023.1.03

Abstract. One of the most critical and key issues in the field of the Industrial Internet of Things security is the authentication. The main aim of this paper is to identify possible methods of solving authentication issues. The relevance of the research is confirmed by the “Information Security Doctrine of the Russian Federation” and emerging risks caused by information and technical impact on industrial facilities in the

current geopolitical environment. Based on the presented literature review, the architecture of the industrial Internet of things, options for protecting authentication protocols from known attacks, as well as options for protection using blockchain technology are presented. When analyzing network models, it was revealed that information protection options do not depend on the model itself, but depend on the architectural level at which the protection of a particular model is built. The paper discusses the advantages and disadvantages of various protection options that should be considered during its implementation. The obtained results can be used to select a method for protecting the authentication protocol when building an information system in the field of the Internet of things.

Keywords: internet of things, industrial internet of things, security, authentication, blockchain.
For citation: GETMANYUK Ivan B.; FEDOROV Ivan R.; ENGALYCHEV Ravil S. Research of authentication methods in the industrial internet of things. IT Security (Russia), [S.l.], v. 30, no. 1, p. 40–57, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1477. DOI: http://dx.doi.org/10.26583/bit.2023.1.03.

Введение

Интернет оказал значительное влияние на современные технологии благодаря широкому применению, позволяя общаться и выполнять ежедневные задачи, не беспокоясь о расстоянии. С каждым днем все больше и больше устройств подключается к Интернету. Эволюция Интернета подстегнула концепцию подключения традиционно несетевых устройств к Интернету, в рамках тенденции, известной как Интернет вещей (Internet of Things, IoT) – концепция сети передачи данных между физическими объектами («вещами»), оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой [1]. С интеграцией устройств IoT в различные отрасли промышленности сформировалась концепция Промышленного Интернета вещей, которая привлекает все больше внимания [2]. Промышленный (индустриальный) Интернет вещей (Industrial Internet of Things, IIoT) – это IoT для корпоративного отраслевого применения – система объединенных компьютерных сетей и подключенных промышленных (производственных) объектов со встроенными датчиками и программным обеспечением для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека [3].

IoT все чаще используется во всем мире для ежедневного улучшения качества жизни. Области приложений IoT приведены на рис. 1. Эти области включают транспорт, промышленные системы, приложения для здравоохранения, маркетинг, умное сельское хозяйство, умные дома, умные города и даже умное образование. Данные приложения напрямую влияют на жизнь человека [4].

Различные компании разрабатывают и выпускают устройства IoT, которые подходят для различных отраслей промышленности и повседневной жизни, но, к сожалению, многие из этих продуктов имеют серьезные проблемы с безопасностью из-за недостатков архитектуры, в результате чего конфиденциальность данных (в том числе персональные данные пользователей) и целостность становится главной проблемой в развитии этой технологии [5].

Поэтому важным условием распространения IoT должно быть повышение кибербезопасности платформ и конечного оборудования. Производители устройств и разработчики программного обеспечения берут на себя защиту от внешнего воздействия и киберрисков, в том числе выявление уязвимостей и проверку устройств [6].

Проблема рисков для безопасности и конфиденциальности IoT широко изучалась исследовательским сообществом [7, 8]. Основными причинами недостатков присущих IoT, являются отсутствие или плохо реализованные функции безопасности, которые часто остаются неисправленными из-за сложности или отсутствия обновлений [9]. Кроме того, обычные пользователи не осведомлены об угрозах безопасности, создаваемых устройствами IoT, и, более того, не знают, как безопасно настроить свои сети [10]. В

результате устройства IoT все чаще становятся жертвами атаки, например, Bashlite [11] и Mirai [12].

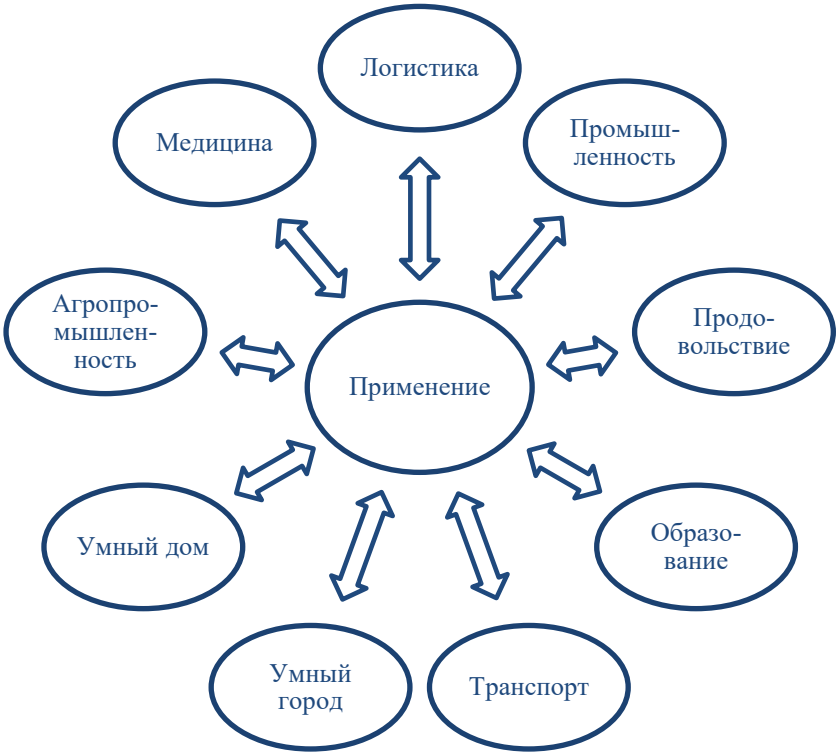

Рис. 1. Приложения IoT
Fig. 1. IoT applications that illustrate vertical independent services and domain applications

Существенной разницей между IoT и IIoT областями является, например, более длительный срок службы промышленных устройств по сравнению с потребительскими устройствами, требующими последующего обеспечения мер безопасности и длительного управления исправлениями. Также, сети IIoT, как правило, крупнее по масштабу по сравнению с потребительскими состоящими из нескольких устройств. Кроме того, расширенная и динамичная взаимосвязь между устройствами IoT усложняет внедрение защищенной сетевой архитектуры, основанной на сегрегации, особенно по мере развития предлагаемых услуг [13].

На основании существующих публикаций на тему IoT и IIoT, рассмотрения возможных компьютерных атак на данные компьютерные сети, проведем анализ существующих вариантов решения защиты информации, передаваемой при аутентификации устройств в этих сетях. Результатом исследования является выявление достоинств и недостатков рассматриваемых вариантов, поиск нерешенных проблем в части аутентификации, а также выбор наиболее приоритетного варианта или технологии для защиты механизма аутентификации в IIoT.

1. Вопросы безопасности промышленного Интернета вещей

Решение вопросов безопасности и аутентификации в IIoT изучается исследователями регулярно [14–15]. Общий подход по решениям заключается в необходимости классифицировать атаки в соответствии с типичными архитектурными

уровнями IIoT, для обеспечения подходящих контрмер на каждом уровне. В настоящее время не существует единой и общепринятой архитектуры IIoT, они зависят от требований системы и выбора разработчика, так как отсутствуют единые стандарты.

Различные разработчики поддерживают такие стандарты, как WirelessHART (сетевая технология для беспроводных устройств на базе протокола Highway Addressable Remote Transducer Protocol) [16] и Foundation Fieldbus (цифровая система связи автоматизации, включающая два протокола информационного обмена – H1 и High Speed Ethernet) [17]. Преимущество использования стандартов заключается в том, что если определенный тип датчика/устройства от одного поставщика выходит из строя, то его можно было бы заменить устройством от другого поставщика, если они используют тот же стандарт протокола и сетевую технологию. Новые стандарты начали появляться в связи с необходимостью мониторинга промышленных систем и процессов, например, стандарты промышленной беспроводной сенсорной сети (IWSN) ZigBee, WirelessHART, беспроводная сеть ISA 100.11a и беспроводная сеть для промышленной автоматизации процессов (WIA-PA) [18].

В [19–21] представлены различные варианты архитектуры IIoT, поскольку существуют значимые различия с точки зрения бизнеса, использования, функциональности, масштабируемости и реализации систем. Архитектура IIoT классифицируется на основе слоев – ограниченного набора ресурсов, с помощью которых реализуется множество прикладных задач, характерных для данного слоя (рис. 2). Для исследования будем рассматривать архитектуру IIoT, обсуждаемую в [20]. Это четырехуровневая архитектура, которая потенциально может быть использована в различных системах IIoT (состоит из уровней: сбор данных, сеть, обслуживание и приложение). Выбранная архитектура может содержать компоненты трехслойной архитектуры IIoT, и в то же время четырехслойная архитектура может быть легко дополнена дополнительными компонентами для представления более гранулированной пятислойной архитектуре IIoT.

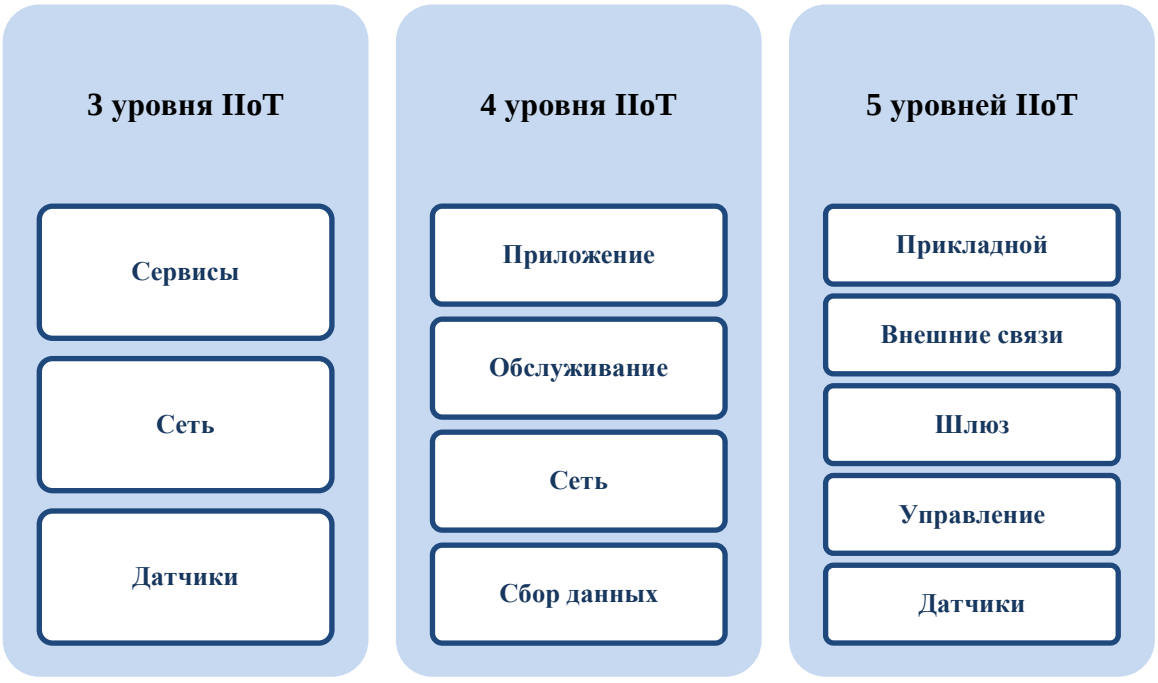

Рис. 2. Архитектуры IIoT [22]
Fig. 2. IIoT architectures [22]

Четырёхуровневая архитектура может обеспечивать базовые функциональные возможности и способна поддерживать бесперебойную связь с конечными пользователями. Уровень сбора данных собирает информацию из физической среды и отправляет собранную информацию на следующий уровень (сетевой уровень). Сетевой уровень управляет информацией и преобразует ее на следующий уровень (на уровень поддержки). Уровень обслуживания выполняет задачи анализа данных (например, разделение данных, композиция и т.д.). И наконец, через уровень приложения конечные пользователи могут получить доступ к нужным сервисам.

Вопросы безопасности для систем IIoT, масштаб и характер злоумышленника отличаются от IoT. В случае разнородной динамично развивающейся системы IIoT каждое устройство имеет свою собственную уникальную идентификацию и аутентификацию, при этом они могут быть неизвестны друг другу заранее [14]. В пяти из одиннадцати основных вопросов безопасности в IIoT (рис. 3) обеспечение безопасности процедур управления идентификационными и аутентификационными данными устройств имеет решающее значение для защиты от мошенничества, что также подтверждается в [15, 23].

Корректные процедуры идентификации с аутентификацией устройств IIoT позволяют выполнить правомочную авторизацию устройства для разрешения доступа к определенной информации. Ущерб может быть нанесен путем искажения идентификации устройства (с использованием фальсификации идентификационных данных в системах без процедур аутентификации). Либо может быть выполнено подключение к шлюзу IIoT с помощью перехвата аутентификационных данных, когда злоумышленники получают незаконный доступ к закрытым данным.

При аутентификации может передаваться не только идентификационная информация устройства, но и атрибуты, и содержание системы [24], что также является чувствительной информацией и требует ее защиты.

Рис. 3. Основные вопросы безопасности системы IIoT [19]
Fig. 3. Outline of the core security issues in an IIoT system [19]

Большинство угроз безопасности информации реализуется путем осуществления атак на информационные активы внутренними и внешними нарушителями и/или программными средствами с использованием уязвимостей. Активами на различных уровнях архитектуры IIoT, будут являются:

1) датчики учета и контроля, программируемые логические контроллеры;
2) шлюзы передачи данных IIoT;
3) узлы сетевого оборудования связи;
4) серверные узлы;
5) информация в базах данных;
6) распределённая, самоорганизующаяся сеть датчиков и исполнительных устройств, объединённых между собой посредством радиоканала (Wireless sensor network, WSN). Классификация атак на беспроводные сенсорные сети по направлению воздействия приведена на рис. 4.

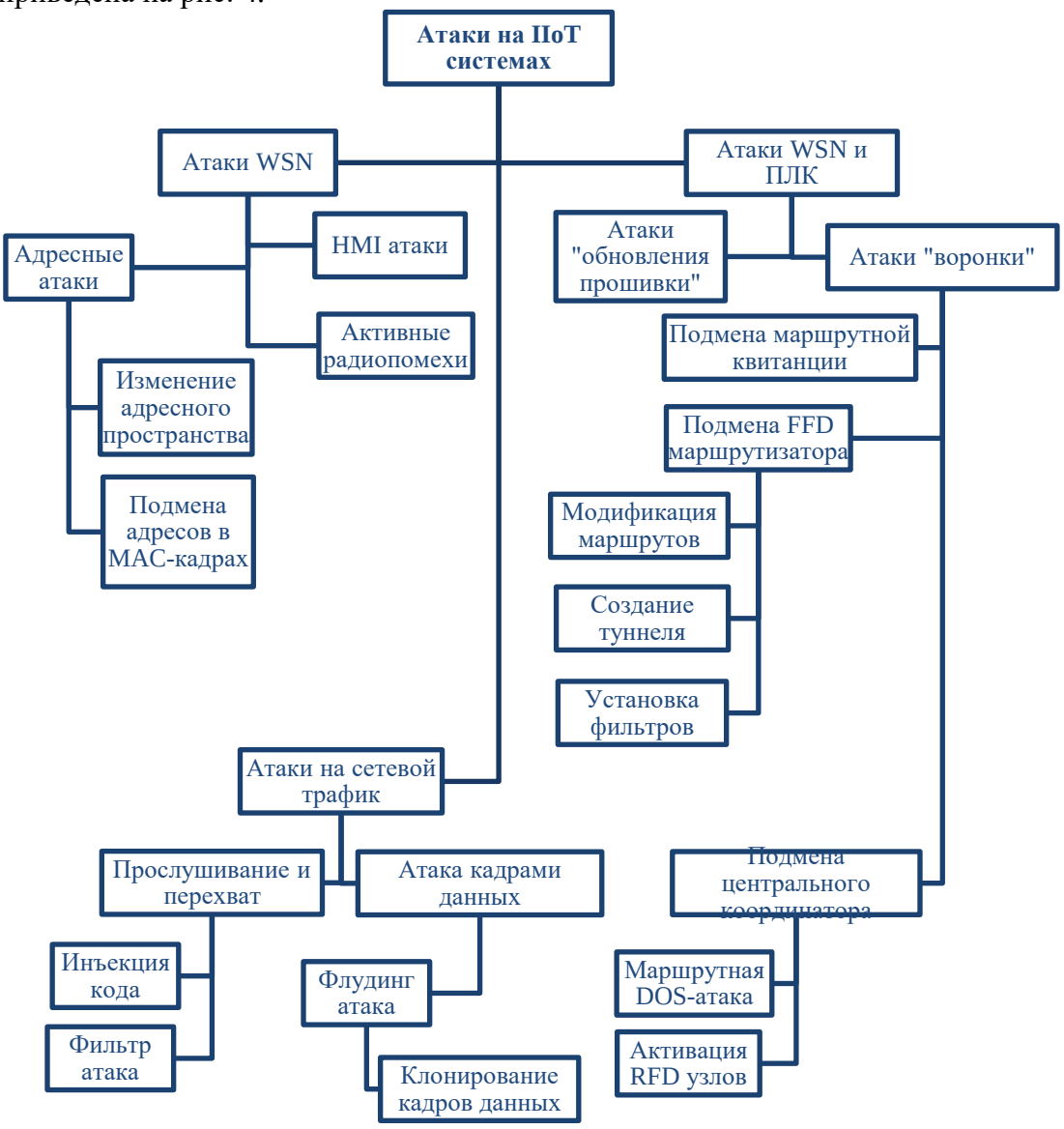

Рис. 4. Классификация атак в промышленных беспроводных сенсорных сетях по направлению воздействия [25]

Fig. 4. Classification of attacks in industrial wireless sensor networks by the direction of the impact [25]

Для атаки «инфицирование данных» может применяться атака «человек посередине» (Man-in-the-middle, MITM), доступ к каналу при которой потребует идентификации атакующего [26]. Не корректная авторизация в системе IIoT приводит к снижению конфиденциальности устройств и данных в каждой системе или сети [27]. Обладая, например, информацией о местоположении, злоумышленник может получить контроль через устройство посредством его отслеживания или других устройств, которые подключены к нему и обмениваются информацией в режиме реального времени [28].

Для корректности взаимодействия устройств IIoT должны использоваться безопасные протоколы обмена информации. В промышленной отрасли необходимо постоянное развитие стандартов взаимодействия. Подводя итог главы, можно сделать вывод, что в настоящее время существует достаточно большое количество вопросов безопасности IIoT и возможных методов атак.

2. Базовые методы защиты IIoT и модели аутентификации

Базовые методы защиты IIoT четырехуровневой архитектуры состоят из:

– систем обнаружения сетевых вторжений (Network-Based Intrusion Detection System, NIDS);

– систем предотвращения вторжений через периметр сети (Network-Based Intrusion Prevention System, NIPS);

– автономных систем предотвращения вторжений на сетевых узлах (Host-Based Intrusion Prevention System, HIPS);

– систем антивирусной защиты;

– межсетевых экранов;

– систем аутентификации и управления доступом пользователей;

– систем аутентификации сетевых ресурсов и кадров данных;

– систем криптографической защиты и управления ключами и т.п.

В соответствии с рассматриваемым четырёхуровневым архитектурным слоем IIoT базовые методы защиты информации приведены на рис. 5.

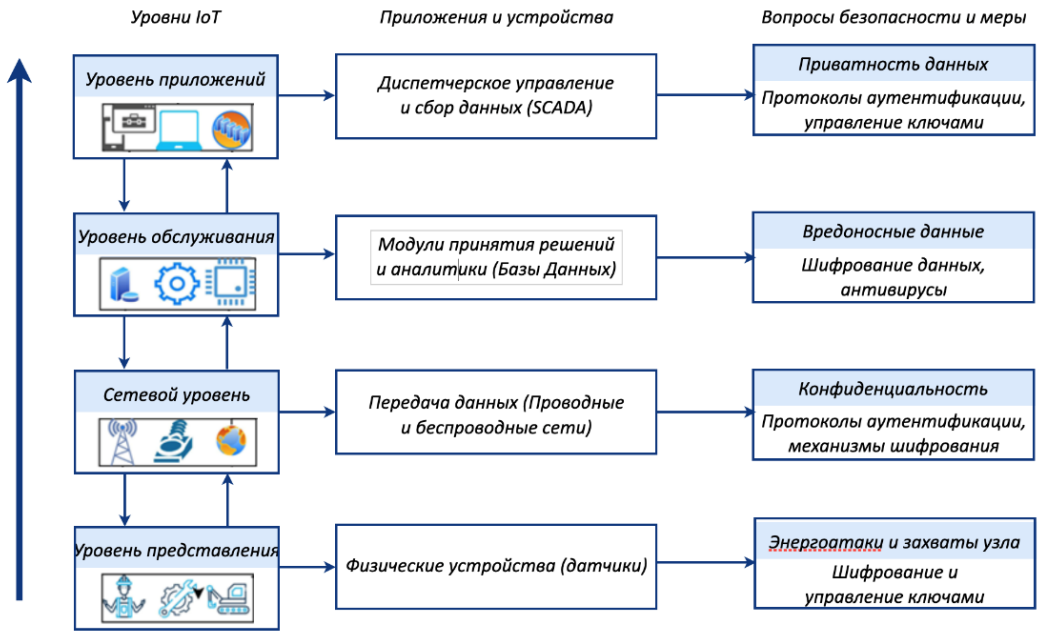

Рис. 5. Базовые механизмы безопасности четырехуровневой архитектуры IIoT [20]
Fig. 5. IoT layered architecture, technology, security issues and basic security mechanisms [20]

Процедура аутентификации является ключевой и неотъемлемой частью архитектуры IIoT на уровнях: приложения, сети и представления.

Разработанный процесс выбора протокола аутентификации для IIoT основан на следующих шагах [29]:

1) Определение сетевой модели: межмашинное взаимодействие (Machine to Machine Communications, M2M), Интернет транспортных средств (Internet of Vehicles, IoV), Интернет распределенных источников энергии (Internet of Energy, IoE), Интернет датчиков (Internet of Sensors, IoS) и т.д.

2) Определение модели аутентификации (взаимная аутентификация, переадресация безопасности, анонимность и скрытность и т.д.).

3) Определение модели атаки (повторная атака, атака на украденную смарт-карту, атака с административным доступом, атака на угадывание пароля в офлайн режиме, атака с подменой и атака на захват сенсора и т.д.).

4) Выбор мер защиты (криптографические методы, фильтр Блума, биометрия, смарт-карты, полином доступа и хаотические карты Чебышева и т.д.).

5) Описание основных этапов протокола (начальная настройка; процесс регистрации и т.д.).

6) Анализ безопасности с использованием формализованных проверок безопасности (ProVerif, BAN-logic и AVISPA и т.д.).

7) Оценка производительности (с точки зрения объема памяти, сложности вычислений, накладных расходов на связь и частоты ошибок и т.д.).

На основании проведенного анализа [29] разработана классификация вариантов аутентификации для IIoT приведенная на рис. 6.

Рис. 6. Классификация вариантов аутентификации для IIoT
Fig. 6. Categorization of authentication methods for the IIoT

Далее приведен анализ возможных вариантов защиты протоколов аутентификации сетевых моделей в соответствии с процессом выбора протокола аутентификации.

2.1 Аутентификации для модели межмашинного взаимодействия (M2M)

M2M – это информационная технология, которая может входить в состав IIoT, в основе которой лежит принцип взаимодействия двух или более объединенных устройств. В M2M коммуникация может строиться на проводной или беспроводной связи, и позволяет обмениваться данными в одностороннем или двухстороннем направлении.

Чтобы ускорить процесс аутентификации в модели M2M по беспроводным каналам связи и избежать перегрузки аутентификации, Лай и др. [30] сосредоточились на проблеме групповой аутентификации и согласования ключей для устройств M2M с ограниченными ресурсами в сетях 3GPP. В частности, авторы предложили новую облегченную схему аутентификации на основе групп для M2M с ограниченными ресурсами, называемую GLARM. Сеть модели, используемая в исследовании основана на стандарте 3GPP с тремя доменами, включая доступ к сети, измененное ядро пакета и домен, отличный от 3GPP, например, Интернет. Чтобы гарантировать взаимную аутентификацию сущностей и безопасное согласование ключей, схема GLARM использует две основные фазы – фазу инициализации и фазу групповой аутентификации и согласования ключей. Достоинства: Устойчивость к DOS-атаке, атаке перенаправления и атаке MITM, низкие накладные расходы на вычисления, может обеспечить QoS для устройств связи машинного типа. Недостатки: некоторые модели конфиденциальности не анализируются, такие как конфиденциальность местоположения и конфиденциальность личных данных, не учитываются нагрузки на память.

2.2 Аутентификации для модели Интернета транспортных средств (IoV)

IoV – это система реализации интеллектуальных транспортных систем, которая в связи с высоким развитием транспортных технологий, высокой скоростью Интернета стала очень востребована. IoV обеспечивает интеграцию транспортных средств с компонентами общественной инфраструктуры, датчиками, вычислительными узлами, и другими транспортными средствами через Интернет. Интеграция IoV направлена на создание окружающей среды для людей, и повышение безопасности всех участников дорожного движения.

Для защиты экосистемы электромобилей от согласованных киберфизических атак Чан и Чжоу [31] предложили двухфакторный протокол аутентификации киберфизических устройств, который может быть применен в IoV. Протокол предназначен для аутентификации киберфизического устройства для предотвращения атаки подмены и механизм безопасности интерфейсной шины для обеспечения надежной связи между интеллектуальным устройством и электромобилем. Достоинства: Устойчивость к атакам подмены. Недостатки: отсутствует сравнение с другими схемами работы, средняя задержка сообщения и проверки не оценена.

2.3 Аутентификации для модели Интернета распределенных источников энергии (IoE)

IoE – совокупность технологий и бизнес-моделей, обеспечивающая возможность гибкого горизонтального взаимодействия «всех со всеми» в связи с производством, передачей и потреблением электроэнергии. IoE тесно связано с технологиями распределенной энергетики (распределенных энергоресурсов, Distributed Energy Resources, DER) к которой относится: распределенная генерация, управление спросом, управление энергоэффективностью, микросети, распределенные системы хранения электроэнергии, электромобили.

Для обеспечения конфиденциальности и целостности проверки аутентификации, Чим и др. [32] предложили схему, называемую PASS, для иерархической структуры умных сетей. Схема PASS фокусируется только на подсистеме «подстанция-потребитель», где реальная идентификация любого интеллектуального устройства может быть известна только центру управления, использующему концепцию псевдоидентификации. Достоинства: требуется дополнительные 368 мс для проверки подписи на подстанции, эффективен в общем нормальном уровне трафика при атаке, дополнительная нагрузка на сообщение составляют всего 20 байт на сообщение запроса. Недостатки: атаки на маршрутизацию не рассматриваются, как и атаки через wormhole, расходы на хранение не учитываются, нет сравнения с другими схемами работы.

2.4 Аутентификации для модели Интернета датчиков (IoS)

IoS – совокупность технологий и бизнес-моделей, обеспечивающих взаимодействие между датчиками (сенсорами) IoT на уровне сбора данных или так называемого «полевого уровня». IoS больше похож на «корни дерева» с датчиками на всех концах передающие данные в основной «ствол» Интернет.

Чанг и Ли [33] предложили гибкий протокол аутентификации с использованием смарт-карты для WSNs, который работает в двух режимах: обеспечивает облегченную схему аутентификации и расширенный протокол на основе ECC, который обеспечивает идеальную прямую секретность. Данные модели эффективны с точки зрения вычислительных затрат на этапах аутентификации. Протокол на основе ECC подходит для использования в экстремально агрессивной среде, где захват узла происходит с высокой вероятностью. Поскольку модификация незначительна, оба режима могут быть реализованы на сенсорном узле с небольшими затратами на хранение. Протокол аутентификации может легко переключаться между двумя режимами в зависимости от требований безопасности. Достоинства: учитывает безопасность сеансового ключа, совершенную секретность пересылки и анонимность пользователя; устойчив к атакам, а именно к повторной атаке и атаке с потерянной смарт-картой, эффективность с точки зрения вычислительных затрат на этапах аутентификации. Недостатки: сохранение конфиденциальности не анализируется по сравнению со схемой GLARM.

В табл. 1 приведены виды атак, отражаемые рассматриваемыми протоколами (методами) защиты данных. Стоит отметить, что при анализе сетевых моделей IIoT представленных выше выявлено, что варианты защиты информации никак не зависят от модели M2M, IoV, IoE или IoS, а зависят от архитектурного уровня, на котором выстраивается защита конкретной модели.

Таблица 1. Виды атак, отражаемые рассматриваемыми протоколами (методами) защиты данных

Вид атаки	Исследователи			
	Лай и др. [30]	Чан и Чжоу [31]	Чим и др. [32]	Чанг и Ли [33]
Атака воспроизведением	+/–	–	–	–
Атака на однотипные устройства	–	–	–	–
Составная атака (Composition)	–	–	–	–
Атака с перенаправлением (Redirection)	+	–	–	+/–
Атака человек посередине (MITM)	+	+/–	+/–	+/–
Атака подмены (Substitution)	+/–	+	–	+/–
DoS – атака	+	–	–	+/–
Replay – атака	–	+/–	+	+
Атака подделкой (Forging)	–	–	+/–	+/–
Атака сговором (Colluding)	–	–	+/–	+/–
Флуд – атака	–	–	–	+/–
Атака по сторонним или побочным каналам (Side-channel)	–	–	–	–
Ложные сообщения (False messages)	–	–	+/–	+/–
Атака Сивиллы (Sybil)	–	–	+/–	–
Отслеживание движения (Movement tracking)	–	–	–	–
Изменение сообщений	–	+/–	+/–	+/–
Атака подражания (Impersonation)	–	–	+/–	+/–
Метод угадывай и определяй (Guessing)	–	–	–	+/–
Атака с украденным верификатором (Stolen-verifier)	–	–	–	–
Атака червоточины (Wormhole)	+/–	+/–	–	+/–
Атака черной дыры (Blackhole)	+/–	+/–	–	+/–
Атака с отслеживанием атрибутов (Attribute-trace)	–	–	–	–
Атака на подслушивание (Eavesdropping)	–	–	+/–	+/–
Атака на основе подобранного открытого текста (Chosen-plaintext)	–	+/–	–	–
Спам	–	+/–	–	+/–
Кража идентификационных данных (Identity theft)	–	+/–	+/–	+/–
Манипуляция пользователем (User manipulation)	–	+/–	+/–	+/–
Атака маршрутизации (Routing)	–	+/–	–	+/–
Атака связности (Linkability)	–	–	–	+/–
Отказ обслуживания (Rejection)	–	–	+/–	+/–
Атака с последовательным ответом (Successive-response)	–	–	–	–
Анализ пакетов (Packet analysis)	+/–	–	+/–	–
Отслеживание пакетов (Packet tracing)	+/–	–	+/–	–
Перебор значений (брутфорс)	+/–	–	–	–

«+» – поддерживается полностью; «–» – не поддерживается; «+/–» –поддерживается частично.

3. Методы защиты информации в IIoT на основе блокчейн

Технология блокчейн была создана для криптовалюты биткоина, но ее можно использовать независимо от платежной системы. Блокчейн можно определить как базу данных транзакций, дублированную и распределенную по нескольким узлам (компьютеры, центры обработки данных и т.д.), собранным в одноранговой сети. База данных состоит из транзакций, например, денежные операции, данные о состоянии оборудования и т.д. Блокчейн представляет собой цепочку блоков, каждый из которых состоит из тела и заголовка. Тело представляет собой набор транзакций, которые могут храниться в открытом или зашифрованном виде. Заголовок содержит информацию о блоке, который представляет собой хэш транзакций блока, метку времени, номер блока и хэш предыдущего блока [34]. В результате система создает цепочку связанных и упорядоченных блоков, и чем длиннее цепочка, тем сложнее ее подделать. В зависимости от типа и характера блокчейн каждый узел может читать транзакции или читать и записывать новые транзакции. Для того, чтобы добавить новую транзакцию в блокчейн, сеть должна установить процедуру консенсуса для определения того, где эта транзакция должна быть отражена в распределенном реестре. Блокчейн может быть частным (приватным), таким как Hyperledger Fabric [35], или публичным, таким как Bitcoin и Ethereum [36]. В частном блокчейн установлены ограничения по участникам консенсуса, т.е. только выбранные доверенные субъекты имеют право проверять транзакции, для достижения консенсуса в нем не требуется много вычислений, это экономит время и энергию. Публичный блокчейн использует неограниченное количество анонимных узлов, которые безопасно обмениваются данными с помощью пары закрытых / открытых ключей. Время и сложность вычислений возрастают в публичном блокчейн с увеличение количества блоков.

Важная особенность безопасности блокчейн, и сетевого консенсуса, в том, что ему можно доверять, когда 51% всех узлов являются доверенными (честными).

В [37] используется математическая модель объекта исследования в виде совокупности уравнений и неравенств. Фреймворк сочетает в своем арсенале технологии дифференциальной конфиденциальности (DP), федеративное обучение (FEDML), смарт контракты и блокчейн Ethereum (ETHBC). PriModChain использует межпланетную файловую систему (IPFS) для управления данными вне цепочки. Подчеркивается важность машинного обучения (ML), которое позволяет проводить прогнозную аналитику и раскрытие важных идей для преобразования отраслей промышленности, описаны основные достоинства использования технологии в IIoT. Недостаток метода заключается в его низкой скорости работы при смене выборки модели обучения.

В [38] рассматривается решение аутентификационного механизма под названием BCTrust для модели M2M на основе блокчейн. BCTrust основан на принципе «Друг моего друга – мой друг» и развернут на блокчейне Ethereum. Это означает, что, если устройство аутентифицируется в одном кластере, оно становится надежным и принимается всеми остальными кластерами. Блокчейн гарантирует, что сохраненная информация доступна для всех участвующих узлов и защищена от изменений. В смарт-контракте только набор надежных узлов имеет права на запись в блокчейне, что сохраняет его безопасность. Эти привилегированные устройства являются процессорами сети. Каждый CPAN имеет пару закрытых / открытых ключей, что позволяет ему безопасно совершать транзакции с блокчейном. Достоинства: противостоит dos/ddos – наиболее распространенным и опасным сетевым атакам; использует алгоритм цифровой подписи эллиптической кривой (ECDSA) обеспечивает быстрые и надежные транзакции [39]; на основе механизма консенсуса сохраненные данные не могут быть фальсифицированы, а поставленная задача не может быть отменена; защищает секретный симметричный ключ и обмениваемые сообщения

(между устройством и CPAN) от криптоанализа и повторных атак. Недостатки: механизм не изучен на масштабируемости сети.

В [40] предложен протокол, называемый Certcoin, представляющий собой децентрализованную инфраструктуру открытых ключей (PKI), основанный на биткойне. Этот децентрализованный PKI создает, публикует, управляет, обновляет, хранит и отзывает ключи, соответствующие заданным идентификаторам. Основываясь на силе, обеспечиваемой механизмом майнинга Биткоина, он обеспечивает хороший способ аутентификации устройств. Этот протокол решает проблему централизации PKI и избавляет системы от использования доверенных органов власти, что иногда может быть очень дорогостоящим. Однако аутентификация устройств с ограниченными возможностями с использованием дерева хэшей очень дорогая.

Большинство классических механизмов аутентификации и безопасности централизованы и часто требуют еще одной доверенной стороны либо больших сопутствующих затрат, как время и мощности вычислений. Обеспечивая полную децентрализацию, высокую безопасность данных и широкий взгляд на систему, блокчейн является более интересным и безопасным решением. Первое, что можно сделать, это регистрировать в блокчейне идентификатора и соответствующей пары ключей каждого устройства, а затем управлять устройством асимметричной криптографией. Это решение является надежным и безопасным, однако асимметричная криптография нежелательна для датчиков ограниченной емкости.

Как показывает проведенное исследование существует достаточно количество решений проблем аутентификации в IIoT и IoT в целом. Каждое решение будет зависеть от угроз ИБ, рисков ИБ, архитектуры сети, типов датчиков, уровня защиты. При разработке или доработке протокола аутентификации необходимо оценивать его накладные расходы, и устойчивость к взлому. Каждый протокол безопасности либо его модификация изначально должен решать задачи для конкретного кейса, и далее необходимо оценивать возможности его масштабирования.

Полученные результаты сравнения базовых алгоритмов защиты и механизмов с использованием блокчейн приведены в табл. 2.

Таблица 2. Сравнение базовых алгоритмов защиты и механизмов с использованием блокчейн

Методы защиты	Достоинства	Недостатки
Базовые	– различные модели аутентификации – многообразие сетевых моделей	– узконаправленная защита – централизованное управление – «накладные» расходы – целостность доставки – масштабируемость
С применением Blockchain	– децентрализация – целостность данных – конфиденциальность – интегрируемость/ универсальность – масштабируемость – конфиденциальность	– 51% достоверных узлов – «накладные» расходы – прозрачность данных

Заключение

Проведенный анализ работ, показал наличие множеств уязвимостей информационной безопасности в IIoT. Четырёхуровневая архитектура, рассмотренная в

работе, позволяет наглядно представить структуру IIoT, рассмотреть ее компоненты, и провести оценку рисков информационной безопасности на каждом из уровней модели. Выявлено, что важным и ключевым вопросом в IIoT является аутентификация, которая может происходить на уровнях приложения, сети, представления.

Рассмотренные в исследованиях протоколы аутентификации, а также их модификации имеют существенные недостатки, которые могут использоваться злоумышленниками в корыстных целях при атаках на инфраструктуру, что не позволяет использовать эти решения, как универсальные, на рассматриваемой архитектуре IIoT. Тем не менее, они могут использоваться в частных задачах с приведенными ограничениями. Полученные результаты работы планируется применить в дальнейших исследованиях аутентификации в IIoT на основе технологии блокчейн.

СПИСОК ЛИТЕРАТУРЫ:

1. Gartner Expert Glossary. 2022. URL: https://www.gartner.com/en/information-technology/glossary/internet-of-things (дата обращения: 18.11.2022).
2. Malik N. et al. A comprehensive review of blockchain applications in industrial Internet of Things and supply chain systems. Applied Stochastic Models in Business and Industry. 2021. DOI: https://doi.org/10.1002/asmb.2621.
3. Экосистема индустриального интернета России. Исследование. РАЭК. Ростелеком. 2017. URL: https://raec.ru/activity/analytics/9847 (дата обращения: 18.11.2022).
4. Mamdouh M. et al. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. Computers & Security. 2021, vol. 111, p. 102491. DOI: https://doi.org/10.1016/j.cose.2021.102491.
5. Zhao Q. et al. Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. Information Processing & Management. 2020, vol. 57, no. 6, p. 102355. DOI: https://doi.org/10.1016/j.ipm.2020.102355.
6. IoT Барометр МТС. 2021. URL: http://i.content-review.com/s/2b3d9e83b5d522145afd58b0909c1078.pdf (дата обращения: 18.11.2022).
7. Yang K., Blaauw D. and Sylvester D. Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey. IEEE Micro, vol. 37, no. 6, p. 72–89, November/December 2017. DOI: https://doi.org/10.1109/MM.2017.4241357.
8. Capellupo M., Liranzo J., Bhuiyan M.Z.A., Hayajneh T., Wang G. Security and Attack Vector Analysis of IoT Devices. In: Wang, G., Atiquzzaman, M., Yan, Z., Choo, KK. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science(). Springer, Cham. 2017, vol 10658, p. 593–606. DOI: https://doi.org/10.1007/978-3-319-72395-2_54.
9. Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. 2015. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets-XIV). Association for Computing Machinery, New York, NY, USA, Article 5, 1–7. DOI: https://doi.org/10.1145/2834050.2834095.
10. Ulf Lindqvist and Peter G. Neumann. 2017. The future of the internet of things. Commun. ACM 60, 2 (February 2017), p. 26–30. DOI: https://doi.org/10.1145/3029589.
11. Marzano A. et al. The Evolution of Bashlite and Mirai IoT Botnets. IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil. 2018, p. 00813–00818. DOI: https://doi.org/10.1109/ISCC.2018.8538636.
12. Manos Antonakakis et al. Understanding the Mirai botnet. 26th USENIX Security Symposium August 16–18, 2017. Vancouver, BC, Canada. 2017, p. 1093–1110. URL: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf (дата обращения: 18.11.2022).
13. Serror M., Hack S., Henze M., Schuba M. and Wehrle K. Challenges and Opportunities in Securing the Industrial Internet of Things. IEEE Transactions on Industrial Informatics. May 2021, vol. 17, no. 5, p. 2985–2996. DOI: https://doi.org/10.1109/TII.2020.3023507.
14. Liu J., Xiao Y. and Chen C. L. P. Authentication and Access Control in the Internet of Things. 32nd International Conference on Distributed Computing Systems Workshops, Macau, China. 2012, p. 588–592. DOI: https://doi.org/10.1109/ICDCSW.2012.23.
15. Babar S., Mahalle P., Stango A., Prasa N., Prasad, R. Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In: Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D. (eds) Recent Trends

in Network Security and Applications. CNSA 2010. Communications in Computer and Information Science. Springer, Berlin, Heidelberg. Vol. 89, p. 420–429. DOI: https://doi.org/10.1007/978-3-642-14478-3_422010.
16. Saifullah A., Xu Y., Lu C. and Chen Y. Real-Time Scheduling for WirelessHART Networks. 31st IEEE Real-Time Systems Symposium, San Diego, CA, USA. 2010, p. 150–159. DOI: https://doi.org/10.1109/RTSS.2010.41.
17. Dirgantoro K.P., Nwadiugwu W.P., Lee J.M., Kim D.S. Dual fieldbus industrial IoT networks using edge server architecture. Manuf. Lett. 2020, 24, p. 108–112. DOI: https://doi.org/10.1016/j.mfglet.2020.04.006.
18. Devan P., Hussin F.A., Ibrahim R., Bingi K., Khanday F.A. A Survey on the Application of WirelessHART for Industrial Process Monitoring and Control. Sensors vol. 21, 2021. DOI: https://doi.org/10.3390/s21154951.
19. Sisinni E., Saifullah A., Han S., Jennehag U. and Gidlund M. Industrial Internet of Things: Challenges, Opportunities, and Directions. IEEE Transactions on Industrial Informatics. Nov. 2018, vol. 14, no. 11, p. 4724–4734. DOI: https://doi.org/10.1109/TII.2018.2852491.
20. Jayalaxmi P., Saha R., Kumar G., Kumar N. and Kim T.-H. A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges. IEEE Access. 2021, vol. 9, p. 25344–25359. DOI: https://doi.org/10.1109/ACCESS.2021.3057766.
21. Panchal A.C., Khadse V.M. and Mahalle P.N. Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India. 2018, p. 124–130. DOI: https://doi.org/10.1109/GCWCN.2018.8668630.
22. Pal S., Jadidi Z. Analysis of Security Issues and Countermeasures for the Industrial Internet of Things. Applied Sciences. 2021, vol.11(20). DOI: https://doi.org/10.3390/app11209393.
23. Pal S., Hitchens M. and Varadharajan V. Modeling Identity for the Internet of Things: Survey, Classification and Trends. 12th International Conference on Sensing Technology (ICST), Limerick, Ireland. 2018, p. 45–51. DOI: https://doi.org/10.1109/ICSensT.2018.8603595.
24. Mahalle P., Babar S., Prasad N.R., Prasad R. Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges. In: Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D. (eds) Recent Trends in Network Security and Applications. CNSA 2010. Communications in Computer and Information Science. Springer, Berlin, Heidelberg. Vol. 89, p. 430–439. DOI: https://doi.org/10.1007/978-3-642-14478-3_432010.
25. Финогеев А. Маршрутизация и защита данных в беспроводных сенсорных сетях. Lambert Academic Publishing, 2016. – 96 с. URL: https://www.lap-publishing.com/catalog/details/store/ru/book/978-3-659-91987-9/маршрутизация-и-защита-данных-в-беспроводных-сенсорных-сетях?locale=ru (дата обращения: 18.11.2022).
26. Kara M. and Furat M. Client-Server Based Authentication Against MITM Attack via Fast Communication for IIoT Devices. Balkan Journal of Electrical and Computer Engineering. 2018, vol. 6, no. 2, p. 88–93. DOI: https://doi.org/10.17694/bajece.419546.
27. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Network. 2015, vol. 76, p. 146–164. DOI: https://doi.org/10.1016/j.comnet.2014.11.008.
28. Ho G., Leung D., Mishra P., Hosseini A., Song D., Wagner D. Smart Locks: Lessons for Securing Commodity Internet of Things Devices. In Proceedings of the 11th Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–3 June 2016, p. 461–472. DOI: https://doi.org/10.1145/2897845.2897886.
29. Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu. Authentication Protocols for Internet of Things: A Comprehensive Survey. Security and Communication Networks. Hindawi. 2017.URL: https://www.researchgate.net/publication/311808641_Authentication_Protocols_for_Internet_of_Things_A_Comprehensive_Survey (дата обращения: 18.11.2022).
30. Lai C., Lu R., Zheng D., Li H., and Sherman X. GLARM: group-based lightweight authentication scheme for resourceconstrained machine to machine communications. Computer Networks. 2016, vol. 99, p. 66–81.
31. Chan A.C.-F. and Zhou J. Cyber–Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem. IEEE Journal on Selected Areas in Communications. July 2014, vol. 32, no. 7, p. 1509–1517. DOI: https://doi.org/10.1109/JSAC.2014.2332121.
32. Chim T.W., Yiu S.M., Hui L.C.K. and Li V.O.K. PASS: Privacy-preserving authentication scheme for smart grid network. IEEE 2nd International Conference on Smart Grid Communications, SmartGridComm. 2011, p. 196–201. DOI: https://doi.org/10.1109/SmartGridComm.2011.6102316.
33. Chang C.-C. and Le H.-D. A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks. IEEE Transactions on Wireless Communications. 2016, vol. 15, no. 1, p. 357–366. DOI: https://doi.org/10.1109/TWC.2015.2473165.
34. Merkle tree. EU General Data Protection Regulation. 2020. URL: https://en.bitcoinwiki.org/wiki/Merkle_tree (дата обращения: 18.11.2022).

35. Marko Vukolić. Rethinking Permissioned Blockchains. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC '17). Association for Computing Machinery, New York, NY, USA. 2017, p. 3–7. DOI: https://doi.org/10.1145/3055518.3055526.
36. Ethereum Homestead Documentation. Online. Ethereum community. 2016. URL: http://www.ethdocs.org/en/latest/index.html (дата обращения: 18.11.2022).
37. Arachchige P.C.M., Bertok P., Khalil I., Liu D., Camtepe S. and Atiquzzaman M. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. IEEE Transactions on Industrial Informatics. Sept. 2020, vol. 16, no. 9, p. 6092–6102. DOI: https://doi.org/10.1109/TII.2020.2974555.
38. Hammi M.T., Bellot P. and Serhrouchni A. BCTrust: A decentralized authentication blockchain-based mechanism. IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain. 2018, p. 1–6. DOI: https://doi.org/10.1109/WCNC.2018.8376948.
39. Johnson D., Menezes A. & Vanstone S. The Elliptic Curve Digital Signature Algorithm (ECDSA). IJIS 1, 36–63 (2001). DOI: https://doi.org/10.1007/s102070100002.
40. Conner Fromknecht, Dragos Velicanu, and Sophia Yakoubov. CertCoin: A NameCoin Based Decentralized Authentication System. 2014. URL: https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf (дата обращения: 18.11.2022).

REFERENCES:

[1] Gartner Expert Glossary. 2022. URL: https://www.gartner.com/en/information-technology/glossary/internet-of-things (accessed: 18.11.2022).
[2] Malik N. et al. A comprehensive review of blockchain applications in industrial Internet of Things and supply chain systems. Applied Stochastic Models in Business and Industry. 2021. DOI: https://doi.org/10.1002/asmb.2621.
[3] The ecosystem of the industrial Internet of Russia. Scientific research. RAEK. Rostelecom. 2017. URL: https://raec.ru/activity/analytics/9847 (accessed: 18.11.2022) (in Russian).
[4] Mamdouh M. et al. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. Computers & Security. 2021, vol. 111, p. 102491. DOI: https://doi.org/10.1016/j.cose.2021.102491.
[5] Zhao Q. et al. Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. Information Processing & Management. 2020, vol. 57, no. 6, p. 102355. DOI: https://doi.org/10.1016/j.ipm.2020.102355.
[6] IoT Barometr MTS. 2021. URL: http://i.content-review.com/s/2b3d9e83b5d522145afd58b0909c1078.pdf (accessed: 18.11.2022) (in Russian).
[7] Yang K., Blaauw D. and Sylvester D. Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey. IEEE Micro, vol. 37, no. 6, p. 72–89, November/December 2017. DOI: https://doi.org/10.1109/MM.2017.4241357.
[8] Capellupo M., Liranzo J., Bhuiyan M.Z.A., Hayajneh T., Wang G. Security and Attack Vector Analysis of IoT Devices. In: Wang, G., Atiquzzaman, M., Yan, Z., Choo, KK. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science(). Springer, Cham. 2017, vol 10658, p. 593–606. DOI: https://doi.org/10.1007/978-3-319-72395-2_54.
[9] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. 2015. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets-XIV). Association for Computing Machinery, New York, NY, USA, Article 5, 1–7.DOI: https://doi.org/10.1145/2834050.2834095.
[10] Ulf Lindqvist and Peter G. Neumann. 2017. The future of the internet of things. Commun. ACM 60, 2 (February 2017), p. 26–30. DOI: https://doi.org/10.1145/3029589.
[11] Marzano A. et al. The Evolution of Bashlite and Mirai IoT Botnets. IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil. 2018, p. 00813–00818. DOI: https://doi.org/10.1109/ISCC.2018.8538636.
[12] Manos Antonakakis et al. Understanding the Mirai botnet. 26th USENIX Security Symposium August 16–18, 2017. Vancouver, BC, Canada. 2017, p. 1093–1110. URL: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf (accessed: 18.11.2022).
[13] Serror M., Hack S., Henze M., Schuba M. and Wehrle K. Challenges and Opportunities in Securing the Industrial Internet of Things. IEEE Transactions on Industrial Informatics. May 2021, vol. 17, no. 5, p. 2985–2996. DOI: https://doi.org/10.1109/TII.2020.3023507.

[14] Liu J., Xiao Y. and Chen C. L. P. Authentication and Access Control in the Internet of Things. 32nd International Conference on Distributed Computing Systems Workshops, Macau, China. 2012, p. 588–592. DOI: https://doi.org/10.1109/ICDCSW.2012.23.

[15] Babar S., Mahalle P., Stango A., Prasa N., Prasad, R. Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In: Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D. (eds) Recent Trends in Network Security and Applications. CNSA 2010. Communications in Computer and Information Science. Springer, Berlin, Heidelberg. Vol. 89, p. 420–429. DOI: https://doi.org/10.1007/978-3-642-14478-3_422010.

[16] Saifullah A., Xu Y., Lu C. and Chen Y. Real-Time Scheduling for WirelessHART Networks. 31st IEEE Real-Time Systems Symposium, San Diego, CA, USA. 2010, p. 150–159. DOI: https://doi.org/10.1109/RTSS.2010.41.

[17] Dirgantoro K.P., Nwadiugwu W.P., Lee J.M., Kim D.S. Dual fieldbus industrial IoT networks using edge server architecture. Manuf. Lett. 2020, 24, p. 108–112. DOI: https://doi.org/10.1016/j.mfglet.2020.04.006.

[18] Devan P., Hussin F.A., Ibrahim R., Bingi K., Khanday F.A. A Survey on the Application of WirelessHART for Industrial Process Monitoring and Control. Sensors vol. 21, 2021. DOI: https://doi.org/10.3390/s21154951.

[19] Sisinni E., Saifullah A., Han S., Jennehag U. and Gidlund M. Industrial Internet of Things: Challenges, Opportunities, and Directions. IEEE Transactions on Industrial Informatics. Nov. 2018, vol. 14, no. 11, p. 4724–4734. DOI: https://doi.org/10.1109/TII.2018.2852491.

[20] Jayalaxmi P., Saha R., Kumar G., Kumar N. and Kim T.-H. A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges. IEEE Access. 2021, vol. 9, p. 25344–25359. DOI: https://doi.org/10.1109/ACCESS.2021.3057766.

[21] Panchal A.C., Khadse V.M. and Mahalle P.N. Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India. 2018, p. 124–130. DOI: https://doi.org/10.1109/GCWCN.2018.8668630.

[22] Pal S., Jadidi Z. Analysis of Security Issues and Countermeasures for the Industrial Internet of Things. Applied Sciences. 2021, vol.11(20). DOI: https://doi.org/10.3390/app11209393.

[23] Pal S., Hitchens M. and Varadharajan V. Modeling Identity for the Internet of Things: Survey, Classification and Trends. 12th International Conference on Sensing Technology (ICST), Limerick, Ireland. 2018, p. 45–51. DOI: https://doi.org/10.1109/ICSensT.2018.8603595.

[24] Mahalle P., Babar S., Prasad N.R., Prasad R. Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges. In: Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D. (eds) Recent Trends in Network Security and Applications. CNSA 2010. Communications in Computer and Information Science. Springer, Berlin, Heidelberg. Vol. 89, p. 430–439. DOI: https://doi.org/10.1007/978-3-642-14478-3_432010.

[25] Finogeev A. Routing and data protection in wireless sensor networks. Lambert Academic Publishing, 2016. – 96 p. URL: https://www.lap-publishing.com/catalog/details/store/ru/book/978-3-659-91987-9/маршрутизация-и-защита-данных-в-беспроводных-сенсорных-сетях?locale=ru (accessed: 18.11.2022) (in Russian).

[26] Kara M. and Furat M. Client-Server Based Authentication Against MITM Attack via Fast Communication for IIoT Devices. Balkan Journal of Electrical and Computer Engineering. 2018, vol. 6, no. 2, p. 88–93. DOI: https://doi.org/10.17694/bajece.419546.

[27] Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Network. 2015, vol. 76, p. 146–164. DOI: https://doi.org/10.1016/j.comnet.2014.11.008.

[28] Ho G., Leung D., Mishra P., Hosseini A., Song D., Wagner D. Smart Locks: Lessons for Securing Commodity Internet of Things Devices. In Proceedings of the 11th Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–3 June 2016, p. 461–472. DOI: https://doi.org/10.1145/2897845.2897886.

[29] Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu. Authentication Protocols for Internet of Things: A Comprehensive Survey. Security and Communication Networks. Hindawi. 2017.URL: https://www.researchgate.net/publication/311808641_Authentication_Protocols_for_Internet_of_Things_A_Comprehensive_Survey (accessed: 18.11.2022).

[30] Lai C., Lu R., Zheng D., Li H., and Sherman X. GLARM: group-based lightweight authentication scheme for resourceconstrained machine to machine communications. Computer Networks. 2016, vol. 99, p. 66–81.

[31] Chan A.C.-F. and Zhou J. Cyber–Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem. IEEE Journal on Selected Areas in Communications. July 2014, vol. 32, no. 7, p. 1509–1517. DOI: https://doi.org/10.1109/JSAC.2014.2332121.

[32] Chim T.W., Yiu S.M., Hui L.C.K. and Li V.O.K. PASS: Privacy-preserving authentication scheme for smart grid network. IEEE 2nd International Conference on Smart Grid Communications, SmartGridComm. 2011, p. 196–201. DOI: https://doi.org/10.1109/SmartGridComm.2011.6102316.
[33] Chang C.-C. and Le H.-D. A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks. IEEE Transactions on Wireless Communications. 2016, vol. 15, no. 1, p. 357–366. DOI: https://doi.org/10.1109/TWC.2015.2473165.
[34] Merkle tree. EU General Data Protection Regulation. 2020. URL: https://en.bitcoinwiki.org/wiki/Merkle_tree (accessed: 18.11.2022).
[35] Marko Vukolić. Rethinking Permissioned Blockchains. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC '17). Association for Computing Machinery, New York, NY, USA. 2017, p. 3–7. DOI: https://doi.org/10.1145/3055518.3055526.
[36] Ethereum Homestead Documentation. Online. Ethereum community. 2016. URL: http://www.ethdocs.org/en/latest/index.html (accessed: 18.11.2022).
[37] Arachchige P.C.M., Bertok P., Khalil I., Liu D., Camtepe S. and Atiquzzaman M. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. IEEE Transactions on Industrial Informatics. Sept. 2020, vol. 16, no. 9, p. 6092–6102. DOI: https://doi.org/10.1109/TII.2020.2974555.
[38] Hammi M.T., Bellot P. and Serhrouchni A. BCTrust: A decentralized authentication blockchain-based mechanism. IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain. 2018, p. 1–6. DOI: https://doi.org/10.1109/WCNC.2018.8376948.
[39] Johnson D., Menezes A. & Vanstone S. The Elliptic Curve Digital Signature Algorithm (ECDSA). IJIS 1, 36–63 (2001). DOI: https://doi.org/10.1007/s102070100002.
[40] Conner Fromknecht, Dragos Velicanu, and Sophia Yakoubov. CertCoin: A NameCoin Based Decentralized Authentication System. 2014. URL: https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf (accessed: 18.11.2022).

Поступила в редакцию – 18 ноября 2022 г. Окончательный вариант – 09 февраля 2022 г.
Received – November 18, 2022. The final version – February 09, 2022.