DOI 10.36622/VSTU.2022.25.2.007
УДК 004.8 : 04.077

КОМПЛЕКСНЫЙ АНАЛИЗ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.А. Ермаков, А.А. Болгов, Ю.А. Гусарева

В работе проводится комплексный анализ систем Интернета вещей с точки зрения их многоуровневой архитектуры, а также отмечены их ключевые характеристики и основные области и виды применения. Детально анализируются этапы создания и развития неоднородных сетей Интернета вещей. Проведен анализ статистики и прогнозов развития предмета исследования. Приведено описание соответствующих уровней модели взаимодействия открытых систем применительно к системам Интернета вещей. Сформирован набор общих характеристик, а также отличительных особенностей для систем Интернета вещей. Проанализированы наиболее распространённые области применения устройств Интернета вещей. Сформированы требования к безопасности на каждом уровне архитектуры систем, построенных на базе Интернета вещей. Проведен детальный анализ актуальных для решения проблем в области обеспечения информационной безопасности систем Интернета вещей.

Ключевые слова: интернет вещей, неоднородность, сеть, конфиденциальность, аутентификация, целостность, доступность.

Введение

Интернет вещей представляет собой универсальную технологию, которая позволяет всем объектам (вещам), находящимся в сфере деятельности человека, быть подключенными к Интернету с возможностью соединения друг с другом без непосредственного участия человека в управлении ими. Интернет вещей включает в себя множество устройств, которые могут быть подключены, как к проводным сетям, так и к беспроводным. Эти объекты имеют уникальную схему адресации, которая позволяет им взаимодействовать друг с другом для создания новых приложений и услуг, таких как «умные дома», «умный транспорт», «умные автомобили», «умные сети», «умные города», «интеллектуальное управление дорожным движением» и т. д., которые призваны улучшить качество предоставляемых услуг.

Концепцию Интернета вещей нельзя назвать новой, поскольку на текущий момент она уже прошла несколько этапов развития. Этапом зарождения принято считать 1982 год, когда в университете Карнеги-Меллона был запатентован бытовой автомат с напитками, подключенный к APRANET, способный передавать информацию о температуре товаров внутри. Основная идея заключалась в том, чтобы подсчитывать количество товара в каждом ряду и время, которое они находятся внутри аппарата. Если товар находился в автомате дольше порогового времени, то он помечался как «холодный». Этот эксперимент вдохновил многих изобретателей по всему миру на создание подобных собственных устройств, подключенных к сети [1].

Следующим этапом развития считается начало 1990-х годов, и связано патентом на технологию сверхвысокочастотной радиочастотной идентификации, которая обеспечивает высокую скорость передачи данных и работу на больших расстояниях. Несмотря на успешно проведенные эксперименты, эта технология так и не получила коммерческого применения, и патент вскоре был внедрен в сфере обработки штрих-кодов, а впоследствии для создания множества других приложений. Однако из-за высокой стоимости и низких объемов продаж данная технология не нашла широкого распространения [2].

Следующим этапом развития является 1999 год, когда в Центре автоматической идентификации Массачусетского технологического института (MIT)

применили технологию RFID для объединения разнородных объектов в единую систему. RFID-метки применялись для отслеживания продуктов в цепочке поставок. Идея состояла в том, чтобы использовать серийный номер RFID-метки для отслеживания продуктов, чтобы уменьшить затраты, поскольку производство более сложных чипов с большим объемом памяти обходится дороже. Данные, полученные с RFID-меток, хранились в базе данных, доступ к которой можно было получить через Интернет.

Единой позиции о первом использовании термина Интернета вещей на сегодняшний день нет. Ряд зарубежных источников утверждают, что впервые термин введен в 1999 году Кевином Эштоном [3], в то время как другие утверждают, что Нил Гершенфельд впервые упомянул идею Интернета вещей в своей книге. Тем не менее, термин Интернет вещей был официально представлен Международным союзом электросвязи (МСЭ) в 2008 году [4].

В последствии понятие Интернета вещей было определено многими исследователями. Однако определение, представленное МСЭ в 2012 году, является наиболее устоявшимся. В соответствии с этим определением под Интернетом вещей понимается глобальная инфраструктура для информационного сообщества, обеспечивающая предоставление передовых услуг путем объединения (физических и виртуальных) объектов на основе существующих и развивающихся совместимых информационных и телекоммуникационных технологий [5]. Кроме того, в [6] предложено одно из наиболее наглядных представлений системы Интернета вещей, которое представлено на рис. 1. В соответствии с представленной концепцией Интернет вещей позволяет людям и устройствам быть связанными в любой момент времени, в любом месте, при этом используя любую доступную технологию связи или сервис.

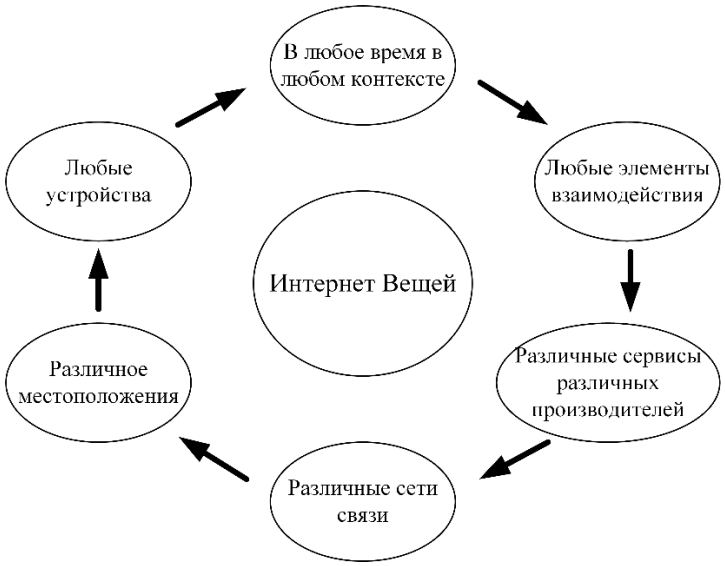

Рис. 1. Иллюстрация связи различных устройств Интернета вещей

Расширение Интернета вещей

Общемировой тенденцией на текущем этапе развития технологии является стремление к обеспечению подключения и реализации обмена данными через интернет различных конечных устройств. Количество таких устройств уже подключенных к сети непрерывно растет [7]. Благодаря неограниченным возможностям и преимуществам системы Интернета вещей, регулярно создаются новые приложения и сервисы. По данным Statista [7], ожидается, что к концу 2022 года количество устройств Интернета вещей во всем мире достигнет примерно 43 млрд., а к концу 2025 года превысит 75 млрд.

Рынок Интернета вещей растет практически экспоненциально. По данным Statista [7], суммарная выручка от внедрения технологии Интернета вещей в 2020 году составила 420,6 млрд. долларов. Ожидается, что это число значительно увеличится до 1710 миллиардов долларов к концу 2023 года.

Архитектура Интернета вещей

Комитет по архитектуре Всемирного форума Интернета вещей (IWF) выпустил эталонную модель Интернета вещей в октябре 2014 года [8]. Эта эталонная модель является основой для стандартизации и ускорения процессов развертывания применений технологии Интернета вещей в различных сферах деятельности. Эталонная модель Интернета вещей спроектирована в соответствии с принципами модели взаимодействия открытых систем, как показано на рис. 2. Модель регламентирует, на каких уровнях должны выполняться различные виды обработки данных, и позволяет различным производителям создавать совместимые друг с другом устройства Интернета вещей, что преобразует технологию из концептуальной модели в реальную и доступную для реализации систему.

Рис. 2. Уровни эталонной архитектуры Интернета вещей

Уровень 1 – это физический уровень. Он содержит физические устройства и контроллеры, которые управляют различными объектами. Эти объекты представляют собой вещи в среде Интернета вещей, которые используют различные типы устройств для сбора, отправки и получения информации. Например, датчики, которые собирают информацию об окружающей среде [9].

Уровень 2 – канальный уровень или коммуникации и подключения устройств. Этот уровень используется для соединения различных устройств Интернета вещей друг с другом с помощью коммутаторов, шлюзов, маршрутизаторов и брандмауэров.

Уровень 3 – это периферийные вычисления. Этот уровень принимает данные, поступающие с канального уровня и преобразует их в формат, подходящий для хранения и обработки на более высоком

уровне. На этом уровне компоненты обработки работают с огромным объемом данных и поэтому выполняют операции преобразования данных для уменьшения их размера.

Уровень 4 – это накопление данных. Этот уровень связан с хранением данных, поступающих с различных устройств Интернета вещей. Эти данные фильтруются и обрабатываются соответствующим вычислительным уровнем, который выполняет обработку больших объемов данных и помещает их в хранилище, чтобы они были доступны на более высоких уровнях. Различные типы данных в различных форматах и от разнородных обработчиков могут поступать с периферийного вычислительного уровня для хранения.

Уровень 5 – это уровень абстракции данных. Этот уровень объединяет и форматирует хранимые данные управляемым и эффективным способом так, чтобы сделать их доступными для различных приложений.

Уровень 6 – это прикладной уровень. Этот уровень связан с интерпретацией информации для различных приложений Интернета вещей. Этот уровень охватывает множество приложений, которые используют входные данные или управляют множеством устройств [8].

Уровень 7 – уровень взаимодействия и процессов. Этот уровень определяет объекты и субъекты, которым требуется взаимодействовать, чтобы сделать систему Интернета вещей более полезной.

Основные характеристики Интернета вещей

Интернет вещей представляет собой перспективную технологию, направленную на повышение качества предоставляемых услуг путем создания новых приложений и цифровых сервисов, облегчающих повседневные процессы. Существует набор общих для всех устройств класса Интернета вещей, свойств который включает в себя:

- **Масштаб.** количество устройств Интернета вещей может достигать миллиарда. Это крупномасштабная сеть, которой необходимо управлять для того чтобы устройства могли взаимодействовать друг с другом. Кроме того, эта широкомасштабная сеть генерирует огромное количество данных, которые создают глобальную проблему, связанную с их интерпретацией и анализом.
- **Интеллект.** Сочетание сложных программных алгоритмов с аппаратными средствами позволяют устройствам Интернета вещей решать интеллектуальные задачи, например, принимать решения в зависимости от ситуации и осуществлять интеллектуальное взаимодействие с другими устройствами сети.
- **Восприятие.** Датчики являются основой системы Интернета вещей. Они используются для восприятия изменений в окружающей среде и генерации данных, которые описывают ее состояние. Датчики применяющие различные технологии измерений обеспечивают возможность представления реальной обстановки окружающей среды, для повышения осведомленности лиц, принимающих решения.
- **Динамичность.** Технология Интернета вещей позволяет практически без ограничений по количеству устройств в сети объединять различные объекты, что делает систему динамической по топологии. Также, устройства Интернета вещей могут функционировать и конфигурироваться динамически в зависимости от внешних условий.
- **Неоднородность.** Сеть Интернета вещей может включать в себя устройства с разнородными функциями, использующими различные операционные системы, аппаратные платформы, протоколы связи и прочее. Эта неоднородность создает существенные затруднения в управлении такой системой.
- **Автономность.** Большинство устройств Интернета вещей проектируются автономными и в малых габаритах, что ограничивает возможности по хранению данных и вычислительной мощности.
- **Совместимость.** Одним из основных свойств систем Интернета вещей является возможность подключения различных устройств с различными характеристиками и использованием для создания приложений и

сервисов интегрированной информации от них.

- **Самоконфигурируемость.**

Устройства должны быть сконфигурированы для выполнения определенной задачи. Но в устройствах Интернета вещей есть возможность самоконфигурации, которая позволяет им работать без вмешательства человека. Например, эти устройства могут самостоятельно обновляться на новейшее программное обеспечение без участия пользователя [8].

- **Уникальная идентификация.** В сети Интернета вещей каждый объект Интернета вещей идентифицируется и распознается с помощью уникального идентификатора. Эти идентификаторы предоставляются производителями устройств, для решения задач по их обновлению, сбору необходимой информации, регистрации их статуса, а также удаленного управления.
- **Контекст.** В среде Интернета вещей существует множество датчиков, которые обрабатывают информацию об окружающей среде, собирают и хранят необходимую информацию. Эти датчики могут принимать решения, основанные на собранных данных, которые делают их контекстно-зависимыми.

Приложения технологии Интернета вещей. Способность систем Интернета вещей соединять различные физические и виртуальные объекты в единую систему, создает новые сервисы и приложения, которые могут быть применены в различных сферах жизни. Самые распространённые на сегодняшний день области, в которых используется Интернет вещей – это электронное здравоохранение, сельское хозяйство, сети поставок и логистики, умный дома, умные города, умные сети, умные автомобили, а также носимые устройства.

Электронное здравоохранение. Технология Интернета вещей успешно продемонстрировала, что может обеспечивать ряд преимуществ в сфере здравоохранения, создавая новые услуги для пациентов и поддерживая инновации в этой области. Существует множество носимых устройств, разработанных для мониторинга и отслеживания состояния здоровья пациента. Также эти устройства могут использоваться для отправки предупреждающих сообщений при ухудшении контролируемых показателей. Кроме того, само устройство может рекомендовать пациенту лечение. Если по какой-то причине здоровье пациента ухудшается, в перспективе устройство могло бы отправлять срочные сообщения в больницу или машины скорой помощи для немедленной госпитализации [10].

Умное сельское хозяйство. Благодаря наличию множества датчиков в среде Интернета вещей, фермеры могут использовать собранные данные для обеспечения большей рентабельности производства. Кроме того, для повышения производительности, с помощью датчиков могут измеряться такие параметры почвы, как влажность, уровень соли и температура. Также благодаря применению беспроводных технологий, таких как геопозиционирование и дистанционное зондирование, появляется возможность быстрого и эффективного сбора соответствующей информации о почве, что позволяет автоматизировать процессы для увеличения производительности сельскохозяйственного производства [11]. В последнее время наблюдается значительный рост внедрения устройств Интернета вещей в сельском хозяйстве. Прогнозируется, что к концу 2022 года количество устройств Интернета вещей в сельском хозяйстве достигнет около 75 миллионов [10].

Сети поставок и логистики. Используя RFID и NFC, существует возможность отслеживать товары от производителя до места реализации. RFID-метки, размещаемые на товарах, используются для уникальной идентификации каждого товара, сбора соответствующей информации и передачи ее в режиме реального времени вместе с информацией о местоположении. Эти метки используются для передачи сообщений, которые точно описывают тип товара, размеры и варианты упаковки, а также температуру и влажность окружающей среды. Кроме того, автоматизированный сбор данных позволяет в режиме реального времени отслеживать количество товаров, что в свою очередь позволяет избежать

ручного подсчета и исключить человеческий фактор. Интернет вещей способен совершить революцию в сети поставок, как с точки зрения операционной эффективности, так и с точки зрения возможности получения прибыли [12].

Умный дом. Умный дом – одно из самых популярных приложений технологии Интернета вещей. Благодаря датчикам и технологиям управления, а также беспроводным сенсорным сетям (WSN) создается возможность подключения различных домашних устройств для решений бытовых задач. Умные дома обеспечивают большую энергоэффективность, при которой умные устройства можно настроить на автоматический запуск, а затем отключение по завершении выполнения целевого назначения [13].

Умный город. Умный город строится на основе устройств Интернета вещей, таких как счетчики, датчики света, датчики мониторинга загрязненности воздуха и т.п., которые используются для мониторинга и сбора информации об окружающей среде города для предоставления актуальных данных для улучшения качества предоставления коммунальных услуг и городской инфраструктуры. Решения на базе Интернета вещей используются в различных инфраструктурных проектах современных городов, таких как уличное освещение, утилизация мусора, умная парковка и управление дорожным движением [14].

Для интеллектуальных транспортных систем, собранная датчиками информация о дорожном движении, может быть отправлена на телефоны граждан для информирования о загруженности магистралей в режиме реального времени, что в свою очередь может помочь водителям выбирать пути объезда и планировать маршрут. Для решения задач утилизации и сортировки мусора, датчики Интернета вещей могут быть установлены в мусорных баках для отправки сообщений коммунальным службам об их наполненности [15].

Умные электросети. Датчики Интернета вещей могут использоваться для сбора соответствующей информации о потреблении электроэнергии в домах для ее более эффективного перераспределения и оптимизации оплаты. Например, возможна реализация сервиса по выбору оптимального тарифа оплаты электроэнергии в зависимости от статистики потребления. Кроме того, информация с датчиков Интернета вещей может быть использована для предоставления потребителям всей необходимой информации о различных поставщиках электроэнергии в автоматизированном режиме, чтобы потребитель мог выбрать наилучшего.

Одним из основных приложений умной электросети являются умные счетчики, которые собирают, записывают и анализируют электропотребление в разное время суток. Эта информация может использоваться потребителями для регулирования энергопотребления и оптимизации затрат [14].

Автомобильная сеть. В настоящее время идет активное внедрение умных или подключенных к сети автомобилей. Автомобили данного типа могут получать доступ к сети Интернет и обмениваться различными данными с другими устройствами. Количество автомобилей, оснащенных таким оборудованием, непрерывно увеличивается, что создает благоприятные условия для разработки соответствующих сервисов для умных автомобилей [16]. Автомобиль с доступом в сеть имеет ряд потенциальных преимуществ по сравнению с автономными автомобилями. Одним из таких преимуществ является возможность уменьшения числа дорожно-транспортных происшествий и минимизации человеческого фактора за счет возможности дистанционного или автоматизированного управления автомобилем. Беспилотные автомобили могут сэкономить время и снизить стресс от вождения. Многие автопроизводители утверждают, что планируют выпуск полностью автономных автомобилей к концу 2023 года [17].

Носимые устройства. Носимые устройства вызывают огромный интерес на рынках во всем мире. Многие компании производят такие устройства большими партиями для удовлетворения повышенного спроса. По данным Statista [7], ожидается, что

к концу 2022 года количество подключенных носимых устройств достигнет 830 миллиардов. Носимые устройства оснащены датчиками и могут подключаться к сети Интернет для обмена данными. Эти датчики собирают данные о пользователе, которые затем обрабатываются для извлечения значимой информации. Наиболее распространенные носимые устройства используются в фитнесе, здравоохранении и развлечениях [18].

Безопасность Интернета вещей

Обеспечение безопасности – одна из основных задач, решение которой способно обеспечить успешное внедрения различных приложений технологии Интернета вещей. Ключевая ценность систем на базе технологии Интернета вещей заключается в возможности объединения подсистем различного масштаба в единую сеть, позволяя им взаимодействовать друг с другом через Интернет. В этом контексте защита передачи данных и соединений устройств Интернета вещей должна быть одним из основных приоритетов для анализа [19].

Интернет вещей по своей сути представляет собой динамическую систему, в которой каждый элемент с низким уровнем защищенности создать угрозу безопасности и устойчивости всей системы, поскольку устройства Интернета вещей сильно взаимосвязаны. Простота подключения и доступ к множеству устройств создает предпосылки для серьезных рисков безопасности, особенно в крупномасштабных распределенных сетях разнородных устройств. Также серьезной уязвимостью в безопасности является возможность устройств Интернета вещей подключаться к другим устройствам без какого-либо протокола аутентификации, запроса разрешения или даже уведомления их владельцев.

Управление рисками безопасности в контексте Интернета вещей должно быть важнейшим приоритетом для дальнейшего развития и внедрений приложений технологии Интернета вещей. Пользователи должны быть уверены в безопасности своих устройств и приложений на базе технологии Интернета вещей [20].

Требования к безопасности Интернета вещей

Снижение рисков безопасности системы Интернета вещей может быть обеспечено за счет применения классических методов и подходов обеспечения свойств конфиденциальности, целостности и доступности информации.

Для обеспечения конфиденциальности – обмен сообщениями между отправителем и получателем должен быть защищен от любого не аутентифицированного пользователя [21]. Для системы Интернета вещей конфиденциальность должна обеспечиваться не только внутри сети подключения, но и при передаче сообщений между различными устройствами Интернета вещей.

Для обеспечения целостности данных циркулирующих в системе Интернета вещей соответствующая проверка может выполняться на каждом узле, участвующем в обмене между отправителем и получателем.

Обеспечение свойства доступности необходимо для выполнения требований к качеству услуг, предоставляемых устройствами Интернета вещей или коммуникационными сетями [22].

Помимо требований по обеспечению основных свойств информации необходимых для систем Интернета вещей, существуют и другие требования безопасности, которые должны быть обеспечены на каждом уровне архитектуры сети Интернета вещей, что показано на рис. 3. Проблема аутентификации – одна из ключевых проблем безопасности на физическом уровне Интернета вещей, позволяющая исключить несанкционированный доступ к элементам и обеспечить безопасность канала связи между элементами Интернета вещей от различных типов атак. Одним из вариантов решения является применение шифрования передаваемых данных с помощью нересурсоемкого алгоритма, особенно для автономных устройств Интернета вещей с ограниченными аппаратными возможностями [23].

Рис. 3. Требования к безопасности на каждом уровне архитектуры Интернета вещей

Для канального уровня необходимы меры по обеспечению безопасности каналов связи такие как, идентификация и аутентификация для предотвращения доступа к не разрешенным узлам. Кроме того, на этом уровне распространены атаки типа распределенного отказа в обслуживании (DDoS), поэтому необходима разработка мер защиты от данного типа атак.

Для уровней абстракции данных, накопления и периферийных вычислений требуется разработка множества средств обеспечения безопасности приложений для защиты данных, использующих облачные сервисы хранения и вычислений. Помимо современных антивирусных программ, для уровней приложений и уровня взаимодействия необходима разработка и внедрение надежных алгоритмов шифрования, аутентификации для обеспечения конфиденциальности данных пользователей. Кроме того, разграничение прав доступа и менеджмент паролей имеют важное значение для информационной безопасности на этом уровне [23].

Риски безопасности

В виду относительной новизны технологии, риски безопасность по-прежнему остаются основным фактором, ограничивающим эффективное развитие систем Интернета вещей. Существует ряд рисков в области безопасности, которые требуют снижения в интересах повышения доверия к технологии и увеличения темпов внедрения устройств Интернета вещей.

Ограниченные аппаратные ресурсы. Большинство устройств Интернета вещей имеют ограниченные возможности по обработке и хранению данных в виду их малых размеров и простоты выполняемых ими функций, что позволяет им работать автономно с низким энергопотреблением. Следовательно, сложные алгоритмы обеспечения безопасности не подходят для этих устройств, поскольку они не способны выполнять сложные вычислительные

операции в режиме реального времени. Вместо этого они могут использовать только вычислительно эффективные алгоритмы обеспечения безопасности [24].

Большие данные. Системы Интернета вещей включают в себя, как правило, большое количество устройств, которые генерируют большой объем данных. Эти данные различны по своей структуре и формату и могут поступать в режиме реального времени. Объем, скорость обработки и разнообразие характеристик больших данных вызывают проблемы, связанные с операциями хранения и анализа. Системы Интернета вещей считаются одним из основных источников больших данных. Хоть облачные хранилища и представляют собой хорошее решение для хранения данных в течении длительного времени, но при этом обработка такого огромного объема данных является серьезной проблемой, поскольку суммарная производительность различных приложений в значительной степени зависит от производительности службы управления данными. Более того, одной из главных проблем большого объема данных является целостность данных. Сложность обеспечения безопасности и целостности больших объемов данных растет по мере увеличения числа источников данных, поэтому необходимо разрабатывать дополнительные механизмы по обеспечению безопасности [25].

Безопасность телекоммуникаций. Обеспечение безопасности отдельных устройств в сети Интернета вещей недостаточно для обеспечения безопасности системы в целом, поэтому дополнительно необходимо анализировать риски безопасности связанные с каналами связи, соединяющими различные элементы системы, такие как конечные устройства Интернета вещей и облачные сервисы, которые должны быть защищен от различных типов атак. Большинство устройств Интернета вещей передают свои данные в текстовом формате без шифрования, что делает их легкой мишенью для различных сетевых атак типа анализ трафика. Очевидным решением является применение надлежащего метода шифрования [26]. Кроме того, использование изолированных сегментов сетей может повысить безопасность за счет изоляции устройств и создания VPN-туннелей.

Устойчивость системы. Риски нарушения устойчивости системы являются важным аспектом, требующим разработки метода их снижения. Устойчивость относится к способности системы реагировать на непредсказуемые ситуации без регресса [27]. Следовательно, если устройство Интернета вещей скомпрометировано, система должна быть в состоянии защитить остальные сетевые узлы. Зачастую, если есть заражённое устройство, его сброс или замена помогает решить проблему. При этом основной задачей для решения данной проблемы является разработка принципов и протоколов построения сетей устройств Интернета вещей, которые способны выполнять выявление скомпрометированных устройств и изолировать их для поддержания общей безопасности системы, что является сложно формализуемой задачей. Таким образом, существует необходимость в разработке эффективной методики для изоляции скомпрометированных устройств [27].

Цифровая криминалистика. Благодаря большому числу устройств, системы Интернета вещей становятся важным источником доказательств, который может предоставить важную информацию для проведения следственных мероприятий на протяжении всего процесса расследования, однако и это сопряжено с рядом проблем. Например, важно определить, источник сгенерировавший данные и его местоположение, что затруднительно в контексте специфики технологии построения сетей Интернета вещей. Также, поскольку устройства Интернета вещей имеют ограниченный объем памяти, данные, отправляются в облачные хранилища, где в виду различных задержек нарушается временной порядок сохранения данных. Помимо этого, динамичность и неоднородность систем Интернета вещей проявляется в интеграции таких различных источников данных как компьютеры, планшеты, мобильные устройства, облачные

хранилища, различные типы датчиков и меток RFID. Соответственно проблема анализа больших данных помимо неоспоримых преимуществ может привести к усложнению процесса расследования [28].

Гетерогенность. Система Интернета вещей, своей природе представляет собой гетерогенную систему. Она включает в себя различные устройства с различными аппаратными и программными возможностями. Эти устройства были созданы разными производителями с элементарными алгоритмами безопасности, что делает их уязвимыми для злоумышленников. Кроме того, если эти устройства используют программное обеспечение с открытым исходным кодом, то обновления их встроенного ПО будет затруднено [29].

Аутентификация и контроль доступа. Обеспечение эффективного механизма авторизации и контроля доступа для системы Интернета вещей является одним из основных принципов обеспечения безопасности системы. Устройства Интернета вещей должны получать доступ к службам или приложениям только после правильного предоставления своих идентификационных данных. Однако существует множество уязвимостей связанных с аутентификацией устройств, которые предоставляют злоумышленникам возможности для несанкционированного доступа, что в свою очередь позволяет нарушать целостность данных или самих устройств. Известными мерами обеспечения безопасности в устройствах Интернета вещей являются двухфакторная аутентификация и принудительное использование надежных паролей [30].

Заключение

В данной статье проведен комплексный обзор систем, построенных на базе технологии Интернета вещей, основанный на анализе с точки зрения ее многоуровневой архитектуры. В результате обзора различных источников, посвященных тематике выбранного исследования, были выделены и описаны основные свойства и приложения систем Интернета вещей. Также в ходе анализа были выделены основные требования в контексте обеспечения безопасности на каждом уровне архитектуры систем Интернета вещей. В результате было выявлено, что в системах Интернета вещей, как и в других технологиях, находящихся на ранних стадиях развития, вопросы обеспечения безопасности являются серьезной проблемой, стоящей на пути эффективного развития.

Основным научным результатом данной статьи является идентификация и описание основных уязвимостей безопасности в системах Интернета вещей. Ключевыми причинами существования таких уязвимостей является принципиальная неоднородность систем, большое количество генерируемых, агрегируемых и обрабатываемых данных, надежность и безопасность применяемых протоколов связи, а также ограниченные аппаратные ресурсы, связанные с малыми размерами и автономностью датчиков и устройств исследуемых систем.

Список литературы

1. Farooq M. U. Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). / M. U. Farooq, M. A. Waseem // International Journal of Computer Applications, 2015, 113(1). P. 1–7.

2. Roberto M. Towards a definition of the Internet of Things (IoT). / M. Roberto, B. Abyi, R. Domenico // IEEE Internet of Things, 2015, P. 1–86.

3. Ashton K. That Internet of Things. // Thing. RFID Journal, 2009. URL: http://www.rfidjournal.com/articles/pdf?4986 (дата обращения: 19.10.2021).

4. ITU. The Internet of Things. ITU Internet Report 2005. / URL: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf (дата обращения: 19.10.2021).

5. ITU-T. Overview of the Internet of things. Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks, 06/2012. URL: https://www.itu.int/rec/T-REC-Y.2060-201206-I (дата обращения: 19.10.2021).

6. Guillemin P. Internet of Things Strategic Research Roadmap / P. Guillemin, P. Friess // 2009. URL: https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2430372/SINTEF%2BS13363.pdf (дата обращения: 21.10.2021).

7. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025, 2018. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (дата обращения: 21.10.2021).

8. Stallings W. The Internet of Things: Network and Security Architecture. // The Internet Protocol Journal, 2015, No. 18(4), P. 2–24.

9. Cisco. The Internet of Things Reference Model. White Paper, 2014, pp. 1–12.

10. Akkaş M. A., Sokullu R. An IoT-based greenhouse monitoring system with Micaz motes. // International Workshop on IoT, M2M and Healthcare (IMH 2017), 2017, No. 113, P. 603–608.

11. Krishna K. L., Silver O., Malende W. F., Anuradha K. Internet of Things application for implementation of smart agriculture system. // International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, No. 25(15), P. 54–59.

12. Guo Z., Zhang, Z., Li W. Establishment of intelligent identification management platform in railway logistics system by means of the Internet of Things. // Procedia Engineering, 2012, No. 29, P. 726–730.

13. Pătru I. I., Carabaş M., Bărbulescu M., Gheorghe L. Smart home IoT system. // Proceedings of 15th International Conference of Networking in Education and Research, 2016, P. 365–370.

14. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities. // IEEE Internet of Things Journal, 2014, No. 1(1), P. 22–32.

15. Khatoun R., Zeadally, S. Cybersecurity and privacy solutions in smart cities. // IEEE Communications Magazine, 2017, No. 55(3), P. 51–59.

16. Kalmeshwar M., Prasad N. Internet of Things: Architecture, Issues and Applications. // International Journal of Engineering Research and Applications, 2017, No. 07(06), P. 85–88.

17. Xu D. Specification and analysis of attribute-based access control policies: An overview. / D. Xu, Y. Zhang // Proceedings of 8th International Conference on Software Security and Reliability (SERE-C 2014), 2014, P. 41–49.

18. Cirani S. Wearable Computing for the Internet of Things. / S. Cirani, M. Picone // IEEE Computer Society, 2015, P. 35–41.

19. Elkhodr M. The Internet of Things: Vision & challenges. / M. Elkhodr, S. Shahrestani, H. Cheung // Proceedings of IEEE. 2013. Tencon - Spring Conference. P. 218–222.

20. Iqbal M. A. A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches. / M. A. Iqbal, O. G. Olaleye, M. A. Bayoumi // Global Journal of Computer Science and Technology: E Network, Web & Security, 2016, No. 16(7), P. 1-9.

21. Maple C. Security and privacy in the internet of things. // Journal of Cyber Policy, 2017, No. 2(2), P. 155-184.

22. Yu Y. Goal Modelling for Security Problem Matching and Pattern Enforcement. / Y. Yu [etc.]// International Journal of Secure Software Engineering, 2016, No. 8(3), P. 42–57.

23. Suo H. Security in the internet of things: A review. / H. Suo, J. Wan, C. Zou, J. Liu // International Conference on Computer Science and Electronics Engineering (CCSEE 2012), 2012, No. 3, P. 648–651.

24. Musaddiq A. A Survey on Resource Management in IoT Operating Systems. / Musaddiq A. [etc.] //IEEE Access, 2018, No. 6, P. 8459–8482.

25. Waqas Aman. Modeling Adaptive Security in IoT Driven eHealth. In: Norwegian Information Security Conference (NISK 2013), 2013, P. 61–69.

26. Maheshwari N., Dagale H. Secure communication and firewall architecture for IoT applications. // 10th International Conference on Communication Systems and Networks (COMSNETS 2018), 2018, P. 328–335.

27. Kitchin R., Dodge M. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. // Journal of Urban Technology, 2017, P. 1–19.

28. Zia T. Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT). / T. Zia, P. Liu, W. Han // Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES ’17), 2017, P. 1–7.

29. Alur R. Systems Computing Challenges in the Internet of Things. / R. Alur [etc.] // ArXiv Preprint ArXiv:1604.02980, 2015, P. 1–15.

30. Habib K., Leister W. Context-Aware Authentication for the Internet of Things. // The Eleventh International Conference on Autonomic and Autonomous Systems Fined, 2015, P. 134–139.

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 23.05.2022

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Болгов Андрей Александрович – аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Гусарева Юлия Александровна – студентка, Воронежский государственный технический университет, e-mail: mnac@comch.ru

COMPREHENSIVE ANALYSIS OF INTERNET OF THINGS SYSTEMS TO IDENTIFY VULNERABILITIES IN THE CONTEXT OF INFORMATION SECURITY

S.A. Ermakov, A.A. Bolgov, Ju.A. Gusareva

The paper provides a comprehensive analysis of the Internet of Things systems from the point of view of their multilevel architecture, as well as their key characteristics and main areas and application. The stages of creation and development of heterogeneous Internet of Things networks are analyzed in detail. The analysis of statistics and forecasts of the development of the subject of research is carried out, the description of the corresponding levels of the open systems interaction model in relation to the Internet of Things systems is given. A set of common characteristics, as well as distinctive features for the Internet of Things systems, has been formed. The most common applications of Internet of Things devices are analyzed. Security requirements have been formed at each level of the architecture of systems built on the basis of the Internet of Things. A detailed analysis of the problems relevant to solving in the field of information security of Internet of Things systems has been carried out.

Keywords: Internet of Things, heterogeneity, network, confidentiality, authentication, integrity, availability.

Submitted 23.05.2022

Information about the authors

Sergey A. Ermakov – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

Andrey A. Bolgov – Graduate Student, Voronezh State Technical University, e-mail: mnac@comch.ru

Julia A. Gusareva –Student, Voronezh State Technical University, e-mail: mnac@comch.ru