«ИНТЕРНЕТ ВЕЩЕЙ» В ПРОМЫШЛЕННОСТИ: ОБЗОР КЛЮЧЕВЫХ ТЕХНОЛОГИЙ И ТРЕНДОВ

ЛИ ДА СЮЙ (LI DA XU), ВУ ХЕ (WU HE)
whe@odu.edu
СЯНЧАН ЛИ (SHANCANG LI)
shanchang.li@bristol.ac.uk
ПЕРЕВОД: АЛЕКСЕЙ ОСОТОВ

Для понимания развития «Интернета вещей» в промышленности в данной работе приведен обзор современных исследований в сфере IoT, ключевых технологий и основных приложений IoT в промышленности, а также перечислены текущие проблемы и определены будущие тенденции.

ВВЕДЕНИЕ

Предполагается, что «Интернет вещей» (Internet of things, IoT) предложит перспективные решения проблем по преобразованию функционирования и роли многих промышленных систем. Например, IoT уже используется для создания интеллектуальных транспортных систем, благодаря которым появляется возможность отслеживать местоположение каждого транспортного средства, вести мониторинг его передвижения, а также предсказывать его будущую дислокацию и вероятный дорожный трафик.

Термин «Интернет вещей» изначально был предложен для обозначения однозначной идентификации объектов, связанных посредством технологии радиочастотной идентификации RFID [1]. Позже он стал затрагивать гораздо больше технологий, таких как датчики, приводы, GPS- и мобильные устройства. Сегодня общепринятое определение «Интернета вещей» следующее: динамическая глобальная сетевая инфраструктура с самостоятельной настройкой возможностей на основе стандартных и совместимых протоколов связи, где физические и виртуальные «вещи» имеют идентификаторы, физические атрибуты и виртуальные персоналии, используют интеллектуальные интерфейсы и легко интегрируются в информационную сеть [2].

В частности, интеграция датчиков/приводов, RFID-меток и коммуникационных технологий служит основой для «Интернета вещей» и объясняет, как различные физические предметы и устройства вокруг нас могут быть связаны с Интернетом, а также позволяет этим объектам и устройствам взаимодействовать друг с другом для достижения общих целей [3].

Интерес к использованию технологии IoT в различных отраслях промышленности возрастает [4]. Проекты по внедрению промышленного «Интернета вещей» уже были реализованы в таких областях, как сельское хозяйство, пищевая промышленность, экологический мониторинг, видеонаблюдение и др. Между тем число публикаций про «Интернет вещей» тоже стремительно растет. Авторы провели обширный анализ литературы, изучив соответствующие статьи из пяти основных академических баз данных (IEEE Xplore, Web of Knowledge, ACM digital library, INSPEC и ScienceDirect), для того чтобы помочь исследователям понять текущее положение «Интернета вещей» в промышленности и перспективы исследований, касающихся его использования.

ПРЕДПОСЫЛКИ И ТЕКУЩИЕ ИССЛЕДОВАНИЯ IoT

«Интернет вещей» можно рассматривать в качестве глобальной сетевой инфраструктуры, состоящей из множества подключенных устройств, которые используют сенсорные, коммуникационные, сетевые и информационные технологии [5]. Основополагающей технологией для «Интернета вещей» является технология RFID, позволяющая микрочипам посредством беспроводной связи передавать считывателям идентификационную информацию. С помощью RFID-считывателей люди могут идентифицировать, отслеживать и контролировать любые объекты, автоматически подключенные с помощью RFID-меток [6]. Технология RFID широко используется в логистике, фармацевтическом производстве, розничной торговле и управлении цепочками поставок начиная еще с 1980-х гг. [7, 8]. Другая основополагающая технология для IoT — беспроводные сенсорные сети (WSN), которые в основном используют взаимодействующие интеллектуальные датчики (сенсоры) для совместной работы и мониторинга. Область их применения включает в себя мониторинг окружающей среды, медицинский мониторинг, производственный контроль, мониторинг трафика и т. д. [9], [10].

Достижения в обеих технологиях (RFID и WSN) внесли значительный вклад в развитие «Интернета вещей». Кроме того, теперь множество других технологий и устройств, таких как штрихкоды, смартфоны, социальные сети и облачные вычисления, также используется для формирования широкой сети поддержки IoT [11–16] (рис. 1).

Сегодня IoT также набирает популярность в логистике, различных отраслях промышленности, розничной торговле и фармацевтике. В связи с развитием беспроводной связи, смартфонов и датчиков сетевых технологий все больше и больше сетевых «вещей», или «умных» объ-

ектов, участвуют в IoT. В результате все эти IoT-технологии оказывают значительное влияние на новые информационные и коммуникационные технологии (ИКТ) и технологии корпоративных систем (рис. 2).

Чтобы обеспечить высокое качество услуг для конечных пользователей, в рамках «Интернета вещей» должны быть разработаны технические стандарты, спецификации, определяющие обмен информацией и ее обработку, а также связи между вещами. Успех в использовании IoT зависит от стандартизации, которая обеспечит интероперабельность, совместимость, надежность и эффективную работу в мировом масштабе [17]. Многие страны и организации заинтересованы в разработке стандартов для IoT, так как это может принести огромную экономическую выгоду в будущем. Сегодня Международный телекоммуникационный союз, Международная электротехническая комиссия, Международная организация по стандартизации, Институт инженеров электротехники и электроники, Европейский Комитет по электротехнической стандартизации, Китайский институт по электронным стандартам и Американский национальный институт стандартов занимаются разработкой различных стандартов для «Интернета вещей» [18, 19]. При этом необходимо согласовывать стандартизации различных организаций с международными стандартами, а также национальными и региональными организациями по стандартизации [20]. Благодаря созданию общепринятых стандартов разработчики и потребители смогут использовать приложения и сервисы IoT в больших масштабах при сохранении развития и расходов (на техническое обслуживание) в долгосрочной перспективе. Стандартизация технологий IoT также ускорит их распространение.

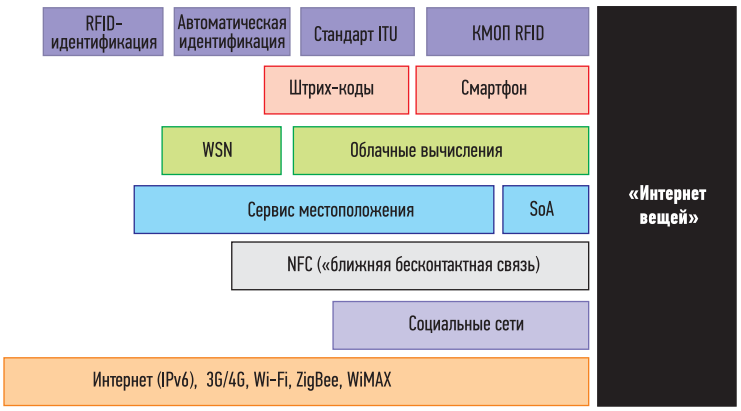

РИС. 1. ◄ Технологии, связанные с IoT

КЛЮЧЕВЫЕ ТЕХНОЛОГИИ

Технологии идентификации и отслеживания

Технологии идентификации и отслеживания, применяемые в IoT, включают системы RFID, штрихкоды и интеллектуальные датчики. Простая RFID-система состоит из RFID-считывателя и RFID-метки. Благодаря способности этой системы к выявлению и отслеживанию устройств и физических объектов она все чаще используется в промышленных отраслях, таких как логистика, управление цепями поставок, служба мониторинга здоровья [6, 43]. Другое преимущество системы RFID заключается в предоставлении точной информации в режиме реального времени о подключенных устройствах, что позволяет сократить затраты на рабочую силу, упростить бизнес-процессы, повысить точность информации об оборудовании и в итоге улучшить общую экономическую эффективность.

На данный момент развитие технологий RFID фокусируется на следующих аспектах [6, 7, 8, 43]: 1) активные RFID-системы с расширенным спектром передачи; 2) технология управления RFID-приложениями [7, 8].

Также существует много возможностей для развития RFID-приложений [44]. Например, RFID-технология может быть интегрирована с WSN для лучшего выявления «вещей» и слежения за ними в режиме реального времени. Развивающиеся беспроводные интеллектуальные сенсорные технологии,

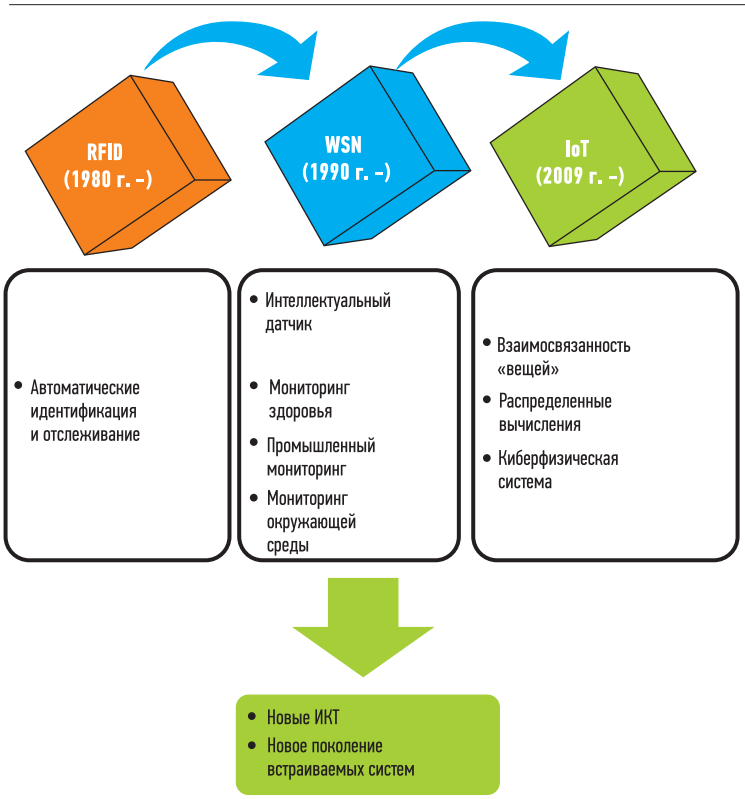

РИС. 2. ◄ Связанные с IoT технологии и их влияние на новые информационно-коммуникационные технологии (ИКТ) и на корпоративные системы

такие как электромагнитные датчики, биосенсоры, встроенные датчики, датчики тегов, независимые теги и сенсорные устройства, в дальнейшем поспособствуют внедрению и развертыванию производственных служб и приложений. Посредством интеграции данных, полученных интеллектуальными датчиками с помощью RFID, могут быть созданы более мощные приложения IoT, которые подходят для индустриальной среды.

Коммуникационные технологии в IoT

Реализация «Интернета вещей» может содержать множество электронных аппаратов, мобильных устройств и промышленного оборудования. Разным «вещам», которые можно подключить к сетевым и коммуникационным технологиям, соответствуют различные способы коммуникации, соединения по сети, обработки и хранения данных, а также пропускания электроэнергии. Например, многие смартфоны уже сейчас обладают качественной связью, богатыми сетевыми возможностями и способами обработки и хранения данных, а в мониторах сердечного ритма наблюдаются лишь ограниченные возможности коммуникации и вычислений.

«Интернет вещей» включает в себя ряд гетерогенных сетей, таких как WSN, беспроводные ячеистые сети, WLAN и т. п. Они помогают «вещам» в IoT обмениваться информацией. Сетевой шлюз в состоянии облегчить коммуникацию или взаимодействие различных устройств посредством Интернета, а также может использовать свою «сеть знаний» для локального выполнения алгоритмов оптимизации, что позволяет применять его при обработке множества сложных аспектов коммуникации в сети [44].

У «вещей» могут быть различные требования к качеству сервиса (QoS-требования, англ. quality of service — качество обслуживания, качество сервиса) по производительности, энергоэффективности и безопасности. К примеру, многим устройствам для работы нужны аккумуляторы, и поэтому снижение энергопотребления является для них одной из главных проблем. Напротив, для устройств с постоянным питанием улучшение энергосбережения чаще всего не является первоочередной задачей. IoT также значительно выиграет от использования существующих протоколов Интернета, таких как IPv6, поскольку это позволит напрямую обращаться к любому числу необходимых «вещей» через Интернет [3, 19, 20]. Основные коммуникационные протоколы и стандарты включают в себя радиочастотную идентификацию RFID (например, ISO 18000 6c EPC Class 1 Gen 2), NFC, IEEE 802.11 (WLAN), IEEE 802.15.4 (ZigBee), IEEE 802.15.1 (Bluetooth), мультихоп-беспроводные датчики и ячеистые сети, маломощные беспроводные персональные пространственные сети IETF (6LoWPAN), межмашинные соединения (M2M), а также традиционные IP-технологии (IP, IPv6 и т. д.).

Сети для IoT

Для беспроводных сетей существует довольно много слоев пересекающихся протоколов, например беспроводные датчики и приводные сети (WSAN) или ad-hoc-сети (AHNs) [37]. Однако они должны быть переработаны, прежде чем подойдут для применения в «Интернете вещей». Причина в том, что «вещи» в IoT часто обладают весьма разнообразными возможностями коммуникаций и вычислений, а также различными требованиями к качеству сервиса (QoS). Узлы в WSN, как правило, имеют схожие требования к оборудованию и сетям связи. Кроме того, в сети IoT для поддержки обмена информацией используется Интернет, но в отличие от WSN и AHN Интернет не нужно «включать», чтобы обеспечить соединение.

Управление сервисами в IoT

Управление сервисами в «Интернете вещей» связано с их реализацией и качеством, которые отвечают потребностям пользователей и приложений. Сервис-ориентированную архитектуру (англ. Service-oriented Architecture, SOA) можно использовать для инкапсуляции услуг, скрывая детали их реализации, например используемые протоколы [45]. Это дает возможность разделить компоненты в системе и, следовательно, скрыть гетерогенность от конечных пользователей. Сервис-ориентированная архитектура «Интернета вещей» позволяет приложениям использовать разнородные объекты, такие как совместимые сервисы [11].

Более того, динамический характер приложений «Интернета вещей» требует от него последовательного предоставления надежных услуг. Эффективная сервис-ориентированная архитектура может минимизировать негативные последствия, вызванные перемещением устройства или отказом батареи. Хорошим примером является OSGi-платформа (Open Services Gateway Initiative — спецификация динамической модульной системы и сервисной платформы для Java-приложений) [46], которая применяет динамическую сервис-ориентированную архитектуру (dynamic SOA architecture) для развертывания интеллектуальных сервисов. С этой целью OSGi используется в различных контекстах — например, для мобильных приложений, плагинов, серверов приложений и т. д. В «Интернете вещей» композиция сервисов на базе OSGi-платформы может быть реализована посредством Apache Felix iPoJo [47].

Сервис представляет собой сбор данных, а также режимы, которые необходимы, чтобы выполнить определенную функцию, обслужить устройство или его части. Сервис могжет предоставляться различными способами: так, он может ссылаться на другие первичные или вторичные сервисы и/или на набор характеристик сервиса. Сервисы можно разделить на два типа: первичные и вторичные. Первые выполняют первичные функции в узле IoT, и их можно рассматривать как основные компоненты сервиса, которые могут быть включены в другой сервис. Вторые могут предоставлять вспомогательные функции для основного сервиса или другие дополнительные услуги. Сервис может обладать одним или несколькими признаками, которые определяют структуры данных, разрешения, дескрипторы и прочие атрибуты сервисов [32, 38]. В сервис-ориентированном IoT сервисы могут быть созданы и развернуты поэтапно [3, 19, 20]: 1) развитие структурной платформы сервисов; 2) суммирование функциональных и коммуникационных возможностей устройств; 3) предоставление единого комплекса сервисов. Сервис управления идентификационной информацией включает в себя управленческий контекст и классификацию объектов. «Интернет вещей» также позволяет создать зеркало для каждого реаль-

ного объекта в IoT. Кроме того, IoT имеет сервис-ориентированную и связанную архитектуру, в которой виртуальные и физические объекты могут взаимодействовать между собой. Сервис-ориентированный IoT позволяет каждому из компонентов предлагать свои функциональные характеристики в качестве стандартных сервисов, что значительно повышает эффективность как всех устройств, так и сетей, участвующих в «Интернете вещей».

КЛЮЧЕВЫЕ ПРИЛОЖЕНИЯ IoT В ПРОМЫШЛЕННОСТИ

IoT-приложения пока находятся на относительно ранней стадии развития [19, 20, 32]. Однако «Интернет вещей» используется все чаще. Довольно много приложений для IoT разрабатывается и/или уже используется для мониторинга окружающей среды, в службах здравоохранения, управлении товарными запасами и продукцией, а также в сферах, связанных с продуктами питания, транспортом, поддержкой рабочих мест и домов, обеспечением безопасности и видеонаблюдения. В работах [19] и [20] дается обзор применения «Интернета вещей» в различных областях. Мы же в нашем обсуждении фокусируемся именно на промышленных приложениях IoT, для разработки которых необходимо решить несколько задач. В зависимости от предполагаемой области применения дизайнерам нужно найти некий компромисс для достижения баланса между издержками и выгодами [48]. Ниже приведены некоторые приложения IoT в промышленности.

Использование IoT в горном производстве

Обеспечение безопасности на шахтах является большой проблемой для многих стран в связи с условиями труда на подземных рудниках. В целях предотвращения и уменьшения количества несчастных случаев необходимо использовать технологии IoT, которые смогут принимать аварийные сигналы из шахты [53]. С помощью RFID, Wi-Fi и других технологий и устройств беспроводной связи, обеспечивающих эффективное взаимодействие между наземным и подземным пространствами, горнодобывающие компании смогут отслеживать местоположение шахтеров и анализировать критически важные данные по безопасности, полученные от датчиков. Еще одним полезным приложением являются химические и биологические сенсоры, применяемые для диагностики и раннего определения заболеваний у шахтеров, что особенно важно, поскольку они работают в опасных условиях. Эти сенсоры можно использовать для получения биологической информации о состоянии человеческого тела и органов, для выявления опасной пыли, вредных газов и других факторов окружающей среды, которые могут стать причиной несчастных случаев. Проблема использования всех этих технологий заключается в том, что беспроводным устройствам нужна энергия, которая потенциально может привести к взрыву газа в шахте. Таким образом, необходимы дополнительные исследования характеристик безопасности IoT-устройств, используемых в горнорудной промышленности.

Использование IoT в области транспорта и логистики

Роль «Интернета вещей» в транспортной и логистической отраслях промышленности становится все более значимой [19]. Поскольку все больше и больше физических объектов оснащаются штрихкодами, RFID-метами или датчиками, транспортные и логистические компании могут отслеживать в реальном времени движение физических объектов от исходного пункта к месту назначения по всей цепочке поставок, наблюдая за производством, доставкой, дистрибьюцией и т. д. [54]. Кроме того, ожидается, что IoT предоставит перспективные решения для преобразования транспортных систем и автомобильных сервисов [55]. Так как средства передвижения обладают все более мощными сетевыми и коммуникативными возможностями, а также средствами зондирования и обработки данных, «Интернет вещей» можно использовать как для их улучшения, так и для того, чтобы делиться малоиспользуемыми ресурсами с другими автомобилями на парковке или на дороге.

Например, интеллектуальная информационная система (iDrive), недавно разработанная компанией BMW, использует различные датчики и метки для мониторинга обстановки, в частности отслеживания местоположения транспортного средства и обеспечения схемы проезда [56]. Группа авторов [57] разработала интеллектуальную систему мониторинга для контроля температуры и влажности внутри грузовиков-рефрижераторов посредством RFID-меток, датчиков и беспроводных коммуникационных технологий. В ближайшем будущем мы увидим развитие автомобиль-

ного автопилота, который сможет обнаруживать пешеходов или другие транспортные средства, а также маневрировать таким образом, чтобы избежать столкновения [58]. Также для широкого применения «Интернета вещей» в сфере транспорта и логистики важны безопасность и защита конфиденциальности, так как многие водители опасаются утечки информации и вторжения в частную жизнь. Разумные усилия с помощью технологий, законов и регулирования будут необходимы для предотвращения несанкционированного доступа или раскрытия конфиденциальных данных.

ИССЛЕДОВАТЕЛЬСКИЕ ПРОБЛЕМЫ И БУДУЩИЕ ТЕНДЕНЦИИ

Общепризнано, что технологии и приложения «Интернета вещей» пока что находятся в зачаточном состоянии [32]. Все еще остается множество научных проблем внедрения IoT в промышленность, касающихся технологий, стандартизации, безопасности и конфиденциальности [19, 20]. В будущем необходимо стремиться к их решению, изучая особенности различных отраслей индустрии, для того чтобы обеспечить оптимальное внедрение IoT-устройств в промышленных условиях. Отраслевую специфику и требования к таким факторам, как стоимость, безопасность, конфиденциальность и риски, необходимо осознать еще до того, как «Интернет вещей» начнет широко использоваться в промышленности.

Технические проблемы

Хотя уже было проведено немало исследований по технологиям IoT, остается еще достаточно технических проблем.

1. Дизайн сервис-ориентированной архитектуры (SOA) для IoT доставляет определенные трудности, так как сервис-ориентированные «вещи» могут пострадать от своей производительности и ценовых издержек. Также, по мере того как все больше и больше физических объектов подключается к сети, часто возникают проблемы с масштабируемостью на разных уровнях, включая передачу данных и работу по сети, обработку данных и управление, а также обеспечение сервисов [20].
2. «Интернет вещей» является очень сложной гетерогенной сетью, включающей в себя соединения между разными типами сетей с помощью различных коммуникационных технологий. В настоящее время отсутствует общепринятая единая платформа, которая скрывает неоднородность выделенных сетевых/коммуникативных технологий и обеспечивает прозрачность именованных сервисов для различных приложений [20]. Передача больших по объему данных по сети в одно и то же время также может стать причиной частых задержек, конфликтов и коммуникативных проблем. Эта задача может быть разрешена путем сбора данных с помощью большого количества устройств. Управление связанными «вещами» с точки зрения облегчения взаимодействия субъектов и администрирования адресации, идентификации и оптимизации устройств на уровнях архитектуры и протоколов является одной из важных исследовательских задач [17].
3. Отсутствие общепринятого языка описания делает затруднительным развитие сервиса и усложняет интеграцию ресурсов физических объектов в сервисы, приносящие дополнительный доход (VAS-сервисы). Развитые сервисы могут быть несовместимы с разным коммуникационным и внедренным окружением [19, 22]. Кроме того, для распространения технологии IoT должны быть разработаны мощные методы обнаружения сервисов и службы именования объектов [19, 20].
4. Так как «Интернет вещей» часто развивается на основе традиционного ИКТ-окружения и на него влияет все, что подключено к сети, потребуется много работы, чтобы провести интеграцию IoT с существующими, в том числе устаревшими, ИТ-системами в единую информационную инфраструктуру. Помимо этого, большое количество подключенных к Интернету связанных «вещей» будет автоматически воспроизводить в режиме реального времени огромный поток данных [61],

которые не будут иметь особого смысла, если люди не смогут найти эффективный способ их анализа и понимания [62]. Анализ или осмысление больших объемов данных, генерируемых как приложениями IoT, так и существующими ИТ-системами, потребует серьезных навыков, и это может оказаться сложным для многих конечных пользователей. Кроме того, для интеграции IoT-устройств с внешними ресурсами, такими как существующие программные системы и вебсервисы, необходимы разработки различного промежуточного ПО, так как приложения сильно разнятся по отраслям. Выстраивание практических приложений, в которых разнородные и зависящие от «Интернета вещей» данные комбинируются с обычными, может оказаться сложной задачей для различных отраслей промышленности.

Стандартизация

Быстрое развитие «Интернета вещей» усложняет стандартизацию. Однако именно она играет важную роль в дальнейшем становлении и распространении «Интернета вещей». Стандартизация в IoT призвана снизить барьеры для входа новых поставщиков сервисов и пользователей, служит для улучшения взаимодействия различных приложений и сервисов, а также для обеспечения лучшего качества продуктов или сервисов более высокого уровня. Достаточная координация усилий в процессе стандартизации обеспечит устройствам и приложениям из разных стран возможность обмениваться информацией [20]. Различные стандарты, используемые в IoT (например, стандарты безопасности, связи и идентификации), могут оказаться ключевыми факторами для распространения и разработки технологий IoT. К специфическим вопросам в области стандартизации «Интернета вещей» относятся проблемы совместимости, уровня радиодоступа, семантической интероперабельности, а также безопасности и конфиденциальности [63–65]. Кроме того, рекомендуется разработать и отраслевые стандарты или инструкции для упрощения интеграции различных сервисов при внедрении «Интернета вещей» в промышленность.

Информационная безопасность и защита конфиденциальности

Широкое распространение новых технологий и сервисов «Интернета вещей» будет во многом основываться на информационной безопасности и защите конфиденциальности данных, которые становятся проблематичными в IoT из-за особенностей их развертывания, мобильности и комплексности [66]. Многие из существующих сегодня технологий доступны для бытового использования, но не подходят для промышленных приложений, в которых предъявляются повышенные требования по безопасности. Существующие технологии шифрования, заимствованные из WSN (беспроводной сенсорной сети) или других сетей, должны быть тщательно проверены перед их использованием для защиты информации при реализации «Интернета вещей». Так как IoT позволяет многие повседневные вещи отслеживать, мониторить и связывать, значительное количество личной и персональной информации может собираться автоматически [19]. Защита приватности в среде «Интернета вещей» станет более серьезной, чем в традиционной среде ИКТ, так как количество векторов атак на «вещи» IoT, видимо, будет намного больше [67, 68, 69]. К примеру, монитор здоровья будет собирать данные пациента, такие как частота сердечных сокращений и уровень сахара в крови, а затем отправлять информацию непосредственно в кабинет врача по сети. При этом она может быть украдена или взломана. Другой пример — биодатчик, используемый в пищевой промышленности. Он может применяться для мониторинга температуры и бактериального состава продуктов питания, хранящихся в холодильнике. Когда что-то портится, данные об этом отправляются в компанию через сеть. Однако такая информация должна быть строго конфиденциальной, чтобы защитить репутацию пищевой компании [20]. Следует отметить, что некоторые вопросы, такие как определение конфиденциальности в IoTи ее юридическое толкование, по-прежнему четко не определены. Несмотря на то, что уже существуют сетевые технологии безопасности, для обеспечения основ конфиденциальности и безопасности в IoT предстоит проделать еще много работы. В первую очередь, необходимо изучить следующие аспекты: 1) определение безопасности и конфиденциальности с социальной, правовой и культурной точек зрения; 2) механизм доверия и репутации; 3) безопасность связи — в частности, сквозное шифрование (end-to-end); 4) конфиденциальность переписки и данных пользователя; 5) защита сервисов и приложений.

Направления исследований

Подход к развитию инфраструктуры «Интернета вещей» будет поэтапным, включающим в себя расширение существующих методов идентификации, таких как RFID. При этом для решения множества вышеописанных проблем необходимы международное сотрудничество и высокий уровень системной перспективы [20, 70–73]. В связи с этим мы определили, помимо уже указанных, некоторые направления исследования.

1. Интеграция социальных сетей с IoT-решениями. В последнее время возник большой интерес к использованию социальных сетей для улучшения коммуникаций между различными «IoT-вещами». Недавно группой ученых [42] была предложена новая парадигма — социальный «Интернет вещей» (SIoT). Также наблюдается тенденция перехода от «Интернета вещей» к новому направлению, называемому «Веб вещей» (Web of Things), которое позволит IoT-объектам стать акторами и равноправными участниками процессов во Всемирной паутине [74–77].
2. Разработка «зеленых» IoT-технологий. Так как «Интернет вещей» включает в себя миллиарды подключенных через беспроводную сеть коммуникативных датчиков, потребляемая ими мощность вызывает большую тревогу и ограничивает использование «Интернета вещей». Улучшение энергосбережения должно стать важнейшей целью для разработчиков IoT-устройств, прежде всего беспроводных датчиков [78, 79].
3. Разработка контекстно зависимых решений связующего програм-

много обеспечения IoT. Когда миллиарды датчиков подключены к Интернету, для человека становится невозможным обработать все данные, собранные этими датчиками. Контекстно зависимые техники вычислений, такие как связующее программное обеспечение IoT, предназначены для лучшего понимания данных с датчиков и помощи в отборе информации для обработки [61]. В настоящее время большинство связующего программного обеспечения IoT не имеет возможностей для осознания контекста. Европейский союз назвал контекстную зависимость важной областью исследований IoT и указал сроки (2015–2020 гг.) для проведения компьютерных исследований и разработки контекстно-зависимого «Интернета вещей» [21].

4. Применение методов искусственного интеллекта для создания умных «вещей». Некоторые исследователи [80] предлагают создать «Интернет разумных вещей», привнеся искусственный интеллект в «вещи» и коммуникационные сети. По их мнению, будущие системы IoT должны иметь такие характеристики, как «самоконфигурирование, самооптимизация, самозащита и самоисцеление» [81, 82]. В будущем «умные» вещи станут еще умнее [83], контекстно зависимы, будут обладать большой памятью и широкими возможностями обработки, а также способностью рассуждать.
5. Объединение «Интернета вещей» и облачных вычислений. Облака — хороший способ подключения «вещей», они могут предоставить нам доступ к различным «вещам» через Интернет. Дальнейшие исследования будут сосредоточены на внедрении новых моделей и платформ, которые обеспечат «зондирование как сервис» в облаках [84–86].

ЗАКЛЮЧЕНИЕ

В качестве сложной киберфизической системы «Интернет вещей» объединяет различные устройства, оснащенные зондированием, идентификацией, обработкой данных, коммуникацией и обладающие сетевыми возможностями. В частности, датчики и исполнительные устройства становятся все мощнее, дешевле и меньше, что приводит к их повсеместному использованию. Индустрия сильно заинтересована в развертывании IoT-устройств для разработки промышленных приложений, таких как автоматический мониторинг, контроль, управление, эксплуатация и техническое обслуживание. Предполагается, что из-за стремительного развития технологий и промышленной инфраструктуры «Интернет вещей» будет широко применяться в промышленности. Например, в пищевой промышленности интеграция беспроводных сенсорных сетей (WSN) и радиочастотной идентификации (RFID) служит для построения автоматизированных систем контроля, мониторинга и отслеживания качества продуктов питания по всей цепочке поставок. ⬣

Полная версия статьи доступна на сайте: