ИНТЕРНЕТ ВЕЩЕЙ: КРАТКИЙ ОБЗОР

Вопросы и проблемы использования сети Интернет в более глобальном масштабе

ОКТЯБРЬ 2015 ВЕРСИЯ ДЛЯ ЦВЕТНОЙ ПЕЧАТИ

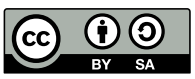
Internet Society™

ИНТЕРНЕТ ВЕЩЕЙ: КРАТКИЙ ОБЗОР

Вопросы и проблемы использования сети Интернет в более глобальном масштабе

Карен Роуз, Скотт Элдридж, Лайман Чапин

ОКТЯБРЬ **2015** ВЕРСИЯ ДЛЯ ЦВЕТНОЙ ПЕЧАТИ



Internet Society™

СОДЕРЖАНИЕ

ЧТО ТАКОЕ ИНТЕРНЕТ ВЕЩЕЙ? 11

КАКИЕ ВОПРОСЫ ПОДНИМАЕТ ИНТЕРНЕТ ВЕЩЕЙ? 27

КРАТКОЕ СОДЕРЖАНИЕ

Интернет вещей - это новая тема, имеющая важное техническое, социальное и экономическое значение. Потребительские товары, товары длительного пользования, автомобили и грузовики, промышленные и энергетические компоненты, датчики и другие предметы повседневной жизни проектируются с подключением к Интернету и с мощными функциями анализа данных, что обещает полностью изменить наш стиль работы, образ жизни и развлечения. Влияние IoT на Интернет и экономику в ближайшем будущем трудно переоценить, и согласно некоторым оценкам, к 2025 году 100 млрд устройств будут оснащены функциями IoT, а глобальные экономические показатели их воздействия составят 11 триллионов долларов США.

Однако, в то же время, перед Интернетом вещей стоит ряд проблем, которые могут помешать нам воспользоваться его потенциальными преимуществами. Постоянные сообщения о взломе подключенных к Интернету устройств, проблемы ведения наблюдения и опасения в отношении личной конфиденциальности уже привлекли внимание общественности. На настоящий момент технические вопросы продолжают оставаться нерешенными, а также возникают новые сложности в области политики, законодательства и дальнейшего развития.

Данный документ призван оказать содействие членам Internet Society вещей в поддержании диалога по этому вопросу с учетом различных прогнозов в отношении его потенциальных опасностей и преимуществ. Интернет вещей затрагивает ряд сложных вопросов из различных областей.

Основные предпосылки для изучения возможностей и проблем IoT:

ОПРЕДЕЛЕНИЯ IOT

Термин «Интернет вещей» обычно относится к тем сценариям, когда подключением к сети и вычислительными функциями оснащаются предметы, датчики и другие предметы повседневной жизни, обычно не считающиеся компьютерами, благодаря чему эти устройства могут генерировать и использовать данные и обмениваться ими при минимальном участии человека. Тем не менее, единого и универсального определения не существует.

ПОДДЕРЖИВАЮЩИЕ ТЕХНОЛОГИИ

Концепция объединения компьютеров, датчиков и сетей для мониторинга и управления устройствами существует уже несколько десятилетий. Тем не менее, недавнее слияние нескольких тенденций на рынке технологий приблизило Интернет вещей к повседневной реальности. В число этих тенденций входят *Доступ из любой точки*, *Широкое распространение сетей на основе протокола IP*, *Экономические тенденции в области вычислительных систем*, *Миниатюризация*, *Достижения в области анализа данных*, а также *Развитие облачных вычислений*.

МОДЕЛИ ПОДКЛЮЧЕНИЯ

Для внедрения IoT используются различные технические модели обеспечения связи, каждая из которых имеет свои собственные характеристики Четыре общих модели обеспечения связи, описанные комиссией по архитектуре Интернет: *от устройства к устройству*, *от устройства к облаку*, *от устройства к шлюзу* и *совместное использование данных на сервере*. Эти модели демонстрируют гибкость возможностей подключения и использования устройств IoT.

ПОТЕНЦИАЛ ДЛЯ ТРАНСФОРМАЦИИ

Если тенденции и планы в отношении IoT найдут свое воплощение в реальности, это может привести к изменению взглядов на потенциальные последствия и проблемы в мире, где чаще всего взаимодействие с Интернетом является результатом пассивного контакта с подключенными объектами, а не активного контакта с содержимым. Потенциальное достижение этого результата — «гиперподключенного мира» — является проявлением универсальности применения архитектуры Интернета, которая не ограничивает область приложений или услуг, для которых может применяться данная технология.

Были изучены пять ключевых областей проблем IoT для определения наиболее насущных проблем и вопросов, связанных с этой технологией. Эти области включают безопасность; конфиденциальность; интероперабельность и стандарты; законодательство, нормативные требования и права; а также молодые экономики и развитие.

БЕЗОПАСНОСТЬ

Несмотря на то, что проблемы безопасности в области информационных технологий сами по себе не новы, многие примеры внедрения IoT ставят перед нами новые уникальные проблемы в области безопасности. Решение этих проблем и обеспечение безопасности в области продуктов и услуг IoT должно быть основным приоритетом. Пользователи должны быть уверены в том, что устройства IoT и связанные с ними услуги в области данных не имеют уязвимых мест, особенно по мере распространения этой технологии и ее интеграции в нашу повседневную жизнь. Недостаточно защищенные услуги и устройства IoT могут использоваться как потенциальные точки доступа для кибератак и открывать возможность хищения данных в связи с отсутствием необходимой защиты потоков данных.

Взаимосвязанность устройств IoT означает, что каждое недостаточно защищенное устройство, подключенное к Интернету, может повлиять на общий уровень безопасности и устойчивости системы. Эта проблема усугубляется другими факторами, такими как массовое развертывание устройств IoT с однородной структурой, способность некоторых устройств автоматически подключаться к другим устройствам, а также вероятность применения этих устройств в незащищенной среде.

Согласно общему правилу, разработчики и пользователи устройств и систем IoT несут коллективное обязательство обеспечить защиту пользователей и Интернета как такового от потенциальных угроз. В связи с этим, для создания эффективных и правильных методов защиты IoT, соответствующих масштабу и уровню сложности этих опросов, необходим совместный подход на основе сотрудничества.

КОНФИДЕНЦИАЛЬНОСТЬ

Полное раскрытие потенциала Интернета вещей зависит от выбора стратегий, учитывающих право на конфиденциальность в соответствии с широким спектром ожиданий. Потоки данных и специфика пользователей, управляемые устройствами IoT, могут обеспечить невероятную ценность для пользователей IoT, но проблемы конфиденциальности и потенциальных злоупотреблений могут препятствовать полному внедрению Интернета вещей. Это означает, что конфиденциальность и уважение к праву на конфиденциальность имеют ключевое значение для завоевания доверия пользователей по отношению к Интернету, подключенным устройствам и связанным с ними услугам.

Интернет вещей выводит на новый уровень полемику о конфиденциальности, так как широкое применение может в корне изменить методы сбора, анализа, употребления и защиты личных данных. Например, IoT усиливает озабоченность вероятностью дополнительного наблюдения и слежения, невозможностью отказаться от предоставления некоторых данных и возможностью объединения нескольких потоков данных IoT для создания подробных цифровых описаний пользователей. Это важные проблемы, но они не являются неразрешимыми. Чтобы понять все открывающиеся возможности, необходимо разработать стратегии учета личных предпочтений в отношении конфиденциальности в соответствии с ожиданиями пользователей, при этом продолжая развивать новаторские технологии и услуги.

ИНТЕРОПЕРАБЕЛЬНОСТЬ / СТАНДАРТЫ

Фрагментированная среда патентованных технических реализаций IoT снижает их ценность для пользователей и отрасли целом. Несмотря на то, что полная интероперабельность продуктов и услуг не всегда целесообразна или необходима, потребители могут отказываться от покупки продуктов и услуг IoT при отсутствии гибкой интеграции, высокой сложности владения и возможной зависимости от поставщика.

Кроме того, неправильно созданные и настроенные устройства IoT могут оказать отрицательное влияние на сетевые ресурсы, к которым они подключаются, а также на Интернет в целом. Правильные стандарты, эталонные модели и передовые методы также будут способствовать ограничению распространения устройств, которые могут оказать отрицательное влияние на Интернет. Использование общих, открытых и широкодоступных стандартов в качестве технических составляющих устройств и услуг IoT (таких, как протокол Интернета) обеспечит широкий ряд преимуществ для пользователей, инновации и экономические возможности.

ЗАКОНОДАТЕЛЬСТВО, НОРМАТИВНЫЕ ТРЕБОВАНИЯ И ПРАВА

Использование устройств IoT поднимает ряд нормативно-правовых вопросов, а также расширяет круг уже существующих проблем в отношении Интернета. Круг этих вопросов очень широк, и скорость изменений в области технологии IoT часто опережает адаптацию соответствующих нормативно-правовых систем и политики.

Одна категория вопросов касается транснациональных информационных потоков, которые возникают, когда устройства IoT осуществляют сбор данных о лицах в одной юрисдикции и передают их в другую юрисдикцию, где действуют другие законы в отношении обработки данных. Кроме того, данные, полученные устройствами IoT, иногда могут быть доступны для ненадлежащего использования, что может привести к дискриминации в отношении некоторых пользователей. Другие правовые вопросы в отношении устройств IoT включают конфликт между наблюдением со стороны правоохранительных органов и гражданскими правами; хранение данных и политики их уничтожения; а также правовую ответственность за их непредусмотренное использование, пробелы в защите или конфиденциальности.

Несмотря на наличие многочисленных и сложных проблем нормативно-правового характера, принятие руководящих принципов интернет-сообщества для расширения возможности пользователей *подключаться*, *высказываться*, *вводить новшества*, *обмениваться*, *делать выбор* и *доверять* является основным условием для нормативно-правовой адаптации в отношении IoT для защиты прав пользователей.

РАЗВИВАЮЩИЕСЯ ЭКОНОМИКИ И ВОПРОСЫ РАЗВИТИЯ

Интернет вещей открывает широкие социальные и экономические перспективы для развивающихся экономик. Они включают в себя такие области, как устойчивое ведение сельского хозяйства, качество и использование воды, здравоохранение, развитие промышленности, а также управление использованием окружающей среды, в числе прочих. Как таковой, IoT может стать инструментом для достижения целей устойчивого развития, поставленных ООН.

Широкий спектр проблем IoT не ограничивается странами с развитой промышленностью. Развивающиеся регионы также должны внести свой вклад, чтобы воспользоваться потенциальными преимуществами IoT. Кроме того, необходимо будет учесть уникальные потребности и вопросы внедрения этой технологии в менее развитых регионах. Такие вопросы, как наличие необходимой инфраструктуры, стимулирование рынка и инвестиций, потребность в технических навыках и наличие соответствующей политики.

Интернет вещей уже здесь. Он станет инструментом для создания принципиально нового, «подключенного» мира, с более тесным взаимодействием между предметами, их средой и людьми. Тем не менее, чтобы воспользоваться потенциальными преимуществами для людей, общества и экономики, необходимо решить вопросы и проблемы, связанные с IoT.

И наконец, для поиска возможности максимального использования преимуществ Интернета вещей при максимальном снижении рисков недостаточно обсуждения различных точек зрения, противопоставляющих возможности IoT его потенциальным опасностям. Вместо этого требуется активное участие на основе имеющихся данных, наличие диалога и сотрудничество различных заинтересованных сторон для поиска наиболее эффективных путей развития.

ВВЕДЕНИЕ

Интернет вещей (IoT) - важная тема в сфере технологии, политик и инженерных разработок, активно обсуждаемая как в специализированной литературе, так и в широкой прессе. Эта технология воплощена в широком наборе сетевых продуктов, систем и датчиков, применяющих достижения в области вычислительной техники, миниатюризации электроники и сетевых соединений для интеграции новых функций, которые ранее не были возможны. На многочисленных конференциях, в отчетах и прессе обсуждается возможное воздействие «революции IoT», от новых рыночных возможностей и моделей бизнеса до проблем безопасности, конфиденциальности и технической интероперабельности.

Крупномасштабное внедрение устройств IoT во многом изменит наш стиль жизни. Для потребителей новые продукты IoT, такие как бытовая техника с подключением к Интернету, компоненты домашней автоматики и устройства для регулирования электроэнергии приближают нас к концепции «умного дома», обеспечивая более высокий уровень безопасности и энергоэффективности. Другие личные устройства IoT, такие как носимые устройства для фитнеса и контроля за состоянием здоровья, а также медицинские устройства с подключением к сети меняют методы оказания медицинских услуг. Преимуществами этой технологии смогут воспользоваться инвалиды и пожилые люди, так как она способна обеспечить более высокий уровень независимости и качества жизни по разумной цене.[1] Такие системы IoT как, транспортные средства, подключенные к единой сети, интеллектуальные системы управления дорожным движением и встроенные датчики на дорогах и мостах приближают нас к идее «интеллектуальных городов» для снижения числа пробок и сокращения энергопотребления. Технология IoT обеспечивает возможность трансформировать сельское хозяйство, промышленность, производство и потребление электроэнергии путем увеличения доступности информации по всей цепочке добавленной стоимости на производстве с использованием сетевых датчиков. Однако для того, чтобы воспользоваться всеми преимуществами IoT, необходимо принять во внимание и решить ряд вопросов.

Ряд компаний и научно-исследовательских организаций делают многочисленные прогнозы относительно потенциального воздействия IoT на Интернет и экономику в течение ближайших пяти или десяти лет. Например, согласно прогнозам Cisco, к 2019 году будет насчитываться 24 млрд объектов, подключенных к Интернету;[2] Со своей стороны Morgan Stanley прогнозирует к 2020 году 75 млрд таких устройств.[3] Huawei заглядывает еще дальше и прогнозирует 100 млрд устройств с подключением IoT к 2025 году.[4] McKinsey Global Institute считает, что финансовое влияние IoT на глобальную экономику может достигнуть от 3,9 до 11,1 млрд. долларов к 2025 году.[5] Несмотря на обилие прогнозов и невозможность определить точные показатели, в целом они сулят перспективу значительного роста и влияния.

Некоторые обозреватели считают IoT символом мира полностью взаимосоединенных устройств, прогресса, эффективности и широких возможностей, а также потенциальным повышением ценности для промышленности и глобальной экономики, выражающимся в миллиардах.[6] Другие предупреждают, что IoT является предвестником мрачного мира постоянного наблюдения, нарушений конфиденциальности и безопасности, а также зависимости потребителей. Внимание общественности привлекли заголовки в прессе о взломе автомобилей, подключенных к сети Интернет,[7] озабоченность постоянным наблюдением, основанная на функциях распознавания голоса в «интеллектуальных» телевизорах,[8] и опасения в отношении конфиденциальности в связи с потенциальным злоупотреблением данными IoT[9]. Это обсуждение возможностей в сравнении с рисками, в сочетании с постоянным появлением информации в популярных СМИ и маркетингом могут усложнить понимание IoT.

В целом можно сказать, что Интернет-сообщество интересуется IoT, так как эта технология представляет развивающийся аспект взаимодействия людей и организаций с Интернетом в личной, общественной и экономической жизни. Даже если самые скромные прогнозы окажутся верными, многочисленные области применения IoT могут привести к фундаментальным изменениям во взаимодействии пользователей с Интернетом и его воздействия на них. В свою очередь, это приведет к возникновению новых проблем и к новому взгляду на уже существующие проблемы, беспокоящие пользователей и потребителей, в области технологии, политики и законодательства. Вероятно, IoT также будет оказывать разное влияние на различные экономики и регионы, открывать различные возможности и ставить различные проблемы во всем мире.

Данный документ призван оказать содействие членам сообщества Интернета вещей в поддержании диалога по этому вопросу с учетом различных прогнозов в отношении его потенциальных опасностей и преимуществ. Он включает компетентный краткий обзор основных характеристик IoT и некоторых ключевых вопросов и проблем, которые ставит эта технология по отношению к Интернет-сообществу и нашим основным ценностям.[10] В этом документе также рассматриваются некоторые уникальные аспекты Интернета вещей, благодаря которым эта технология способна трансформировать Интернет.

В рамках данного краткого обзора мы не ставим своей задачей поиск определенной программы действий для Интернет-сообщества в отношении IoT. Мы считаем этот документ информационным ресурсом и отправной точкой для обсуждения вопросов IoT среди членов Интернет-сообщества.

Данный документ включает четыре основных раздела:

ЧТО ТАКОЕ ИНТЕРНЕТ ВЕЩЕЙ?

Краткое описание его происхождения, определения и технические модели подключения.

СТР. 11

КАКИЕ ВОПРОСЫ ПОДНИМАЕТ ИНТЕРНЕТ ВЕЩЕЙ?

Вводная часть и обсуждение проблем, связанных с IoT.

СТР. 27

ЗАКЛЮЧЕНИЕ

СТР. 67

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Дополнительная информация и ссылки на проекты по всему миру, предназначенные для решения вопросов IoT.

СТР. 71

ПРИМЕЧАНИЯ К РАЗДЕЛУ

Введение

1. Для получения дополнительной информации об IoT и о том, каким образом он может помочь лицам с инвалидностью, см. (на английском языке): Valerio, Pablo “Google: IoT Can Help The Disabled”. *InformationWeek*, 10 марта 2015 г. http://www.informationweek.com/mobile/mobile-devices/google-iot-can-help-the-disabled/a/d-id/1319404; а также Domingo, Mari Carmen. “An Overview of the Internet of Things for People with Disabilities”. *Journal of Network and Computer Applications* 35, № 2 (март 2012): 584–96. doi:10.1016/j.jnca.2011.10.015.

2. “Cloud and Mobile Network Traffic Forecast - Visual Networking Index (VNI)”. *Cisco, 2015 г.* http://cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

3. Danova, Tony. “Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020.” *Business Insider*, 2 октября 2013 г. http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10

4. “Global Connectivity Index”. Huawei Technologies Co., Ltd., 2015. Интернет. 6 сент. 2015 г. http://www.huawei.com/minisite/gci/en/index.html

5. Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, Dan Aharon “The Internet of Things: Mapping the Value Beyond the Hype”. McKinsey Global Institute, июнь 2015 г.

6. Thierer, Adam, Andrea Castillo. “Projecting the Growth and Economic Impact of The Internet of Things”. George Mason University, Mercatus Center, 15 июня 2015 г. http://mercatus.org/sites/default/files/IoT-EP-v3.pdf

7. Greenberg, Andy. “Hackers Remotely Kill a Jeep on the Highway—With Me in It.” *WIRED*, 21 июля 2015 г. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

8. “Samsung Smart TV’s Voice Recognition Creates Privacy Concerns.” *CBS This Morning*. CBS News, 10 февраля 2015 г. http://www.cbsnews.com/videos/samsung-smart-tvs-voice-recognition-creates-privacy-concerns/

9. Bradbury, Danny. “How Can Privacy Survive in the Era of the Internet of Things?” *The Guardian*, 7 апреля 2015 г., разд. Technology. http://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things

10. “Values and Principles”. *Principles*. Internet Society, 2015 г. http://www.internetsociety.org/who-we-are/mission/values-and-principles

11. На тему IoT написано множество документов и статей. Читатели, заинтересованные в получении дополнительной информации, помимо приведенной в данном документе, могут ознакомиться с источниками, указанными в примечаниях и в справочном разделе в конце данного документа.

ЧТО ТАКОЕ ИНТЕРНЕТ ВЕЩЕЙ?

ПРОИСХОЖДЕНИЕ, ОПРЕДЕЛЯЮЩИЕ ФАКТОРЫ И ОБЛАСТИ ПРИМЕНЕНИЯ

Термин «Интернет вещей» (IoT) впервые использовал в 1999 году британский новатор в области технологий по имени Кевин Эштон для описания системы, в которой предметы физического мира могут подключаться к Интернету с помощью датчиков.[12] Эштон создал этот термин для того, чтобы проиллюстрировать потенциальные возможности подключения меток радиочастотной идентификации (RFID),[13] используемых в корпоративных цепочках поставок, для подсчета и отслеживания товаров без необходимости вмешательства со стороны человека. Сегодня термин «Интернет вещей» широко используется для описания сценариев, в которых подключение к Интернету и вычислительные функции распространяются на ряд объектов, устройств, датчиков и других предметов повседневной жизни.

Несмотря на то, что термин «Интернет вещей» является сравнительно новым, концепция объединения компьютеров и сетей для мониторинга и управления устройствами существует уже несколько десятилетий. Например, уже в конце 1970-х гг. осуществлялось коммерческое использование систем для удаленного мониторинга счетчиков электрической сети через телефонные линии.[14] В 1990-х гг. достижения в области беспроводной технологии сделали возможным широкое распространение корпоративных и производственных решений «машина-машина» (M2M) для мониторинга и управления оборудованием. Однако многие из этих ранних решений M2M были созданы на основе закрытых специализированных сетей на фирменных или отраслевых стандартах,[15] а не на сетях на основе протокола Интернета (IP) и стандартах Интернета.

Идея использования IP для подключения к Интернету устройств, не являющихся компьютерами, не нова. Первое устройство с подключением к Интернету — тостер с поддержкой протокола IP, который можно было включать и выключать через Интернет — был представлен на интернет-конференции в 1990 году. [16] В течение следующих нескольких лет появились другие предметы с поддержкой протокола IP, включая автомат прохладительных напитков[17] в университете Карнеги-Меллона в США и кофеварка[18] в Троянском зале в Кембриджском университете в Великобритании (которая оставалась подключенной к Интернету до 2001 года). С самых первых эксцентричных шагов упорная работа в области исследований и разработок привела к созданию «интеллектуальной сети объектов»,[19] которая стала основой для сегодняшнего Интернета вещей.

Если идея подключения объектов друг к другу и к Интернету не нова, следует спросить, почему Интернет вещей вновь отличается такой популярностью?

В более широкой перспективе слияние нескольких тенденций рынка и технологии[20] позволяет просто и недорого подключить большее число устройств меньшего размера (см. вставку 1, стр. 13).

ВСТАВКА 1

ТЕНДЕНЦИИ РЫНКА И ТЕХНОЛОГИИ, СПОСОБСТВУЮЩИЕ РАЗВИТИЮ IOT

ПОВСЕМЕСТНОЕ ПОДКЛЮЧЕНИЕ

Повсеместное недорогое и высокоскоростное сетевое подключение, особенно с помощью лицензированных и нелицензированных услуг беспроводной связи и технологий, позволяет подключить к сети практически любой предмет.

ШИРОКОЕ ПРИМЕНЕНИЕ СЕТЕЙ НА ОСНОВЕ ПРОТОКОЛА IP

Протокол IP стал основным глобальным сетевым стандартом, обеспечивающим четко определенную и широко используемую платформу для программного обеспечения и инструментов, которая может быть легко и без больших затрат включена в широкий спектр устройств.

ЭКОНОМИЧЕСКИЕ ТЕНДЕНЦИИ В ОБЛАСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Под воздействием отраслевых инвестиций в исследования, разработки и производство, закон Мура[21] продолжает обеспечивать все большие вычислительные возможности по все более низкой цене и энергопотреблении.[22]

МИНИАТЮРИЗАЦИЯ

Достижения в области производства позволяют применять самые современные технологии вычислений и связи в объекты очень маленького размера.[23] В сочетании с более высокой экономичностью вычислений это послужило толчком для создания недорогих датчиков малого размера, на которых основано множество областей применения IoT.

ДОСТИЖЕНИЯ В ОБЛАСТИ АНАЛИЗА ДАННЫХ

Новые алгоритмы и быстрый рост вычислительной мощности, объема хранения данных и облачных услуг делают возможными агрегирование, корреляцию и анализ больших объемов данных; эти крупные и динамические наборы данных обеспечивают новые возможности получения информации и знаний.

РАЗВИТИЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Облачные вычисления, использующие удаленные сетевые ресурсы для обработки, управления и хранения данных, позволяют небольшим и распределенным устройствам взаимодействовать с мощными функциями анализа и управления на сервере.

В отчете McKinsey “Unlocking the Potential of the Internet of Things” (на английском языке)[25] описывается широкий спектр возможных областей применения с точки зрения условий, в которых IoT будет обеспечивать преимущества для отрасли и пользователей (см. вставку 2, стр. 15).

Многие организации разработали свою собственную классификацию и деление на категории для областей и примеров использования IoT. Например, «промышленный IoT» это термин, широко используемый компаниями и ассоциациями для описания областей применения IoT, связанных с производством товаров и услуг (в том числе производство и инженерные инфраструктуры).[26] Другие определяют IoT по типу устройств. Например, носимые технологии[27] и оборудование.[28] А некоторые рассматривают IoT в контексте интегрированных, географически привязанных разработок, таких как «умный дом» или «умный город».[29] Какова бы ни была область применения, очевидно, что IoT может применяться практически в любой области нашей жизни.

По мере увеличения числа устройств, подключенных к Интернету, ожидается существенное увеличение трафика. Например, согласно прогнозам Cisco, интенсивность сетевого обмена данными между устройствами (не включая ПК) увеличится с 40% в 2014 г. до почти 70% в 2019 г.[30] Cisco также прогнозирует, что число «межмашинных» подключений ("M2M") (включая промышленные, домашние, медицинские, автомобильные и другие вертикали IoT) увеличится с 24% от всех подключенных устройств в 2014 г. до 43% в 2019 г.

Результатом этих тенденций станет то, что через десять лет понятие подключения к Интернету существенно изменится. Как указал профессор Массачусетского технологического института (MIT) Нил Гершенфельд, «…Возможно, стремительный рост Всемирной паутины был лишь искрой, которая приведет к настоящему взрыву теперь, когда вещи начинают подключаться к сети».[31]

В сознании обычных людей Всемирная паутина уже практически стала синонимом Интернета. Сетевые технологии способствуют взаимодействию между людьми и контентом, делая его определяющей характеристикой нынешнего Интернета. Использование Интернета во многом характеризуется активным участием пользователей, скачивающих и создающих

70%

Согласно оценкам Cisco, процент интернет-трафика, генерируемого устройствами, не являющимися ПК, увеличится почти до 70% к 2019 г.

контент через компьютеры и смартфоны. Если прогнозы относительно роста IoT окажутся верными, может произойти сдвиг в сторону более пассивного взаимодействия с Интернетом между пользователями и такими объектами, как автомобильные компоненты, бытовая техника и устройства с самодиагностикой. Эти устройства отправляют и получают данные от имени пользователя, при минимальном участии человека, а иногда даже без его ведома.

Развитие IoT может привести к изменению образа мышления, если наиболее распространенное взаимодействие с Интернетом и данными, полученными на основе этого взаимодействия, будет происходить в результате пассивного взаимодействия с подключенными предметами вокруг. Потенциальное достижение этого результата — «гиперподключеного мира» — является подтверждением общего назначения Интернета без ограничения области применения или услуг, в которых может применяться эта технология.[32]

ВСТАВКА 2

«УСЛОВИЯ» ДЛЯ ИСПОЛЬЗОВАНИЯ IOT

УСЛОВИЯ	ПРИМЕРЫ
ЧЕЛОВЕК Устройства, закрепленные на человеческом теле или внутри него	Устройства (носимые и проглатываемые) для мониторинга и поддержания здоровья, а также для обеспечения хорошего самочувствия людей; управление ходом заболевания, повышение уровня физической подготовки или производительности
ЖИЛЬЕ Здания, в которых живут люди	Домашние контроллеры и системы безопасности
ТОЧКИ РОЗНИЧНЫХ ПРОДАЖ Места, где потребители делают покупки	Магазины, банки, рестораны, арены — любые места, где люди принимают решения о покупках и делают их; кассы самообслуживания, специальные предложения, оптимизация товарных запасов
ОФИСЫ Места занятости работников умственного труда	Управление энергопотреблением и безопасностью в офисных зданиях; повышение производительности, в том числе, для мобильных сотрудников
ПРОИЗВОДСТВЕННЫЕ ПРЕДПРИЯТИЯ Стандартизованная производственная среда	Места с повторяющейся последовательностью рабочих операций, включая больницы и фермы; производственная эффективность, оптимизация использования оборудования и инвентаря
РАБОЧИЕ ОБЪЕКТЫ Специализированная производственная среда	Горная промышленность, нефтегазовая промышленность, строительство; производственная эффективность, профилактическое обслуживание, здоровье и безопасность
ТРАНСПОРТНЫЕ СРЕДСТВА Системы внутри движущихся транспортных средств	Транспортные средства, включая автомобили, грузовики, суда, самолеты и поезда; обслуживание по техническому состоянию, конструкция на основе условий использования, предпродажный анализ
ГОРОДА Городская среда	Общественные места и инфраструктура в городских условиях; адаптивное регулирование движения транспорта, интеллектуальные счетчики, мониторинг окружающей среды, управление ресурсами
ОТКРЫТЫЕ ПРОСТРАНСТВА За пределами городской среды (и других условий)	В число открытых пространств входят железнодорожные пути, автономные транспортные средства (за пределами города) и аэронавигация; составление маршрута в реальном времени, услуги подключаемой навигации, отслеживание грузов

ИСТОЧНИК: McKinsey Global Institute[24]

РАЗНЫЕ ОПРЕДЕЛЕНИЯ, ОДИНАКОВЫЕ КОНЦЕПЦИИ

Несмотря на активное обсуждение вопросов Интернета вещей во всем мире, для этого термина отсутствует единое, общепринятое определение. Различные группы используют разные определения для описания или распространения определенной точки зрения на то, что представляет собой IoT и каковы его основные характеристики. Некоторые определения указывают на понятие Интернета или протокола Интернет (IP), в то время как другие не упоминают его. Например, взглянем на следующие определения:

Комиссия по архитектуре Интернет (IAB) начинает RFC 7452,[33] «Особенности архитектуры в сетях интеллектуальных объектов», со следующего описания:

> Термин «Интернет вещей» (IoT) обозначает тенденцию, при которой большое число встроенных устройств использует услуги связи на основе протокола Интернет. Многие из этих устройств, часто называемые «интеллектуальными объектами», не управляются напрямую человеком, но существуют в виде компонентов зданий или транспортных средств или установлены в окружающей среде.

В Рабочей группе проектирования Интернет (IETF) термин «сеть интеллектуальных объектов» обычно используется по отношению к Интернету вещей. В этом контексте «интеллектуальные объекты» это устройства, обычно имеющие значительные ограничения, такие как ограниченная мощность, память, ресурсы обработки или ширина диапазона.[34] Работа IETF организована на основе определенных требований по достижению сетевой интероперабельности между несколькими типами интеллектуальных объектов.[35]

Опубликованная в 2012 году Международным союзом электросвязи (ITU) ITU–T Рекомендация Y.2060, *Краткий обзор Интернета вещей*,[36] включает понятие взаимоподключаемости, хотя и не связывает напрямую IoT с Интернетом:

> 3.2.2 Интернет вещей (IoT): глобальная инфраструктура общества с развитой информационной технологией, обеспечивающая возможность предоставления расширенных услуг за счет взаимоподключения предметов (физических и виртуальных) на основе существующей и развивающейся функционально совместимой информации и технологий связи.
>
> Примечание 1 — За счет использования функций идентификации, сбора, обработки и передачи данных IoT использует предметы для того, чтобы предлагать услуги во всех областях при соблюдении требований безопасности и конфиденциальности.
>
> Примечание 2 — В более широкой перспективе IoT может рассматриваться как концепция, оказывающая влияние на общество и технологии.

Это определение для специализированной статьи в журнале IEEE по вопросам связи,[37] связывает IoT с облачными услугами:

> Интернет вещей (IoT) – это концептуальная основа, в соответствии с которой все предметы представлены в Интернете и имеют определенное место в нем. Точнее, Интернет вещей ставит своей задачей предлагать новые области применения и услуги, объединяющие физический и виртуальный мир, в котором межмашинная

> связь (M2M) является основной связью для взаимодействия вещей и приложений в облачных вычислениях.

Оксфордский словарь[38] предлагает точное определение, в котором Интернет рассматривается как элемент IoT:

> Интернет вещей (существительное): соединение через Интернет вычислительных устройств, встроенных в предметы повседневной жизни и обеспечивающих возможность отправки и получения данных этими устройствами.

Все эти определения описывают сценарии, в которых сетевое подключение и вычислительная способность распространяются на целую группу предметов, устройств, датчиков и повседневных предметов, которые обычно не считаются компьютерами; благодаря этому устройства могут генерировать и потреблять данные и обмениваться ими, часто при минимальном участии со стороны человека. Различные определения IoT не всегда противоречат друг другу — они скорее подчеркивают различные аспекты явления IoT с разных точек зрения и перспектив применения.

Однако различные определения могут стать источником путаницы в диалоге на тему IoT, особенно при обсуждениях между группами заинтересованных сторон или отраслевыми сегментами. Аналогичное непонимание возникло в последние годы в отношении нейтральности сети и облачных вычислений, где различные интерпретации терминов создавали барьеры для диалога. Возможно, создание единого определения IoT и не требуется, но в обсуждениях необходимо учитывать различные точки зрения.

В рамках данного документа термины «Интернет вещей» и «IoT» относятся в общем к расширению возможностей подключения к сети и вычислительных способностей для объектов, устройств, датчиков и других предметов, обычно не считающихся компьютерами. Эти «интеллектуальные предметы» требуют минимального вмешательства со стороны человека для создания, использования и обмена данными; при этом часто они имеют возможность подключения к функциям удаленного сбора, анализа и управления данными.

Модели сетевого взаимодействия и связи для интеллектуальных объектов включают в свое число и такие, в которых обмен данными не осуществляется через Интернет или сеть на основе протокола IP. Мы включаем эти модели в наше широкое определение Интернета вещей, которое используется в данном документе. Мы поступаем таким образом в связи с тем, что сгенерированные или обработанные данные, полученные от этих объектов, впоследствии передаются через шлюзы с подключением к сетям на основе протокола IP или каким-либо иным образом включаются в состав функций продукта, доступных через Интернет. Таким образом, пользователей устройств IoT, скорее всего, будут больше интересовать предоставляемые услуги и последствия их использования, чем вопрос, когда или где эти данные передаются через сеть на основе протокола IP.

Для данного документа термины «Интернет вещей» и «IOT» в целом относятся к расширению возможности сетевых подключений и вычислительной способности объектов, устройств, датчиков и других предметов, которые обычно не считаются компьютерами.

МОДЕЛИ КОММУНИКАЦИИ ИНТЕРНЕТА ВЕЩЕЙ

С практической точки зрения полезно рассмотреть, как устройства IoT осуществляют подключение и связь в соответствии со своими техническими моделями связи. В марте 2015 г. Комиссия по архитектуре Интернет (IAB) выпустила директивный документ по архитектуре для сетевого подключения интеллектуальных объектов (RFC 7452),[39] в котором определяется концептуальная основа четырех общих моделей связи, используемых устройствами IoT. Эта основа приводится в обсуждении ниже с объяснением основных характеристик каждой модели.

Подключение от устройства к устройству

Модель связи от устройства к устройству представляет два или несколько устройств, подключенных и осуществляющие связь друг с другом напрямую, а не через промежуточный сервер приложений. Эти устройства осуществляют связь через различные типы сетей, в том числе, сети на основе протокола IP или Интернет. Однако часто эти устройства используют такие протоколы, как Bluetooth,[40] Z-Wave[41] или ZigBee[42] для установления прямой связи от устройства к устройству, как показано на рисунке 1.

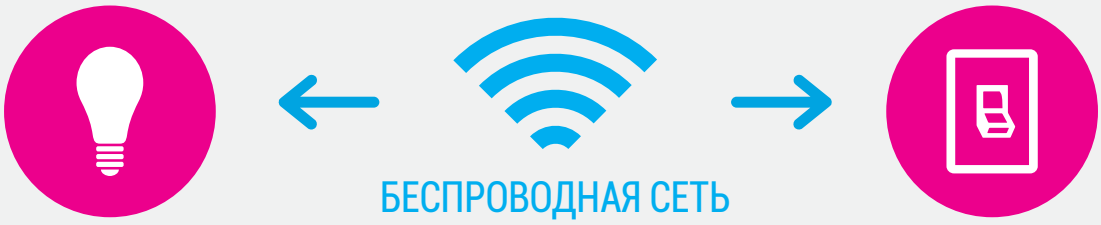
Эти сети со связью от устройства к устройству позволяют устройствам, поддерживающим определенный протокол, осуществлять связь и обмен сообщениями для выполнения своих функций. Эта модель связи обычно применяются в таких приложениях, как домашние системы автоматики, в которых обычно используются пакеты данных малого размера для установления связи между устройствами с низким уровнем требований в области скорости передачи данных. Бытовые устройства IoT, такие как лампочки, выключатели, термостаты и дверные замки, в домашней системе автоматики обмениваются малым объемом информации (например, сообщение о состоянии дверного замка или команда включения света).

Эта связь от устройства к устройству наглядно демонстрирует многие проблемы интероперабельности, которые будут рассматриваться ниже. Согласно описанию в статье, опубликованой в *IETF Journal*, «эти устройства часто находятся в непосредственной связи, обычно они оснащены встроенными [механизмами] безопасности, но также используют определенные модели данных для каждого устройства, требующие дополнительных усилий в разработке [производителями устройств]".[43] Это означает, что производители устройств должны вкладывать средства в разработку определенных форматов данных для каждого типа устройств вместо использования открытой платформы для стандартных форматов.

С точки зрения пользователей, это часто означает, что используемые протоколы передачи данных от устройства к устройству несовместимы, и в результате пользователь вынужден выбирать другие устройства, поддерживающие тот же протокол. Например, устройства, использующие протокол Z-Wave, несовместимы с устройствами семейства ZigBee. Несмотря на то, что эта несовместимость ограничивает выбор пользователя устройствами, принадлежащими к определенному семейству на основе одного и того же протокола, пользователь знает, что продукты определенного семейства работают надлежащим образом.

РИСУНОК 1

Пример модели подключения от устройства к облаку



Лампочка производителя A

Bluetooth, Z-Wave, Zigbee

Переключатель производителя B

ИСТОЧНИК: TSCHOFENIG, H. , et.al. , Architectural Considerations in Smart Object Networking. Tech. № RFC 7452. Internet Architecture Board, март 2015 г., Интернет. https://www.rfc-editor.org/rfc/rfc7452.txt.

Подключение от устройства к облаку

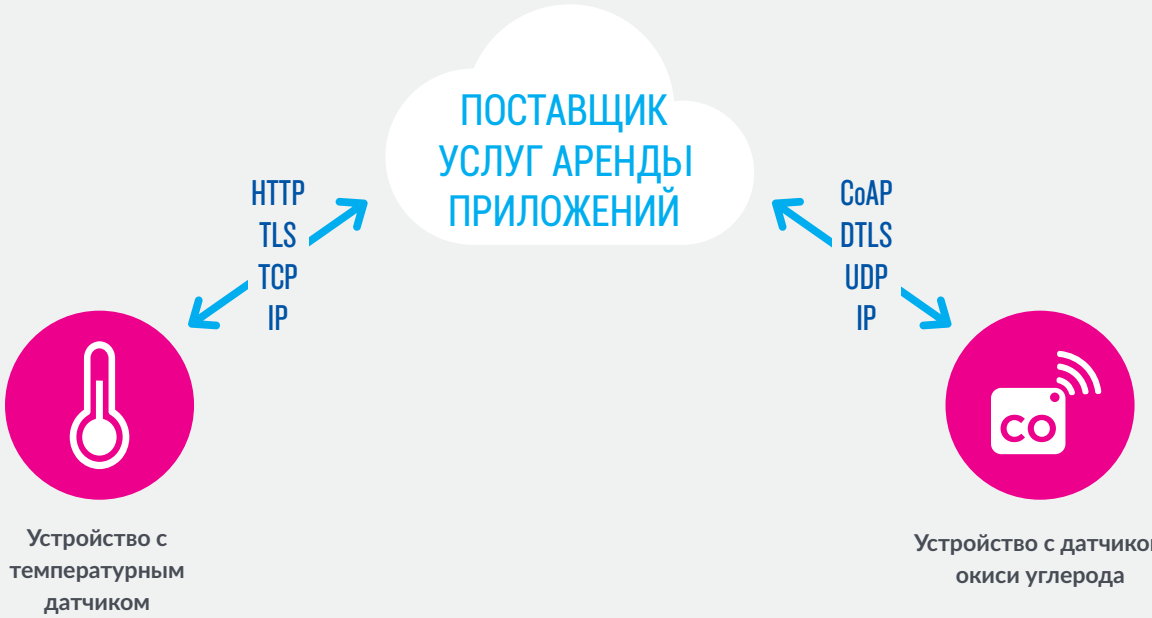
В модели связи от устройства к облаку устройство IoT подключается напрямую к облачной интернет-службе, такой как поставщик услуг аренды приложений, для обмена данными и управления трафиком сообщений. При таком подходе часто используются существующие механизмы связи, такие как традиционные проводные соединения Ethernet или Wi-Fi для установления соединения между устройством и сетью IP, которая, в свою очередь, подключается к облачной службе. Этот подход показан на рисунке 2.

Эта модель соединения используется некоторыми популярными потребительскими устройствами IoT, такими как *самообучающийся термостат Nest Labs*[44] и *SmartTV* производства Samsung.[45] В случае *самообучающегося термостата* Nest устройство передает данные в облачную базу данных, где эти данные могут использоваться для анализа потребления электроэнергии дома. Это облачное подключение позволяет пользователю получать удаленный доступ к своему термостату через смартфон или веб-интерфейс, а также поддерживает обновления программного обеспечения термостата. Аналогичным образом, в случае технологии *SmartTV* производства Samsung, телевизор использует подключение к Интернету для передачи информации о просматриваемых пользователем программах в Samsung для анализа и подключения интерактивной функции распознавания голоса на устройстве телевизора. В этих случаях модель подключения устройства к облаку обеспечивает дополнительную ценность для конечного пользователя за счет расширения стандартных функций устройства.

Тем не менее, проблемы интероперабельности могут возникнуть при попытке интеграции устройств различных производителей. Чаще всего используются облачные услуги и устройство одного производителя.[46] Если для связи между устройством и облачными службами используются патентованные протоколы данных, владелец или пользователь устройства может пользоваться лишь определенной облачной службой, что ограничивает его возможность пользоваться услугами других поставщиков. Такая ситуация обозначается термином «зависимость от поставщика», которая охватывает различные аспекты отношений с поставщиком, такие как владение данными и доступ к ним. В то же время пользователи обычно могут быть уверены в возможности интеграции устройств, созданных для определенной платформы.

РИСУНОК 2

Пример модели подключения устройства к облачной службе



ИСТОЧНИК: TSCHOFENIG, H. , et.al. , Architectural Considerations in Smart Object Networking. Tech. № RFC 7452. Internet Architecture Board, март 2015 г., Интернет. https://www.rfc-editor.org/rfc/rfc7452.txt.

Подключение от устройства к шлюзу

В случае модели подключения устройства к шлюзу или, чаще всего, в модели подключения устройства к шлюзу прикладного уровня (ALG) устройство IoT подключается через службу ALG в качестве канала для использования облачной службы. Проще говоря, это означает, что прикладное программное обеспечение функционирует на устройстве локального шлюза, которое выполняет роль посредника между устройством и облачной службой и обеспечивает безопасность и другие функции, такие как преобразование данных или протоколов. Эта модель показана на рисунке 3.

В пользовательских устройствах присутствуют различные варианты этой модели. Во многих случаях в качестве локального шлюза используется смартфон с приложением для связи с устройством и передачи данных в облачную службу. Эта модель часто используется с популярными потребительскими устройствами, такими как браслеты для занятий спортом. В этих устройствах отсутствует функция прямого подключения к облачной службе, поэтому они часто используют приложения смартфона для работы в качестве шлюза подключения.

Другой разновидностью этой модели подключения устройства к шлюзу являются устройства, выполняющие роль концентратора в приложениях домашней автоматики. Эти устройства используются в качестве локального шлюза между отдельными устройствами IoT и облачной службой, но они также могут заполнять пробелы интероперабельности между самими устройствами. Например, концентратор *SmartThings* представляет собой отдельное устройство шлюза с трансиверами Z-Wave и Zigbee, установленными для поддержания связи с обоими типами устройств.[47] Это устройство устанавливает соединение с облачной службой *SmartThings*, благодаря которому пользователь может получать доступ к устройствам с помощью приложения смартфона и подключения к Интернету.

С более широкой технической перспективы, статья в *IETF Journal* объясняет преимущества использования модели соединения устройства со шлюзом:

> Эта [модель связи] используется в тех случаях, когда интеллектуальные объекты требуют интероперабельности с устройствами, не поддерживающими [протокол Интернета] IP. Иногда этот подход используется для интеграции устройств, поддерживающих только протокол IPv6, что означает, что шлюз необходим для традиционных устройств и услуг, поддерживающих только протокол IPv4.[48]

Другими словами, эта модель связи часто используется для интеграции новых интеллектуальных устройств в традиционную систему с устройствами, которые изначально не могут с ними взаимодействовать. Недостаток этого подхода состоит в том, что необходимость разработки системы и шлюза прикладного уровня увеличивает сложность и стоимость системы в целом.

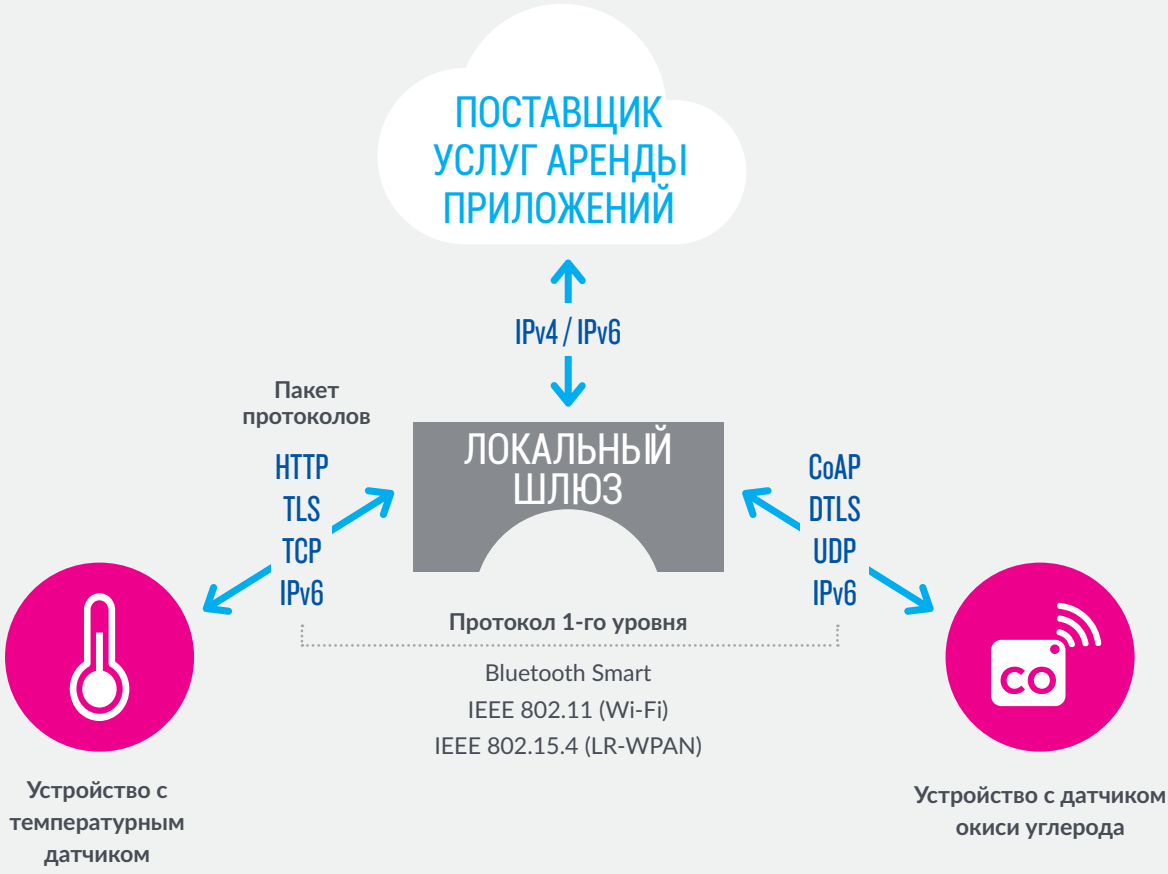
Документ IAB № RFC7452 предлагает следующий взгляд на эту модель:

> Ожидается, что в будущем будут созданы более универсальные шлюзы для снижения стоимости и уровня сложности инфраструктуры для конечных потребителей, предприятий и промышленного применения. Существование таких универсальных шлюзов более вероятно в том случае, если конструкция устройства IoT поддерживает универсальные протоколы Интернета и не требует наличия шлюза прикладного уровня для преобразования протоколов. В целом, использование шлюзов прикладного уровня приводит к более неустойчивому развертыванию, как это наблюдалось в прошлом...[49]

Системы, использующие модель соединения устройства со шлюзом, и их роль в решении проблем интероперабельности устройств IoT до сих пор находятся в процессе развития.

РИСУНОК 3

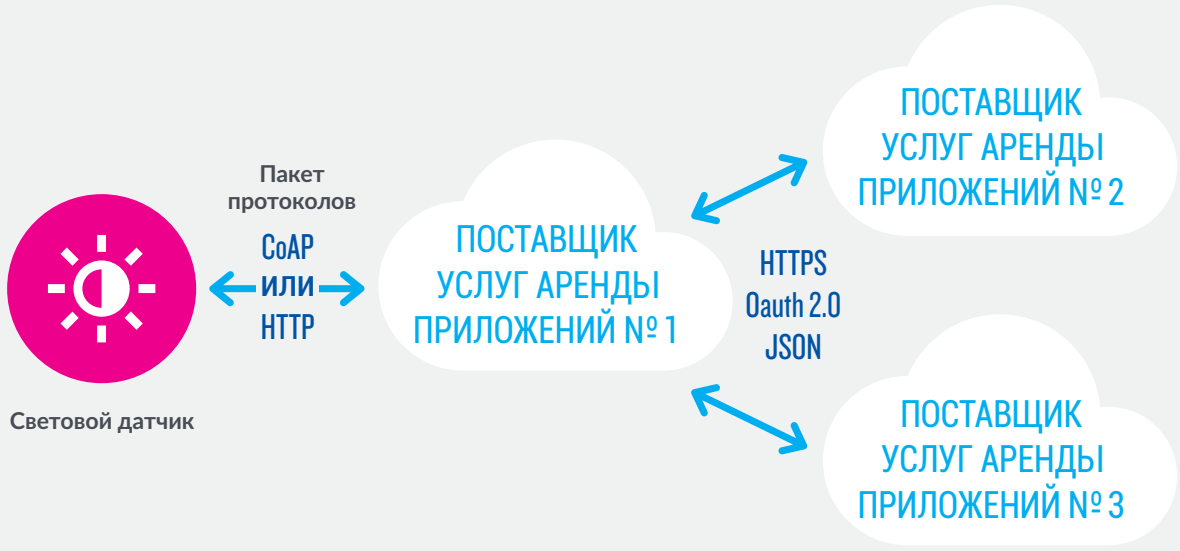
Пример модели подключения от устройства к шлюзу



ИСТОЧНИК: TSCHOFENIG, H. , et.al. , Architectural Considerations in Smart Object Networking. Tech. № RFC 7452. Internet Architecture Board, март 2015 г., Интернет. https://www.rfc-editor.org/rfc/rfc7452.txt.

РИСУНОК 4

Модель совместного использования данных на сервере



ИСТОЧНИК: TSCHOFENIG, H. , et.al. , Architectural Considerations in Smart Object Networking. Tech. № RFC 7452. Internet Architecture Board, март 2015 г., Интернет. https://www.rfc-editor.org/rfc/rfc7452.txt.

Модель совместного использования данных на сервере

Модель совместного использования данных на сервере соответствует архитектуре, позволяющей пользователям экспортировать и анализировать данные интеллектуальных объектов из облачной службы в сочетании с данными из других источников. Такая архитектура поддерживает «…желание [пользователей] предоставлять доступ третьим сторонам к загруженным данным датчиков».[50] Такой подход соответствует модели соединения отдельных устройств с облаком, которая может привести к созданию исходной базы данных, где «устройства IoT загружают данные только для одного поставщика услуг аренды приложений».[51] Архитектура совместного использования данных на сервере позволяет объединять и анализировать потоки данных, полученных от одного устройства IoT.

Например, корпоративный пользователь, ответственный за офис, может быть заинтересован в объединении и анализе данных о потреблении электроэнергии и других коммунальных услуг, получаемых всеми датчиками IoT и системами инженерного обеспечения с подключением к Интернету. В модели подключения отдельных устройств к облачным службам данные каждого датчика или системы IoT находятся в отдельной базе данных. Эффективная архитектура совместного использования данных на сервере должна позволять компании с легкостью получать доступ и анализировать облачные данные, полученные от всех устройств в здании. Кроме того, этот тип архитектуры позволяет обеспечить переносимость данных. Эффективная архитектура совместного использования данных на сервере позволяет пользователям перемещать свои данные при переключении между услугами IoT, преодолевая барьеры традиционных раздельных баз данных.

Модель совместного использования данных на сервере предполагает объединенный подход к облачным услугам;[52] в противном случае необходимы облачные интерфейсы прикладного программирования (API) для обеспечения интероперабельности размещенных на облаке данных с интеллектуальных устройств.[53] На рисунке 4 показано графическое представление этой модели.

Даная модель архитектуры представляет собой подход для обеспечения интероперабельности между этими системами на базе сервера. Как указывается в *IETF Journal*, «стандартные протоколы могут облегчить задачу, но их недостаточно для удаления узкоспециальных баз данных, так как для взаимодействия между различными производителями необходимо наличие общих информационных моделей».[54] Другими словами, эта модель связи эффективна только на основе архитектуры системы IoT. Архитектура на основе общего использования данных на сервере не может в полной мере компенсировать закрытую конструкцию системы.

Общий обзор моделей коммуникации Интернета вещей

Четыре основных модели связи демонстрируют стратегии разработки, применяемые для обеспечения связи между устройствами IoT. Помимо технических аспектов, применение этих моделей во многом определяется различиями между патентованными и открытыми устройствами IoT в сети. А в случае использования модели связи устройства со шлюзом ее основной характеристикой является ее способность преодоления ограничений при подключении патентованных устройств IoT. Это означает, что интероперабельность устройств и открытые стандарты являются ключевым условием для создания и развития взаимосвязанных систем IoT.

Эти модели связи позволяют лучше понять возможность создания дополнительной ценности для конечных пользователей с помощью сетевых устройств. Общая ценность устройств повышается за счет предоставления пользователям более удобного доступа к устройствам IoT и их данным. Например, в трех из четырех моделей связи устройства подключаются к службам анализа данных на основе облачных вычислений. За счет создания каналов передачи данных на облако пользователи и поставщики услуг могут более быстро и легко объединять данные, проводить их обширный анализ и визуализацию, а также применять технологии аналитического прогнозирования, чтобы воспользоваться дополнительными преимуществами данных IoT, получаемых с помощью традиционных приложений узкоспециальных баз данных. Другими словами, эффективные модели связи являются важным фактором для повышения ценности услуг для конечных пользователей за счет возможности применения новых способов использования информации. Однако, несмотря на эти преимущества, здесь также имеются недостатки. При выборе архитектуры необходимо тщательно учесть вопрос дополнительных затрат для пользователей при подключении к облачным ресурсам, особенно в регионах с высокой стоимостью услуг связи.

Несмотря на преимущества эффективных систем связи для пользователей, следует заметить, что эффективные модели связи IoT также способствуют развитию технических инноваций и открывают возможности коммерческого роста. Для того, чтобы воспользоваться преимуществами ранее не существовавших потоков данных IoT, могут создаваться новые продукты и услуги, выполняющие роль катализатора для дальнейших инноваций.

ВСТАВКА 3

IPv6
И ИНТЕРНЕТ ВЕЩЕЙ

Несмотря на расхождения в цифрах, большинство специалистов в области технологий сходятся во мнении, что до 2025 года к сети Интернет будут подключены миллиарды дополнительных устройств, от промышленных датчиков до бытовой техники и автомобилей. По мере развития Интернета вещей устройства, для которых требуется сквозное Интернет-соединение, не смогут использовать протокол IPv4, применяемый сейчас большинством интернет-служб. Для этого потребуется новая технология IPv6.

IPv6 – это долгожданное обновление основного исходного протокола IP, который поддерживает все соединения через Интернет. Протокол IPv6 необходим в связи с тем, что в Интернета заканчиваются уникальные адреса IPv4. Несмотря на то, что протокол IPv4 может поддерживать 4,3 млрд подключенных к Интернету устройств, IPv6 с адресами в количестве 2 в 128-й степени неисчерпаем для практического применения. Это означает около 340 триллионов триллионов триллионов адресов, более чем достаточно, чтобы удовлетворить потребности приблизительно 100 млрд устройств IoT, которые будут введены в эксплуатацию в ближайшие десятилетия.

С учетом прогнозируемого длительного срока службы некоторых датчиков и других устройств, предназначенных для Интернета, проектные решения будут влиять на удобство этих решений в течение десятилетий. Основной сложностью для разработчиков IoT является то, что протокол IPv6 изначально не интероперабелен с IPv4, и большая часть недорогого программного обеспечения для встраивания в устройства IoT использует только протокол IPv4. Тем не менее, многие специалисты считают, что IPv6 – это наилучший вариант связи, который позволит IoT полностью раскрыть свои возможности.

Дополнительную информацию о IPv6 можно найти на страницах сообщества Интернет: http://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6 и http://www.internetsociety.org/deploy360/ipv6/

ПРИМЕЧАНИЯ К РАЗДЕЛУ

Что такое Интернет вещей?

12. Эштон работал над созданием устройств радиочастотной идентификации (RFID), и тесная связь сетей RFID и других датчиков с развитием концепции IoT отражена в названии компании по производству устройств RFID, в которой Эштон работал впоследствии: “ThingMagic.”

13. “Radio-Frequency Identification.” *Wikipedia, the Free Encyclopedia*, 6 сентября 2015 г. https://en.wikipedia.org/wiki/Radio-frequency_identification

14. “Machine to Machine.” *Wikipedia, the Free Encyclopedia*, 20 августа 2015 г. https://en.wikipedia.org/wiki/Machine_to_machine

15. Polsonetti, Chantal. “Know the Difference Between IoT and M2M.” *Automation World*, 15 июля 2014 г. http://www.automationworld.com/cloud-computing/know-difference-between-iot-and-m2m

16. “The Internet Toaster.” Living Internet, 7 января 2000 г., Интернет. 6 сентября 2015 г. http://www.livinginternet.com/i/ia_myths_toast.htm

17. “The “Only” Coke Machine on the Internet.” Carnegie Mellon University Computer Science Department, n.d. Web. 6 сентября 2015 г. https://www.cs.cmu.edu/~coke/history_long.txt

18. Stafford-Fraser, Quentin. “The Trojan Room Coffee Pot.” N.p., май 1995. Интернет. 6 сентября 2015 г. http://www.cl.cam.ac.uk/coffee/qsf/coffee.html

19. RFC 7452, “Architectural Considerations in Smart Object Networking” (март 2015 г.), https://tools.ietf.org/html/rfc7452

20. Другие точки зрения на сходящиеся рыночные тенденции, обеспечивающие развитие IoT’s, включают статью Сьюзан Конант “The IoT will be as fundamental as the Internet itself” по адресу http://radar.oreilly.com/2015/06/the-iot-will-be-as-fundamental-as-the-internet-itself.html и отчет корпорации Intel на слушании Нижней палаты Конгресса США по вопросам IoT по адресу http://docs.house.gov/meetings/IF/IF17/20150324/103226/HHRG-114-IF17-Wstate-SchoolerR-20150324.pdf.

21. Закон Мура получил свое название в честь тенденции, выявленной Гордоном Муром, одним из первых исследователей в области полупроводников. Его наблюдение заключается в том, что количество транзисторов на квадратный дюйм, размещаемых на кристалле интегральной схемы, удваивается примерно каждые два года для увеличения быстродействия при одновременном уменьшении их размера.

22. На тему обсуждения потребления электроэнергии интернет-устройствами и вычислений низкой мощности см. лекцию Джона Куми (Jon Koomey) на встрече под названием “How green is the Internet?” (Насколько экологичен Интернет?), доступную для просмотра по адресу: https://www.youtube.com/embed/O8-LDLyKaBM

23. Помимо других технических достижений, закон Мура также является определяющим фактором миниатюризации электронных устройств.

24. Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, Dan Aharon “The Internet of Things: Mapping the Value Beyond the Hype”. McKinsey Global Institute, июнь 2015 г. стр. 3. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

25. *Там же.*

26. Cicciari, Matt. “What’s Missing from the Industrial Internet of Things Conversation? Software.” *Wired*. http://www.wired.com/insights/2014/11/industrial-internet-of-things-software/

27. “Internet of Things: Wearables.” Application Developers Alliance. http://www.appdevelopersalliance.org/internet-of-things/wearables/

28. Baguley, Richard, and Colin McDonald. “Appliance Science: The Internet of Toasters (and Other Things).” CNET, 2 марта 2015 г. http://www.cnet.com/news/appliance-science-the-internet-of-toasters-and-other-things/

29. “IEEE Smart Cities.” IEEE, 2015 г. Интернет. 6 сентября 2015 г. http://smartcities.ieee.org/

30. “Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 гг.” Cisco, 27 мая 2015 г. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf

31. «История Интернета – взгляд в прошлое» Postscapes, n.d. Интернет. 6 сентября 2015 г. http://postscapes.com/internet-of-things-history

32. Для получения более подробной информации об основных характеристиках Интернета и его архитектуре см. публикацию сообщества Internet Society “Internet Invariants: What Really Matters” (на английском языке), доступную по адресу: http://www.internetsociety.org/internet-invariants-what-really-matters

33. RFC 7452, “Architectural Considerations in Smart Object Networking” (март 2015 г.), https://tools.ietf.org/html/rfc7452

34. Thaler, Dave, Hannes Tschofenig, and Mary Barnes. “Architectural Considerations in Smart Object Networking.” IETF 92 Technical Plenary - IAB RFC 7452. 6 сент. 2015 г., Интернет. https://www.ietf.org/proceedings/92/slides/slides-92-iab-techplenary-2.pdf

35. “Int Area Wiki - Internet-of-Things Directorate.” *IOTDirWiki*. IETF, n.d. Web. 6 сентября 2015 г. http://trac.tools.ietf.org/area/int/trac/wiki/IOTDirWiki

36. “Overview of the Internet of Things.” ITU, 15 июня 2012 г. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060

37. http://www.comsoc.org/commag/cfp/internet-thingsm2m-research-standards-next-steps

38. “Internet of Things.” Oxford Dictionaries, n.d. Web. 6 сент. 2015 г. http://www.oxforddictionaries.com/us/definition/american_english/Internet-of-things

39. Tschofenig, H. , et. al., *Architectural Considerations in Smart Object Networking*. Tech. № RFC 7452. Internet Architecture Board, март 2015 г., Интернет. https://www.rfc-editor.org/rfc/rfc7452.txt

40. См. http://www.bluetooth.com and http://www.bluetooth.org

41. См. http://www.z-wave.com

42. См. http://www.zigbee.org

43. Duffy Marsan, Carolyn. “IAB Releases Guidelines for Internet-of-Things Developers.” *IETF Journal* 11.1 (2015): 6-8. Internet Engineering Task Force, июль 2015 г. Интернет. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

44. “Meet the Nest Thermostat | Nest.” Nest Labs. Интернет. 31 августа 2015 г. https://nest.com/thermostat/meet-nest-thermostat/

45. “Samsung Privacy Policy--SmartTV Supplement.” Корпоративная сеть Samsung 29 сент. 2015. http://www.samsung.com/sg/info/privacy/smarttv.html

46. Duffy Marsan, Carolyn. “IAB Releases Guidelines for Internet-of-Things Developers.” *IETF Journal* 11.1 (2015): 6-8. Internet Engineering Task Force, июль 2015 г. Интернет. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

47. “How It Works.” *SmartThings*, 2015 г. http://www.smartthings.com/how-it-works

48. Duffy Marsan, Carolyn. “IAB Releases Guidelines for Internet-of-Things Developers.” *IETF Journal* 11.1 (2015): 6-8. Internet Engineering Task Force, июль 2015 г. Интернет. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

49. *Tschofenig, H. , et. al.*, стр. 6.

50. *Tschofenig, H. , et. al.*, стр. 9.

51. *Там же.*

52. Подход на основе интегрированных облачных услуг объединяет ресурсы отдельных поставщиков облачных услуг для того, чтобы удовлетворить потребности более крупного бизнеса.

53. Примером общего (не IoT), готового к работе, интегрированного инструмента для совместного использования облачных услуг является *ownCloud*, созданный ownCloud.org. https://owncloud.org/blog/faster-easier-file-sync-and-share-with-federated-self-hosted-owncloud-8-0/

54. *Duffy Marsan, Carolyn.* стр. 7

КАКИЕ ВОПРОСЫ ПОДНИМАЕТ ИНТЕРНЕТ ВЕЩЕЙ?

Невозможно рассмотреть широкий спектр вопросов, касающихся Интернета вещей, в одном документе. Однако в данном разделе мы предлагаем общий обзор пяти основных областей, часто обсуждаемых в связи с IoT:

БЕЗОПАСНОСТЬ СТР. 31

КОНФИДЕНЦИАЛЬНОСТЬ СТР. 39

ИНТЕРОПЕРАБЕЛЬНОСТЬ И СТАНДАРТЫ СТР. 45

ВОПРОСЫ ЗАКОНОДАТЕЛЬСТВА, НОРМАТИВНЫХ ТРЕБОВАНИЙ И ПРАВ СТР. 53

РАЗВИВАЮЩИЕСЯ ЭКОНОМИКИ И ВОПРОСЫ РАЗВИТИЯ СТР. 61

Мы начинаем рассматривать эти вопросы через призму «Возможностей» (заявления об основополагающих принципах сообщества Интернет (ISOC) в отношении возможностей, которые должны быть доступны всем пользователям Интернета и защищены). Они включают возможности ***подключаться***, ***высказываться***, ***вводить новшества***, ***обмениваться***, ***делать выбор*** и ***доверять***.[55] Руководствуясь этими принципами, мы представляем важные аспекты каждого вопроса и выносим на обсуждение ряд проблем.

55. "Values and Principles." Principles. Internet Society, 2015 г. http://www.internetsociety.org/who-we-are/mission/values-and-principles

ВОПРОСЫ БЕЗОПАСНОСТИ

Проблема безопасности IoT

Как видно из принципов, которыми мы руководствуемся в своей работе, обеспечение безопасности, надежности, устойчивости и стабильности приложений и услуг Интернета, имеет критически важное значение для ***доверия*** и использования Интернета.[56] Как пользователи Интернета, мы должны иметь высокую степень уверенности в том, что Интернет, его приложения и подключенные к нему устройства имеют достаточно высокую степень безопасности для выполнения различных задач по отношению к допустимости риска, связанного с их выполнением. Интернет вещей ничем не отличается в этом отношении, и безопасность IoT связана, в основном, с доверием к среде со стороны пользователей. Если люди не верят в защищенность подключенных устройств и полученной информации от недопустимого использования, этот недостаток доверия приводит к отказу от использования Интернета. Этот фактор оказывает глобальное влияние на электронную коммерцию, технические инновации, свободу высказываний и практически все остальные аспекты деятельности онлайн. Обеспечение безопасности продуктов и услуг IoT должно быть основным приоритетом в данной отрасли.

По мере постоянного увеличения числа устройств, подключенных к Интернету, возникают новые потенциальные уязвимые места. Недостаточно защищенные устройства могут служить точками доступа для кибератак, позволяя злоумышленникам перепрограммировать устройство или вызывать его неисправность. Устройства несовершенной конструкции могут подвергать данные пользователей опасности хищения за счет недостаточной защиты потоков данных. Неисправные или дефектные устройства также могут создавать уязвимые точки. Для распространенных недорогих устройств небольшого размера эти проблемы стоят столь же остро или даже еще острее, чем для компьютеров, которые традиционно использовались для подключения к Интернету. Конкурентоспособная стоимость и технические ограничения устройств IoT вынуждают производителей встраивать в эти устройства соответствующие функции безопасности, чтобы обеспечить уровень безопасности и долгосрочной защиты уязвимых мест, превышающий аналогичные характеристики компьютеров.

Помимо потенциальных уязвимых мест, существенное увеличение количества и типов устройств IoT также может способствовать увеличению вероятности кибератак. С учетом функции взаимоподключения устройств IoT, каждое подключенное устройство, не имеющее достаточной защиты, оказывает потенциально отрицательное влияние на безопасность и устойчивость Интернета *в глобальном масштабе*, а не только локально. Например, незащищенный холодильник в США, зараженный вредоносным программным обеспечением, может отправлять тысячи вредоносных сообщений электронной почты получателям во всем мире с помощью домашнего подключения Wi-Fi.[57]

И в довершение всего, в гиперподключенном мире наша способность выполнять ежедневные задачи без помощи устройств или систем с подключением к Интернету, будет снижаться. Сейчас становится все труднее приобрести устройства *без* подключения к Интернету, потому что некоторые поставщики производят только подключенные продукты. Каждый день степень нашей подключенности растет и мы становимся все более зависимыми от устройств IoT для выполнения основных задач. Необходимо, чтобы устройства были защищенными, с учетом того, что никакое устройство не может быть полностью безопасным. Этот повышающийся уровень зависимости от устройств IoT и интернет-услуг, с которыми они взаимодействуют, также открывает злоумышленникам возможности доступа к устройствам. Допустим, мы можем отключить подключенный к Интернету телевизор, если он подвергнется кибератаке, но мы не сможем также просто выключить электросчетчик или систему регулировки движения транспорта либо вживленный кардиостимулятор.

Именно поэтому безопасность устройств и услуг IoT является основой темой обсуждений и должна быть признана критически важной проблемой. Мы все в большей степени зависим от этих устройств для выполнения важных повседневных задач, и их поведение может оказывать глобальное воздействие.

Любое подключенное устройство, не имеющее достаточного уровня безопасности, может отрицательно повлиять на безопасность и устойчивость Интернета в глобальном, а не только в местном масштабе.

Аспекты безопасности

Говоря об устройствах, подключенных к Интернету вещей, необходимо понимать, что их безопасность не является абсолютной. Безопасность устройства IoT не определяется бинарным понятием защищенности или незащищенности. Безопасность IoT следует рассматривать скорее как диапазон уязвимости устройства. Этот диапазон охватывает как незащищенные устройства, не имеющие функций безопасности, до в высшей степени безопасных систем с несколькими уровнями защиты. В этой бесконечной игре в кошки-мышки постоянно возникают новые угрозы безопасности, и производители устройств и сетевые операторы постоянно принимают меры для защиты от этих угроз.

Безопасность и устойчивость Интернета вещей – это эффективность оценки рисков и их устранения. Безопасность устройства – это функция управления риском того, что устройство будет взломано, возникшим в результате ущербом, а также временем и ресурсами для обеспечения необходимого уровня защиты. Для пользователей, которые не могут позволить себе высокую степень риска для безопасности, как в случае оператора системы регулировки движения транспорта или человека с медицинским устройством, подключенным через Интернет, может быть целесообразно потратить значительное время и ресурсы для защиты системы или устройства от кибератак. Аналогичным образом, если пользователя не беспокоит возможность взлома его холодильника и его использования для отправки спама, он не захочет платить за более сложную систему безопасности, если она увеличит стоимость устройства или сделает его более сложным в работе.

На эту оценку рисков и возможных последствий влияет целый ряд факторов. Эти факторы включают в себя наличие четкого понимания существующих рисков безопасности и потенциальных рисков в будущем; Приблизительные экономические и другие последствия в случае осуществления рисков; А также приблизительную стоимость устранения их последствий.[58] Несмотря на то, что это соотношение плюсов и минусов в области безопасности часто рассматривается с точки зрения отдельного пользователя или организации, необходимо также учитывать взаимосвязь устройств IoT как части более обширной экосистемы IoT. Функция сетевого подключения устройств IoT означает, что решения в области безопасности, принимаемые на месте в отношении какого-либо устройства IoT, могут оказывать глобальное воздействие на другие устройства.

С принципиальной точки зрения, разработчики интеллектуальных предметов для Интернета вещей обязаны гарантировать, что эти устройства не будут подвергать опасности своего владельца или других людей. С точки зрения бизнеса и экономики производители заинтересованы в уменьшении затрат, снижении уровня сложности и сокращении времени до выпуска на рынок. Например, становятся все более распространенными устройства IoT, представляющие собой компоненты массового выпуска с низким уровнем прибыли, сами по себе являющиеся добавочной стоимостью продукта, в который они встроены; наращивание объема памяти или установка более быстрого процессора может сделать эти продукты неконкурентоспособными с коммерческой точки зрения.

С точки зрения экономики, недостаточный уровень безопасности устройств IoT приводит к отрицательным внешним последствиям, где затраты возлагаются одной стороной (или сторонами) на другие. Классическим примером является загрязнение окружающей среды, где ущерб и затраты на очистку (отрицательные внешние последствия) в результате действий нарушителей несут другие стороны. Проблема в том, что затраты на решение внешних проблем, возлагаемые на других, обычно не учитывается в процессе принятия решений, за исключением тех случаев, когда, как в случае с загрязнением, на нарушителя налагается штраф с целью заставить его снизить уровень загрязнений. В случае информационной безопасности, как указывается в описании Брюса Шнайера,[59] внешние проблемы возникают в тех случаях, когда производитель продукта не несет ответственность за затраты в результате недостаточного уровня безопасности; В этом случае закон об ответственности может заставить производителей принимать во внимание внешние проблемы и выпускать продукты с более высоким уровнем безопасности.

Эти требования безопасности не являются новыми в области информационных технологий, но масштаб уникальных проблем, которые могут возникнуть с внедрением IoT, делает их весьма существенными.

Уникальные проблемы безопасности устройств IoT

Устройства IoT обычно отличаются от традиционных компьютеров и вычислительных устройств в очень важных аспектах, представляющих угрозу безопасности:

Многие устройства, подключенные к Интернету вещей, такие как датчики и предметы бытовой техники, предназначены для массового развертывания, сопоставимого с числом традиционных устройств, подключенных к Интернету. В результате потенциальное число взаимных подключений между этими устройствами является беспрецедентным. Кроме того, многие из этих устройств смогут самостоятельно устанавливать связь друг с другом непредсказуемым и динамическим способом. Таким образом, может потребоваться пересмотреть существующие инструменты, методы и стратегии, связанные с безопасностью IoT.

Многие системы IoT будут состоять из групп идентичных или почти идентичных устройств. Такая однородность усиливает потенциальное воздействие каждой уязвимости, умножая его на количество устройств, имеющих те же характеристики. Например, уязвимость протокола связи лампочек бренда одной компании с подключением к Интернету может распространиться на все марки и модели устройств, использующих тот же протокол или имеющих аналогичную конструкцию.

Развертывание многих устройств, подключенных к Интернету вещей, будет осуществляться с учетом срока эксплуатации, на много лет превышающего обычные сроки для высокотехнологичного оборудования. Развертывание этих устройств может осуществляться в условиях, затрудняющих или делающих невозможной их модернизацию или изменение конфигурации; Либо эти устройства могут пережить своего производителя и остаться без технической поддержки в долгосрочной перспективе. Такие сценарии демонстрируют то, что механизмы безопасности, работающие в момент развертывания, могут быть непригодны для всего срока службы устройств по мере появления новых угроз. В результате, это может привести к появлению уязвимостей, которые будут сохраняться в течение длительного времени. Это идет вразрез с парадигмой традиционных компьютерных систем, модернизация которых осуществляется путем обновлений операционной системы на протяжении всего срока службы компьютера для устранения угроз безопасности. Техническая поддержка в долгосрочной перспективе и управление устройствами IoT представляют собой серьезную проблему безопасности.

Многие устройства IoT изначально не предполагают возможности обновления либо эта процедура слишком неудобна и непрактична. В качестве примера можно взять отзыв 1,4 млн автомобилей Fiat Chrysler в 2015 году для устранения уязвимости, благодаря которой злоумышленник смог взломать автомобиль с помощью беспроводной сети. Эти автомобили необходимо передать дилеру Fiat Chrysler для установки обновлений вручную, либо владелец автомобиля должен установить обновления самостоятельно с помощью ключа USB. Правда заключается в том, что эти обновления с большой вероятностью не будут установлены на значительный процент этих автомобилей, так как процесс обновления неудобен для пользователей, в результате чего они постоянно подвергаются опасности кибератак, особенно если автомобиль во всех остальных аспектах работает исправно.

Многие устройства IoT работают таким образом, что пользователь не имеет или почти не имеет представления о внутреннем функционировании устройства или создаваемых им потоках данных. Это создает уязвимость в области безопасности, когда пользователь считает, что устройство IoT выполняет определенные функции, в то время как на самом деле оно может выполнять нежелательные действия или собирать данные, которые пользователь не намерен предоставлять. Функции устройства также могут изменяться без предупреждения при обновлении, в результате чего пользователь подвергается опасности в результате любых изменений, вносимых производителем.

Некоторые устройства IoT устанавливаются в таких местах, где трудно или даже невозможно обеспечить их физическую безопасность.

Злоумышленники могут получить прямой физический доступ к устройству. В связи с этим, для обеспечения безопасности необходимы функции защиты от взлома и другие инновации.

Некоторые устройства IoT, такие как датчики состояния окружающей среды, незаметно встраиваются в элементы окружения, где пользователь не замечает устройство и не может контролировать его работу. Кроме того, устройства могут не иметь функции предупреждения пользователя о возникновении проблем безопасности, в результате чего пользователь может не знать о наличии угрозы безопасности в устройстве IoT. Уязвимость может сохраняться в течение длительного времени до того, как она будет замечена и исправлена, в том случае, если исправление или смягчение последствий является в принципе возможным или целесообразным. Аналогичным образом, пользователь может даже не знать, что поблизости имеется датчик, в результате чего уязвимость может оставаться незамеченной в течение долгого времени.

Первые модели, подключенные к Интернету вещей, основаны на предпосылке, что IoT будет продуктом крупных частных и/или государственных технологических предприятий, но в будущем создание своего собственного Интернета вещей (BYIoT) может стать обычной практикой, как это демонстрируют развивающиеся сообщества разработчиков Arduino и Raspberry Pi.[60] И в этом случае передовые отраслевые стандарты безопасности могут не всегда применяться.

Вопросы безопасности IoT

В отношении проблем безопасности, связанных с Интернетом вещей, был поднят целый ряд вопросов. Многие из этих вопросов существовали еще до развития IoT, но теперь стали более острыми в связи с крупномасштабным развертыванием устройств IoT. Вот некоторые из основных вопросов:

ОБЩЕПРИНЯТЫЕ НОРМЫ ПРОЕКТИРОВАНИЯ

Каковы общепринятые нормы проектирования для инженеров и разработчиков при создании более безопасных устройств IoT? Каким образом проблемы безопасности Интернета вещей были проанализированы и приняты во внимание сообществами разработчиков для улучшения качества устройств следующего поколения? Какие имеются образовательные и учебные ресурсы для подготовки инженеров и разработчиков устройств IoT?

СООТНОШЕНИЕ СТОИМОСТИ И БЕЗОПАСНОСТИ

Каким образом заинтересованные стороны принимают решения на основе информации о соотношении затрат и преимуществ применительно к Интернету вещей? Как точно оценить количество и степень рисков безопасности? Что может мотивировать разработчиков и производителей устройств включить функции безопасности в затраты на производство и принять на себя ответственность за какие-либо внешние проблемы, ставшие результатом их решений в отношении безопасности? Каким образом можно совместить функциональность и удобство использования с безопасностью? Как обеспечить техническую поддержку в области безопасности IoT для инноваций, социального и экономического развития?

СТАНДАРТЫ И ПОКАЗАТЕЛИ

Какова роль технических и эксплуатационных стандартов в развитии и развертывании надежных и безопасных устройств IoT? Как эффективно определить и измерить параметры безопасности устройства IoT? Как оценить эффективность мер безопасности и средств профилактики в отношении Интернета вещей? Как обеспечить применение передовых методов в области безопасности?

КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ, ПРОВЕРКА ПОДЛИННОСТИ И КОНТРОЛЬ ДОСТУПА

Какова оптимальная роль шифрования данных для устройств IoT? Являются ли технологии шифрования, проверки подлинности и контроля доступа подходящим решением для предотвращения перехвата потока данных этих устройств? Какие технологии шифрования и проверки подлинности могут быть адаптированы для Интернета вещей, и как их можно внедрить с учетом ограничений, связанных со стоимостью, размером устройств IoT и их скоростью обработки данных? Каковы прогнозируемые проблемы управления, которые должны быть решены с помощью шифрования на уровне IoT? Будут ли решены проблемы контроля жизненного цикла криптоключей и ожидаемого периода, в течение которого каждый алгоритм остается безопасным? Достаточно ли надежны и просты процессы сквозной защиты для использования рядовыми потребителями?

ВОЗМОЖНОСТЬ ОБНОВЛЕНИЯ НА МЕСТЕ УСТАНОВКИ

Должны ли устройства, многие из которых, как предполагается, должны иметь длительный срок службы, разрабатываться с учетом возможности ремонта и обновления для адаптации к растущим угрозам безопасности? Если бы каждое периферийное IoT-устройство имело встроенный модуль управления устройствами, централизованная система управления безопасностью могла бы устанавливать в них новое программное обеспечение и осуществлять настройку параметров. Но системы управления увеличивают расходы и сложность. Могут ли применяться другие подходы для обновления программного обеспечения в условиях широкого использования IoT-устройств? Существуют ли какие-либо классы IoT-устройств, представляющие меньший риск и поэтому не имеющие таких функций? Проводится ли тщательное изучение (кем угодно, включая пользователей) пользовательских интерфейсов IoT-устройств (обычно преднамеренно минимальных) с точки зрения управления устройствами?

ОБЩАЯ ОТВЕТСТВЕННОСТЬ

Как побудить заинтересованные стороны к совместной ответственности и сотрудничеству в области IoT-безопасности?

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Следует ли привлекать к ответственности производителей устройств за продажу программного и аппаратного обеспечения с известными или неизвестными проблемами безопасности? Как адаптировать или расширить законы об ответственности за качество выпускаемой продукции и защиту потребителя, чтобы справиться с любыми отрицательными внешними эффектами, связанными с Интернетом вещей, и будут ли они работать в условиях транснациональных потоков? Можно ли добиться того, чтобы законодательство не отставало и оставалось эффективным в условиях быстрого развития IoT-технологий и увеличения угроз безопасности? Как сбалансировать законодательство для учета потребностей в инновациях, не требующих разрешения, а также в условиях свободы Интернета и свободы слова?

УСТАРЕВАНИЕ УСТРОЙСТВ

Какой подход следует использовать по отношению к устаревшим IoT-устройствам в условиях быстрого развития Интернета и изменения качества угроз безопасности? Должны ли IoT-устройства иметь встроенную функцию выхода из эксплуатации для их блокирования по истечении срока службы? Это требование может привести к тому, что старые неинтероперабельные устройства будут отключаться и заменяться более безопасными и интероперабельными устройствами в будущем. Конечно, это может оказаться весьма затруднительным в условиях открытого рынка. Каковы последствия автоматического вывода из эксплуатации IoT-устройств?

Масштаб этих проблем отражает серьезные беспокойства, связанные с безопасностью IoT-устройств. Но важно не забывать, что если устройство *подключено к* Интернету, оно также является *частью Интернета*,[61] а это значит, что эффективные и приемлемые решения по обеспечению безопасности могут быть приняты, только если участники рынка, имеющие отношение к этим устройствам, примут на вооружение совместный подход к безопасности.[62]

Совместный подход уже проявил свою эффективность среди представителей индустрии, правительств и государственных органов при решении проблем безопасности Интернета и киберпространства, включая Интернет вещей. Эта модель включает в себя разнообразные подходы и инструменты, в том числе добровольный двусторонний обмен информацией, эффективные инструменты контроля над выполнением требований, готовность к чрезвычайным ситуациям и виртуальное обучение, информирование и просвещение, принятие соглашений о международных нормах поведения, а также разработка и внедрение международных стандартов и практик. Мы должны постоянно прилагать усилия для разработки подходов совместной ответственности и управления рисками с учетом масштабов и сложности проблем безопасности IoT-устройств будущего.

ПРИМЕЧАНИЯ К РАЗДЕЛУ

Вопросы безопасности

56. "Values and Principles". *Principles*. Internet Society, 2015 г. http://www.internetsociety.org/who-we-are/mission/values-and-principles

57. Мишель Старр. «Холодильник "поймали" за рассылкой спама через ботнет». CNET, 19 января 2014 г. http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

58. Многие организации разработали правила проведения оценки рисков. Например, Национальный институт стандартов и технологий США (NIST) выпустил набор инструкций в 2012 году, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091, а Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (МЭК) выпустили стандарт ISO/IEC 31010:2009 «Управление риском. Методы оценки риска». http://www.iso.org/iso/catalogue_detail?csnumber=51073

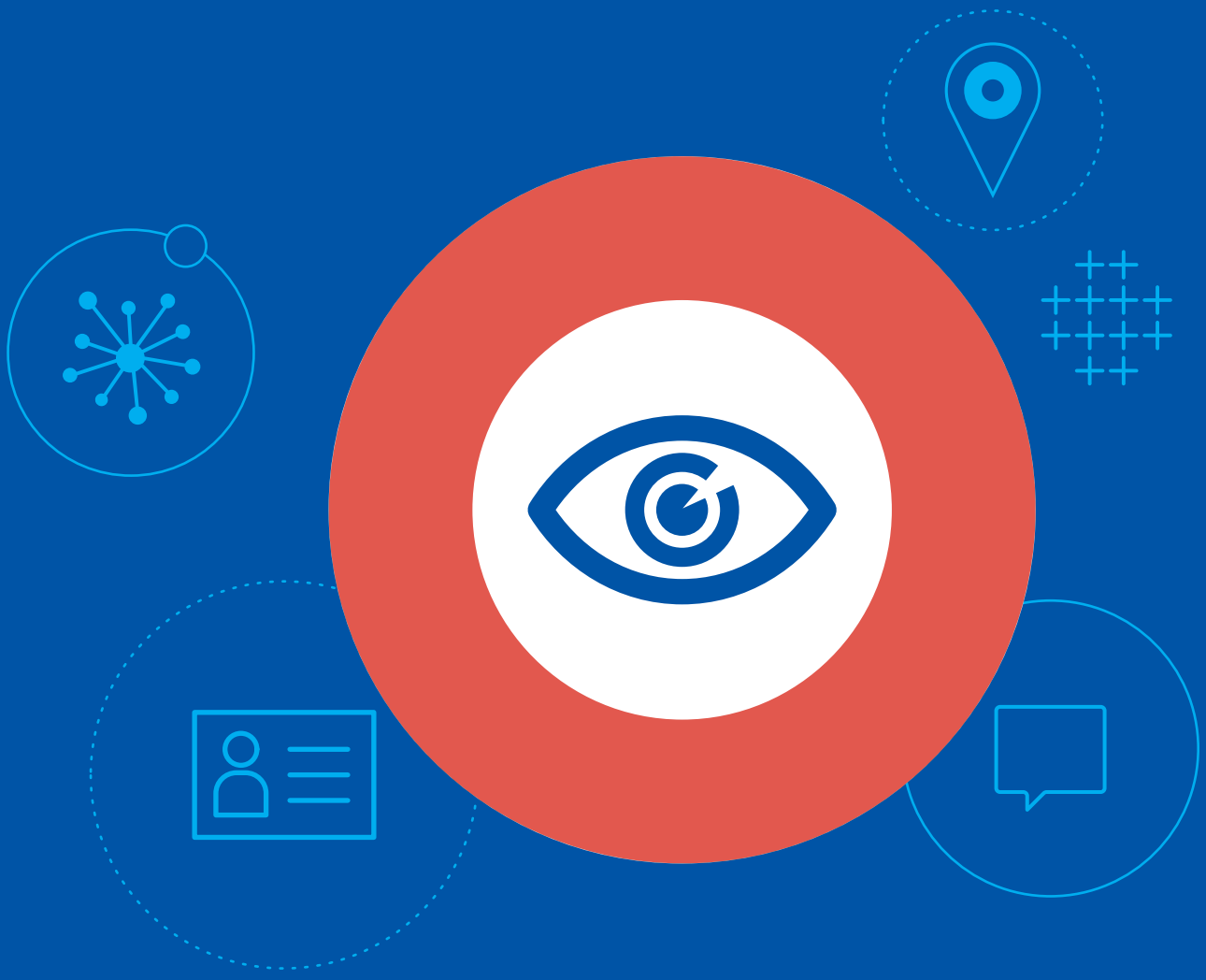
59. См. онлайн-статью Брюса Шнайдера на веб-сайте https://www.schneier.com/essays/archives/2007/01/information_security_1.html

60. См. веб-сайт сообщества разработчиков программного обеспечения с открытым кодом Arduino: http://www.arduino.cc, а также веб-сайт Raspberry Pi Foundation http://www.raspberrypi.org/

61. Олаф Колькман. «Мир совместной безопасности: наш подход к проблемам Интернет-безопасности». Статья в веб-журнале. Internet Society, 13 апреля 2015 г. http://www.internetsociety.org/blog/public-policy/2015/04/introducing-collaborative-security-our-approach-internet-security-issues

62. *Совместная безопасность: подход к решению проблем Интернет-безопасности*. Internet Society, апрель 2015 г. http://www.internetsociety.org/collaborativesecurity

АСПЕКТЫ КОНФИДЕНЦИАЛЬНОСТИ



Общие аспекты конфиденциальности Интернета вещей

Соблюдение права на неприкосновенность частной жизни и предпочтений конфиденциальности является неотъемлемой частью решения проблемы доверия к Интернету, и оно также влияет на возможность людей ***говорить***, ***подключаться***, ***выбирать*** – и делать это продуктивно. Эти права и ожидания иногда сводятся к проблеме этичной обработки данных, подчеркивая важность удовлетворения ожиданий соблюдения прав конфиденциальности и добросовестного использования данных.[63] Интернет вещей способен поставить под вопрос эти традиционные ожидания соблюдения прав частной жизни.

Проблемы конфиденциальности, возникшие с появлением Интернета вещей, очень важно решить, так как они касаются основных прав человека и способности нашего общества доверять Интернету и подключенным к нему устройствам.

Интернет вещей часто представляется масштабной сетью сенсорных устройств, которые собирают данные об окружении и нередко – о людях. Конечно, эти данные могут быть полезными для владельцев устройств, но очень часто они представляют интерес и для производителей и поставщиков устройств. Сбор и использование IoT-данных превращается в настоящую проблему конфиденциальности, когда представления людей, находящихся под наблюдением IoT-устройств, о масштабе и использовании данных, отличаются от соображений сборщика данных.

Кажущиеся безобидными комбинации потоков IoT-данных также могут угрожать конфиденциальности. При объединении или сопоставлении нескольких потоков данных иногда можно получить более точный цифровой портрет человека, чем при использовании одного потока IoT-данных. Например, подключенная к Интернету зубная щетка может записывать и передавать безобидные данные о том, как ее владелец чистит зубы. Но если его холодильник передает данные о том, что он ест, а фитнес-трекер передает данные об его физической активности, то комбинация этих потоков позволяет получить более детальное и точное описание общего состояния здоровья этого человека. Этот эффект группирования данных может быть особенно справедливым в отношении IoT-устройств, так как многие устройства генерируют дополнительные метаданные (например, время и местоположение), которые позволяют получить более конкретную информацию о человеке.

В других ситуациях пользователь может не знать, что IoT-устройство собирает данные о нем и способно передавать их третьим сторонам. Этот тип сбора данных получает все более широкое распространение в области бытовых устройств, таких как «умные телевизоры» и игровые приставки. Такие устройства оснащены функцией распознавания голоса и изображения и поэтому могут непрерывно прослушивать или просматривать происходящее в помещении и активно передавать эти данные в облачный сервис для дальнейшей обработки, и в этом процессе иногда задействованы третьи стороны. Человек может находиться в окружении подобных устройств, не подозревая о том, что его разговоры или действия отслеживаются, а данные записываются. Такого рода функции могут не только приносить пользу осведомленным пользователям, но и создавать проблемы конфиденциальности тем, кто не подозревает о присутствии этих устройств и не может контролировать использование собранных данных.

Независимо от того, известно ли это пользователю и согласен ли он с тем, что его данные собираются и анализируются, подобные ситуации лишь подчеркивают ценность персонализированных потоков данных для компаний и организаций, стремящихся собирать и записывать IoT-данные. Потребность в этих данных приводит к появлению юридических и нормативных проблем, связанных с законами о защите и конфиденциальности данных.

Эти проблемы конфиденциальности важно решить, так как они влияют на основные права человека и его способность доверять Интернету. В целом люди осознают, что их частная жизнь действительно представляет ценность, и у них есть ожидания в том, что касается сбора и использования данных третьими сторонами. Это общее представление о неприкосновенности частной жизни касается и данных, собираемых IoT-устройствами, но эти устройства могут угрожать возможности пользователя выражать и добиваться соблюдения его прав на частную жизнь. Если пользователь потеряет доверие к Интернету из-за несоблюдения его прав на частную жизнь в Интернете вещей, общая ценность Интернета может уменьшиться.

Уникальные аспекты конфиденциальности Интернета вещей

В целом проблемы конфиденциальности усугубляются тем, что Интернет вещей значительно расширяет возможности и доступность отслеживания и наблюдения. Характеристики IoT-устройств и методы их использования направляют дискуссии о проблемах конфиденциальности в новое русло, так как они серьезно меняют методы сбора, анализа, использования и защиты персональных данных. Пример:

Традиционная Интернет-модель «ознакомления и согласия» с политиками конфиденциальности, где пользователи выражают свое отношение путем интерактивного взаимодействия с информацией на компьютерном или мобильном экране (например, путем нажатия кнопки «Принять»), не срабатывает, когда системы не предлагают механизма взаимодействия пользователя с системой. IoT-устройства часто не имеют пользовательского интерфейса для изменения настроек конфиденциальности, и во многих случаях пользователи не знают или не умеют контролировать сбор или использование личных данных. Это создает разрыв между предпочтениями пользователя и действиями IoT-устройств по сбору данных. Поставщики IoT-устройств могут не быть заинтересованы в предоставлении пользователям механизма для выражения своих предпочтений, если считают, что собираемые данные не носят личного характера. Однако опыт показывает, что данные, которые традиционно не считаются личными, на самом деле могут стать таковыми, если их объединить с другими данными.

Если мы сможем разработать эффективный механизм для IoT-устройств, позволяющий пользователю осознанно выражать свои предпочтения конфиденциальности, этот механизм должен охватывать большое количество IoT-устройств, которые должен контролировать пользователь. Нереально ожидать, что пользователь будет напрямую взаимодействовать с каждым IoT-устройством, с которым он сталкивается в течение дня, чтобы выразить свои предпочтения конфиденциальности. Вместо этого механизмы интерфейса конфиденциальности должны подстраиваться под размер проблемы IoT, но при этом оставаться достаточно функциональными и практичными с точки зрения пользователя.

Интернет вещей может изменить ожидания человека о соблюдении прав на частную жизнь в обычных ситуациях. Существуют социальные нормы и ожидания в том, что касается прав на частную жизнь, отличающиеся в общественных местах и личных пространствах, и IoT-устройства ставят эти нормы под вопрос. Например, IoT-технологии наблюдения (например, камеры наблюдения или системы отслеживания местоположения), устанавливаемые обычно в общественных местах, переходят в традиционно личные пространства (например, в дом или личный автомобиль), где ожидания к соблюдению прав на частную жизнь совершенно другие. При этом ставится под вопрос то, что во многих обществах рассматривается как «право на уединение» в доме или личном пространстве. Кроме того, права на частную жизнь в местах, которые считаются общественными (парки, магазины, вокзалы и т.д.), ставятся под вопрос из-за увеличения природы и масштаба наблюдения в этих местах.

IoT-устройства часто используются в условиях, где многолюдность приводит к сбору одних и тех же данных о множестве людей. Например, геолокационный датчик в автомобиле записывает данные о местоположении всех, кто находится в автомобиле, независимо от их желания. Он может отслеживать даже людей в соседних автомобилях. В подобных ситуациях бывает трудно или невозможно разграничить или учесть индивидуальные предпочтения конфиденциальности.

Аналитика больших данных, применяемая к сгруппированным персональным данным, уже начала представлять риск вмешательства в частную жизнь и потенциальной дискриминации. Этот риск усиливается в Интернете вещей за счет масштаба и большей

узнаваемости собираемых личных данных. IoT-устройства могут собирать данные о человеке с беспрецедентной точностью и навязчивостью; группировка и корреляция этих данных может создать детальный портрет индивидуума, что создает возможности для дискриминации и нанесения иного вредя. Изощренность этой технологии может привести к ситуациям, угрожающим здоровью, благополучию, финансам или репутации человека.

Повсеместность, близость и социальный охват множества IoT-устройств может вести к ложному чувству защищенности и заставлять людей разглашать секретные или личные данные, не осознавая и не оценивая в полной мере возможных последствий своих действий.

Вопросы конфиденциальности IoT

Проблемы конфиденциальности могут оказаться слишком сложными для решения, даже если полностью учесть интересы и мотивы всех участников экосистемы Интернета вещей. Но мы знаем, что могут существовать несбалансированные или недобросовестные отношения и интересы между теми, чьи персональные данные собирают, и теми, кто собирает, анализирует и использует эти данные. Источник данных может испытать нежелательное вторжение в частную жизнь, зачастую без его согласия, выбора или ведома. Но лицо, собирающее эти данные, может считать это полезным ресурсом, способным увеличить доход от продуктов и услуг, а также предложить новые источники дохода.

Так как IoT создает новые угрозы для наших представлений о конфиденциальности, важно задать основные вопросы при переоценке моделей конфиденциальности в условиях IoT. В круг этих вопросов входят:

ЗАКОННОСТЬ СБОРА И ИСПОЛЬЗОВАНИЯ ДАННЫХ

Как решить проблему рыночных отношений между источниками данных и сборщиками данных в условиях IoT? Персональные данные имеют личную и коммерческую ценность, которая оценивается источниками и сборщиками по-разному как индивидуально, так и в группе; обе стороны имеют законные интересы, которые могут противоречить один другому. Как выразить эти различающиеся интересы, чтобы разработать правила, справедливые и разумные как для источника, так и для сборщика данных в том, что касается доступа, контроля, прозрачности и защиты?

ПРОЗРАЧНОСТЬ, ВЫРАЖЕНИЕ И УЧЕТ ПРЕДПОЧТЕНИЙ КОНФИДЕНЦИАЛЬНОСТИ

Как сделать политику и практику соблюдения конфиденциальности легкодоступными и понятными в условиях IoT? Какие альтернативы традиционной модели конфиденциальности («ознакомления и согласия») могут использоваться для решения уникальных вопросов Интернета вещей? Какая эффективная модель может использоваться для выражения, применения и соблюдения индивидуальных предпочтений конфиденциальности и многосторонних предпочтений? Возможно ли построить такую многостороннюю модель, и если да, то как она будет выглядеть? Как применить ее в особых условиях, касающихся индивидуальных предпочтений конфиденциальности? Существует ли рынок для передачи управления настройками безопасности коммерческим сервисам, предназначенным для реализации предпочтений пользователя? Существует ли стороннее средство соблюдения конфиденциальности, способное выражать предпочтения пользователя и обеспечивать их соблюдение по всему спектру устройств, исключая при этом потребность в прямом взаимодействии с каждым из них?

РАЗЛИЧИЕ ОЖИДАНИЙ ПРИВАТНОСТИ

Нормы и предпочтения конфиденциальности тесно связаны с социальной и культурной средой пользователя, которая будет различаться в различных группах и странах. Многие IoT-сценарии включают в себя действия по использованию устройств и сбору данных в многонациональном или глобальном масштабе с пересечением социальных и культурных границ. Что это значит с точки зрения разработки широко применимой модели защиты конфиденциальности в условиях Интернета вещей? Как можно адаптировать IoT-устройства и системы, чтобы различать и соблюдать различные предпочтения конфиденциальности пользователей и законы?

ПРОЕКТИРУЕМАЯ КОНФИДЕНЦИАЛЬНОСТЬ

Как заинтересовать производителей IoT-устройств во внедрении принципов проектируемой конфиденциальности в их основные ценности? Как стимулировать включение предпочтений конфиденциальности пользователей в каждый этап разработки и эксплуатации продукта? Как сбалансировать функциональность и требования конфиденциальности? В целом производителям следует ожидать, что продукты и практики, не нарушающие права на частную жизнь, позволяют добиться долгосрочного доверия пользователей, удовлетворенности и лояльности к бренду. Является ли это достаточной мотивацией по сравнению с обратным стремлением к простоте разработки и скорости выхода на рынок? Должны ли устройства разрабатываться с настройками, по умолчанию предусматривающими самый консервативный режим сбора данных (что означает отказ от сбора данных по умолчанию)?

ИДЕНТИФИКАЦИЯ

Как защищать данные, собранные IoT-устройствами, которые в момент сбора не кажутся личными или были «обезличены», но могут быть в будущем превращены в личные данные (например, путем повторной идентификации данных или их комбинации с другими данными)?

Интернету вещей свойственны специфические проблемы конфиденциальности, выходящие за рамки существующих проблем неприкосновенности частной жизни. Необходимо разработать стратегии по соблюдению индивидуальных предпочтений конфиденциальности по всему широкому спектру ожиданий, продолжая при этом стимулировать инновации в новой сфере IoT-технологий.

ПРИМЕЧАНИЯ К РАЗДЕЛУ

Аспекты конфиденциальности

63. Робин Уилтон. *CREDS 2014 –Документ о позиции: четыре этические проблемы доверия Интернету.* Краткий отчет № CREDS-PP-2.0. Internet Society, 2014 г. https://www.internetsociety.org/sites/default/files/Ethical Data-handling - v2.0.pdf

ВОПРОСЫ ИНТЕРОПЕРА-БЕЛЬНОСТИ / СТАНДАРТОВ

Общие аспекты интероперабельности / стандартов IoT

В традиционном Интернете интероперабельность устройств представляет собой ключевую ценность. Важнейшее требование к Интернет-подключению заключается в том, чтобы «связанные» системы были способны «говорить на одном языке» протоколов и кодов. Интероперабельность столь важна, что первые мастерские и семинары для поставщиков Интернет-оборудования так и назывались: «Interops» (от английского Interoperability – «интероперабельность»),[64]. Кроме того, она является ключевым моментом, на который обращено внимание всего сообщества разработки Интернет-стандартов, сконцентрированного вокруг Целевой инженерной группы Интернета (IETF).[65]

Интероперабельность также является краеугольным камнем открытого Интернета.[66] Барьеры, преднамеренно воздвигаемые, чтобы воспрепятствовать обмену информацией, могут лишить пользователей Интернета возможности ***подключаться***, ***говорить***, ***обмениваться информацией*** и ***предлагать инновации*** , нарушая четыре фундаментальных принципа ISOC.[67] Так называемые «закрытые платформы», где пользователи имеют возможность взаимодействовать лишь в рамках ограниченного набора веб-сайтов и сервисов, могут значительно снизить социальные, политические и экономические преимущества от доступа к неограниченному Интернет-пространству.

Интероперабельность устройств способна стимулировать инновации и повышать эффективность производителей IoT-устройств, увеличивая тем самым глобальный экономический продукт.

В условиях полной интероперабельности любое IoT-устройство могло бы устанавливать связь с любым другим устройством или системой и производить желаемый обмен информацией. Но на практике интероперабельность является более сложным явлением. Взаимодействие между IoT-устройствами и системами происходит на различных уровнях и в различных слоях в рамках стека коммуникационных протоколов между устройствами. Кроме того, полная интероперабельность по всему диапазону технической продукции не всегда осуществима, необходима или желательна, особенно если навязывать ее искусственно (например, по требованию властей), что может послужить барьером для инвестиций и инноваций.

Стандартизация и принятие протоколов, определяющих принципы связи (в том числе реальную потребность в наличии стандартов), являются основной темой дискуссий, касающихся Интернета вещей.

Помимо технических аспектов, интероперабельность оказывает значительное влияние на потенциальное экономическое воздействие Интернета вещей. Хорошо налаженная и явно выраженная интероперабельность IoT-устройств способна стимулировать инновации и эффективность производителей, увеличивая тем самым глобальный экономический продукт. Более того, реализация существующих стандартов (а при необходимости – создание новых открытых стандартов) позволяет уменьшить барьеры для создания и внедрения новых бизнес-моделей, а также создает условия для масштабного роста экономики.[68]

Согласно отчету международной консалтинговой компании McKinsey Global Institute за 2015 год, «[в] среднем 40 процентов валового продукта, который может быть создан индустрией Интернета вещей, реализуется лишь благодаря интероперабельности».[69] Далее в отчете говорится: «Интероперабельность является необходимым условием для высвобождения потенциального валового продукта в размере 4 триллионов долларов США в результате использования Интернета вещей в 2025 г. при общей стоимости валового продукта в размере 11,1 триллионов долларов США во всех девяти сферах, проанализированных институтом McKinsey».[70] И хотя некоторые компании видят конкурентные преимущества и экономические выгоды в разработке собственных систем, общие экономические возможности на рынке закрытых систем могут быть весьма ограничены.

Кроме того, интероперабельность по своей природе представляет большую ценность как для индивидуальных, так и для корпоративных потребителей этих устройств. Благодаря ей им становится легче выбирать устройства с лучшим функционалом по более выгодной цене и объединять их в системы для совместной работы. Покупатели могут испытывать сомнения, приобретая IoT-продукты или услуги при отсутствии гибкости интеграции, наличии сложностей для владельцев этих устройств, беспокойство из-за зависимости от поставщика или из-за морального износа при смене стандартов.

Ключевые аспекты и проблемы интероперабельности / стандартов IoT

Основной проблемой создания и признания IoT-устройств являются интероперабельность, стандарты, протоколы и условия использования. В список (хотя и не полный) основных проблем входят:

СОБСТВЕННЫЕ ЭКОСИСТЕМЫ И ПОТРЕБИТЕЛЬСКИЙ ВЫБОР

Некоторые производители устройств видят рыночные преимущества в создании собственных экосистем совместимых IoT-продуктов. Эти экосистемы, которые иногда называют «закрытыми экосистемами», ограничивают взаимодействие лишь теми устройствами и компонентами, которые входят в линейку продуктов данного бренда. Такие производители могут искусственно создавать зависимость пользователей от собственных экосистем, увеличивая стоимость будущего перехода клиентов на другие бренды или компоненты-заменители других поставщиков. Например, на рынке бытовой автоматики электрические лампочки одного поставщика могут не взаимодействовать с переключателями или системами контроля других производителей.

Сторонники интероперабельности рассматривают подобные практики как ограничение выбора потребителей, так как они не позволяют пользователям свободно переходить на альтернативную продукцию. Кроме того, они рассматривают подобные практики как сдерживающий фактор для инноваций и конкуренции, так как они ограничивают возможности конкурентов при создании новой продукции на основе базовой инфраструктуры экосистем. Но некоторые производители экосистем воспринимают подход с закрытыми экосистемами как преимущество для пользователей, предлагая им протоколы, которые можно будет легко и быстро внедрить, когда технологии или рынок потребуют изменений.

Проблемы интероперабельности также распространяются на сбор и обработку данных IoT-сервисами. Одно из основных преимуществ связанных устройств заключается в их способности передавать и получать данные через «облачные» сервисы, которые, в свою очередь, предоставляют доступ к ценной информации или услугам в зависимости от данных. Хотя это чрезвычайно полезно, использование данной функции может также создавать трудности для пользователей, желающих перейти на конкурирующий сервис. Даже если генерируемые устройством данные остаются доступными для пользователей, получение данных представляется невозможным, если они представлены в собственном закрытом формате. Пользователи могут свободно переходить к другим поставщикам услуг и самостоятельно анализировать данные только при условии, что исходные данные находятся в свободном доступе для пользователей-инициаторов и в открытом формате.

ТЕХНИЧЕСКИЕ И СТОИМОСТНЫЕ ОГРАНИЧЕНИЯ

По мере разработки IoT-устройств в этой сфере неизбежно возникают технические, временные и стоимостные ограничения, влияющие на совместимость и дизайн устройств. Некоторые устройства имеют технические ограничения (например, ограниченные внутренние ресурсы обработки данных, память или расход энергии). Кроме того, производители стремятся снизить себестоимость продукции, максимально снижая себестоимость компонентов и разработки продукта. Производители сравнивают затраты и выгоды, чтобы решить, стоят ли дополнительные затраты и потенциально более низкие характеристики продукта

дополнительных преимуществ от внедрения стандартов. В краткосрочной перспективе разработка функционала для обеспечения интероперабельности устройств и проверка на соответствие стандартам может оказаться менее выгодным решением. Иногда гораздо дешевле использовать собственные протоколы и системы, чтобы успешно выйти на рынок. Но с другой стороны, производителям следует также оценивать это с точки зрения долгосрочной перспективы увеличения жизненного цикла продукта за счет интероперабельности.

ОРГАНИЗАЦИОННЫЙ РИСК

«Первопроходцу» часто бывает выгоднее быстро представить свой продукт на мировом конкурентном рынке и занять свою нишу, и это также касается производителей IoT-устройств. Проблемы с интероперабельностью IoT-устройств возникают, когда графики разработки продукта производителем опережают доступность стандартов совместимости. Производители IoT-устройств, готовые вывести продукцию на рынок, могут испытывать неуверенность в графиках разработки стандартов и процессов, воспринимая это как предпринимательский риск, который следует избегать или максимально снижать. Это может сделать альтернативный дизайн более привлекательным по сравнению с применением открытых стандартов совместимости, особенно в краткосрочной перспективе.

ТЕХНИЧЕСКИЙ РИСК

Когда производители или пользователи IoT-устройств планируют разработку продуктов, им следует оценивать технические риски, связанные с разработкой новых протоколов при создании продукта. Внедрение существующих и зарекомендовавших себя стандартов в продукцию или систему может представлять меньший технический риск по сравнению с разработкой и использованием собственных протоколов. Использование общих, открытых и общедоступных стандартов (например, стека Интернет-протоколов) в устройствах или сервисах может дать иные преимущества; например, доступ к более многочисленным техническим кадрам, разработанному программному обеспечению или меньшим затратам по разработке продукта. Эти факторы рассматриваются в RFC 7452 Совета по архитектуре Интернета (IAB) *«Архитектурные решения для создания сетей с «умными» объектами»*.[71]

НЕОПТИМАЛЬНОЕ ПОВЕДЕНИЕ УСТРОЙСТВ

Отсутствие стандартов и документально оформленных рекомендованных приемов оказывают гораздо более сильное влияние, чем просто ограничение потенциала IoT-устройств. Отсутствие этих стандартов может пассивно вызывать неоптимальное поведение IoT-устройств. Другими словами, при отсутствии стандартов, которыми могут руководствоваться производители, разработчики устройств иногда создают продукцию, оказывающую разрушительное воздействие, не беря в расчет их пагубное влияние. И это хуже, чем просто несовместимость устройств. Имея плохо продуманный дизайн и конфигурацию, эти устройства могут негативно влиять на сетевые ресурсы, к которым они подключаются, а также на Интернет в целом.

В своей статье Интернет-эксперт Джефф Хастон называет мир подобных устройств «Интернетом глупых вещей».[72] В качестве примера автор приводит бюджетный кабельный модем, выпущенный одним из производителей и жестко запрограммированный на сервер Висконсинского университета в качестве IP-адреса NTP-сервера, что нарушило тем самым общепринятую практику разработки продуктов. Джефф Хастон

объясняет: «Чем больше продается устройств, тем сильнее растет общий трафик, направляемый на университетский сервер».[73] Такие устройства не просто отличались «неоптимальным поведением», отправляя все NTP-запросы на единственный сервер, но неудачный дизайн производителя также создавал трудности, не предлагая эффективного способа решения этой проблемы.

Существует возможность создания стандартов IoT и рекомендованных приемов, чтобы со временем заметно уменьшить такие проблемы.

УСТАРЕВШИЕ СИСТЕМЫ

Стандартизация совместимости – это настоящая проблема для новых IoT-устройств, которые должны взаимодействовать с уже разработанными и используемыми системами. Это касается многих типов среды, связанных с различными отраслями, способами применения и традиционным использованием определенных сетей устройств. [74] IoT-разработчикам нередко приходится идти на компромиссы ради обеспечения совместимости с устаревшими системами, пытаясь при этом добиться лучшей совместимости с другими устройствами за счет применения стандартов.

КОНФИГУРАЦИЯ

Пользователи сталкиваются с большими трудностями, пытаясь справиться с растущим числом IoT-устройств. Одна из этих трудностей заключается в необходимости легко и быстро менять конфигурацию целого ряда IoT-устройств, подключенных к сети. Когда необходимо сконфигурировать сотни отдельных устройств, очень важно иметь продуманный дизайн и стандартные средства конфигурации, методы и интерфейсы.[75]

УСИЛИЯ ПО РАЗРАБОТКЕ НОВЫХ СТАНДАРТОВ

Помимо традиционных организаций по разработке стандартов, в мире появилось множество новых отраслевых объединений, прилагающих дополнительные усилия по обеспечению доступа, разработки, преобразования и гармонизации стандартов и протоколов, связанных с IoT-устройствами и системами. В их число входят и такие «зрелые» организации, как IETF, ITU и IEEE, и сравнительно новые организации – например, Консорциум промышленного Интернета, Консорциум открытого взаимодействия, консорциумы ZigBee Alliance и AllSeen Alliance и множество других объединений.[76]

Для того, чтобы производители и другие заинтересованные лица приняли активное участие в общих усилиях по стандартизации, потребуется много времени и инвестиций. Кроме того, велика вероятность частичного «схлестывания» и даже конфликта между стратегиями стандартизации при реализации некоторых усилий.[77] Помимо увеличения расходов на разработку стандартов, несогласованность предпринимаемых мер может в конечном итоге привести к созданию конфликтующих протоколов, замедленной разработке продуктов и разобщенности IoT-продуктов, сервисов и производителей.

Вопросы интероперабельности

При рассмотрении проблем интероперабельности и стандартов неизбежно возникают вопросы, связанные с будущим IoT-устройств, в том числе:

В каких сферах стандарты совместимости нужнее и желательнее всего? Каковы их сходства и различия в широком спектре потенциальных способов использования и применения IoT-устройств (например, потребительские товары, промышленное применение и устройства медицинского назначения)? Каковы общие и общедоступные стандарты (например стек Интернет-протоколов), которые могут использоваться в качестве компонентов IoT-устройств и сервисов? Как отсутствие интероперабельности влияет на возможности пользователя подключаться, говорить, обмениваться информацией и предлагать инновации?

Какова оптимальная роль организаций по разработке стандартов, отраслевых консорциумов и заинтересованных групп при разработке IoT-стандартов? Каков потенциал объединения широкого спектра групп, работающих над технической реализацией IoT, для более глубокого обсуждения вопросов внедрения интероперабельности и стандартов? Возможно ли избежать возникновения конкурирующих стандартов, дублирования и конфликтов в связи с тем, что организации по разработке стандартов и консорциумы пытаются решить похожие или перекрестные проблемы без общей координации сверху? Как участники отрасли и другие заинтересованные стороны могут отслеживать всю деятельность, которая ведется в этой обширной сфере?

Каков оптимальный подход к просвещению и привлечению сообщества пользователей и разработчиков для решения проблем «неоптимально ведущих себя» IoT-устройств и отсутствия внедрения стандартов? Какие рекомендованные приемы или базовые модели реализации эффективны в условиях множества способов применения и использования IoT-устройств?

Как Интернет вещей влияет на потребление пропускной способности и других ресурсов и в какой степени необходимо изменить стандарты для удовлетворения этих растущих потребностей? В чем заключаются проблемы облачной интероперабельности, если учитывать важность облачных сервисов для Интернета вещей?

Невозможно отрицать важность интероперабельности IoT-устройств и соответствующих стандартов для рынка и потребителей. Проблема разработки и применения стандартов интероперабельности занимает центральное место в дискуссиях, касающихся инноваций, конкуренции и выбора пользователями услуг, что является неотъемлемой частью основополагающих принципов ISOC.

ПРИМЕЧАНИЯ К РАЗДЕЛУ

Вопросы интероперабельности / стандартов

64. История Интернета: 1988 год. Статья в веб-журнале. Computer Information, 12 августа 2010 г., Интернет 6 сент. 2015 г. См. веб-сайт: http://inthistory4u.blogspot.com/2010/08/1988.html

65. См. веб-сайт: http://www.ietf.org

66. Открытый Интернет: что это такое и как не перепутать его с чем-то другим? Internet Society, 3 сентября 2014 г. См. веб-сайт: https://www.internetsociety.org/doc/open-internet-what-it-and-how-avoid-mistaking-it-something-else

67. "Values and Principles". *Principles*. Internet Society, 2015 г. http://www.internetsociety.org/who-we-are/mission/values-and-principles

68. В разделе 3.5.6. «Интернет вещей» Скользящего плана Европейской Комиссии по стандартизации ИКТ на 2015 год обсуждаются стандарты IoT с точки зрения конкурентоспособности и политики. См. веб-сайт: https://ec.europa.eu/digital-agenda/en/rolling-plan-ict-standardisation

69. Джеймс Маника и др. *Интернет вещей: ценности без рекламы*. McKinsey Global Institute, июнь 2015 г. стр. 2. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

70. *Там же*. 4.

71. Tschofenig, H. , et. al., *Architectural Considerations in Smart Object Networking*. Tech. № RFC 7452. Internet Architecture Board, март 2015 г., Интернет. https://tools.ietf.org/html/rfc7452

72. Джефф Хастон. Интернет глупых вещей. *APNIC Labs*, 28 апреля 2015 г. https://labs.apnic.net/?p=620

73. *Там же*.

74. Примеры протоколов устаревших систем: АСУ ТП (система диспетчерского контроля и сбора данных) – протокол, использовавшийся для управления промышленным оборудованием; CAN-шины (шины сети локальных контроллеров) – протоколы для считывания данных с датчиков автомобилей и промышленного оборудования.

75. Винтон Серф. Персональные коммуникации. 9 сентября 2015 г.

76. См. список организаций, консорциумов и альянсов по разработке IoT-стандартов в конце данного документа в разделе «Дополнительная информация».

77. Стивен Лоусон. Почему «стандарты» Интернета вещей стали еще запутаннее в 2014 году? *PCWorld*, 24 декабря 2014 г. http://www.pcworld.com/article/2863572/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016.html

ВОПРОСЫ ЗАКОНОДАТЕЛЬСТВА, НОРМАТИВНЫХ ТРЕБОВАНИЙ И ПРАВ

Применение IoT-устройств привело к появлению целого ряда проблем и вопросов нормативно-правового и юридического характера, которые следует тщательно рассмотреть. Иногда IoT-устройства ведут к появлению новых юридических, нормативных и гражданско-правовых проблем, которые не существовали до появления этих устройств. В других случаях эти устройства усугубляют юридические проблемы, которые уже существовали. Кроме того, технологии развиваются гораздо быстрее, чем связанное с ними законодательство и нормативно-правовая среда. Ниже обсуждаются некоторые потенциальные нормативные и юридические проблемы, влияющие на весь диапазон применения IoT-устройств.

Защита данных и транснациональные информационные потоки

Отправка данных, собранных IoT-устройствами, за пределы страны может быть недопустимой. Эти устройства используют Интернет для связи, а Интернет охватывает территории всех государств на всех уровнях. IoT-устройства могут собирать данные о физических лицах из одной юрисдикции и передавать эти данные для хранения и обработки в другую юрисдикцию, и при этом часто наблюдается нехватка или отсутствие технических барьеров. Это явление может быстро перерасти в юридическую проблему (например, если собранные данные были признаны персональными или конфиденциальными и подлежат защите в соответствии с законодательством нескольких юрисдикций). Дело осложняется тем, что законодательство о защите данных в той юрисдикции, где находятся устройство и субъект персональных данных, может не соответствовать или противоречить законам страны, где данные хранятся и обрабатываются.

Подобные ситуации являются проблемой транснациональных информационных потоков и ставят вопросы о законодательной базе, которая должна применяться. Другими словами, какой правовой режим регулирует сбор данных устройством, а какой режим регулирует хранение и использование собранных данных? Этот сценарий также вызывает вопросы нормативного характера. Можно ли изменить эти законы, чтобы уменьшить степень разобщенности в Интернете, при этом защитив права пользователей? Распространяются ли требования юрисдикции с более жестким законодательством о защите данных при обработке и передаче через IoT на другие юрисдикции?

Интернет вещей привел к появлению целого ряда нормативно-правовых проблем и способен усугубить уже существующие проблемы, связанные с Интернетом. Защита возможности пользователей подключаться, говорить, создавать инновации, делиться информацией, выбирать и доверять должна быть ключевым принципом при разработке законов и норм.

В то время, как многие проблемы транснациональных информационных потоков рассматриваются и решаются в условиях потока данных традиционного Интернета,[78] IoT-устройства порождают новые проблемы. Эти устройства все больше способны автоматически подключаться к другим устройствам и системам и передавать данные в другие страны без ведома пользователей. Это способно привести к появлению таких ситуаций, когда пользователь фактически несет юридическую ответственность за соблюдение требований по транснациональной передаче данных, даже не зная, что это происходит. Эти проблемы сложны, но они становятся еще более сложными по мере того, как технологии опережают в своем развитии законодательство.

Дифференциация данных IoT

Данные, собираемые IoT-устройствами, могут содержать исчерпывающую информацию о лицах, вступающих в контакт, и могут использоваться как во благо, так и во вред. Взять хотя бы проблему с персональными фитнес-трекерами. Люди часто носят эти устройства в течение нескольких дней или недель, и эти трекеры собирают точные данные о перемещениях пользователей, а также другие биометрические данные. Эта информация анализируется приложениями, чтобы оценить состояние здоровья пользователя, количество сожженных калорий, а также продолжительность и качество сна. Конечно, подобный анализ приносит пользу для человека, так как он позволяет оценить физическую активность пользователя, когда тот пытается сбросить вес или достичь другие фитнес-цели.

Однако эти же данные могут использоваться и во вред. Некоторые американские планы медицинского страхования побуждают участников предоставлять страховым компаниям доступ к данным их фитнес-трекеров в обмен на снижение стоимости страховки.[79] Человек, который готов сообщить свои биометрические данные ради получения скидки, может рассматривать это как дополнительное удобство. С другой стороны, эти данные могут использоваться во вред – особенно для тех кто испытывает финансовые проблемы. Вот что пишет один из комментаторов:

> Представьте себе схему определения цен [на страховку], которая «наказывает» страдающих от недосыпания родителей-одиночек или малооплачиваемых работников, которые не могут позволить себе полноценное питание. А финансовые стимулы на предоставление страховым компаниям и другим заинтересованным сторонам доступа к данным о состоянии здоровья могут стать столь жесткими, что «согласие» на участие в программе превращается в единственно возможный выбор.[80]

Подобные ситуации становятся все более распространенными. Новые автомобили, оснащенные GPS-метками и подключенные к каналам передачи данных, передают информацию о местонахождении и поведении водителя за рулем (например, превышение скорости и резкое торможение) удаленным системам, либо используются для помощи водителям или улучшения дорожного сервиса. В то время как эти возможности служат во благо пользователей, данные могут использоваться и дискриминирующими способами. Например, операторы автопарков могут использовать эти данные для навязчивого контроля водителей, не имеющих возможности избавиться от непрерывного наблюдения. Это довольно прямые примеры того, как IoT-данные могут использоваться дискриминирующим образом; однако остается неясным, как различные комбинации IoT-данных будут использоваться для дискриминации в будущем.

Данные, собираемые IoT-устройствами, могут содержать исчерпывающую информацию о лицах, вступающих в контакт, и эти данные могут использоваться как во благо, так и во вред. Эти данные могут использоваться в благородных целях и для разработки функционала, представляющего ценность для пользователей. С другой стороны, те же данные могут использоваться дискриминирующим образом.

Кроме того, возможность возникновения практик дискриминирующего ценообразования или недобросовестного обслуживания может усугубляться в зависимости от качества, специфики и объема сгенерированных IoT-данных о пользователях. IoT-данные часто могут быть привязаны к таким метаданным, как дата, время и местоположение, которые значительно улучшают качество данных для анализа. Кроме того, IoT-датчики обычно имеют довольно узкое предназначение. А это значит, что данные, получаемые с помощью таких датчиков, часто привязаны к конкретным оперативным ситуациям, позволяя получить специфическую информацию при установлении связи с человеком или группой людей. Фактически устройство можно отождествлять с конкретным человеком, если оно имплантировано – как, например, в случае с подключенным к Интернету кардиостимулятором или дозатором инсулина. В других случаях такой уровень специализации нежелателен и может непреднамеренно привести к негативным результатам. IoT-датчики, находящиеся в собственности или под контролем третьих лиц, могут собирать идентифицируемые данные о человеке без его ведома и согласия. Эти данные могут использоваться во вред человека, за которым ведется наблюдение.

И, наконец, эти устройства обеспечивают непрерывных поток данных без вмешательства человека. Комбинация этих характеристик делает анализ IoT-данных весьма детальным и полезным для исследований, для разработки продукции, а также в других областях. Алгоритмы анализа крупных блоков данных могут справляться с гигантскими массивами IoT-данных и выполнять статистическую и семантическую корреляцию для выделения пользователей в группы и кластеры с конкретными характеристиками. В то же время эти алгоритмы вполне могут незаконно распределять пользователей по категориям и манипулировать этими характеристиками.

Подобное использование IoT-данных приводит к возникновению многочисленных проблем практического, юридического и нормативного характера. В первую очередь, какие дискриминирующие или недобросовестные практики по отношению к пользователям были выявлены? Существуют ли дискриминирующие практики, которые выявить практически невозможно? Есть ли разница с юридической точки зрения, если дискриминирующее решение принято человеком или машиной? Это сложная область, где должны быть проведены серьезные научные исследования с целью разработки инструментов по выявлению недобросовестных практик алгоритмирования, особенно в современных условиях, когда большинство алгоритмов анализа данных является коммерческой тайной отдельных компаний и недоступно широкой публике. Как найти верный баланс между значительными коммерческими и социальными преимуществами от анализа IoT-данных и возможностью появления дискриминирующих практик, направленных против пользователей? Как стимулировать появление инновационных принципов в сфере IoT-данных, одновременно защищая пользователей от недобросовестных практик? Как добиться большей прозрачности? Способны ли существующие законы о конфиденциальности и защите прав потребителей справиться с такими ситуациями? Какие средства защиты необходимы при появлении дискриминирующих практик? Следует ли разделить IoT-устройства по категориям, чтобы контролировать их в зависимости от природы генерируемых ими данных, особенно если они могут быть использоваться во вред?

Устройства IoT как инструмент правоохранительных органов и общественной безопасности

IoT-устройства могут способствовать обеспечению правопорядка и общественной безопасности, однако необходимо тщательно обдумать последствия с точки зрения закона и общества. Вне всяких сомнений, IoT-устройства и генерируемые ими данные могут использоваться как эффективное средство борьбы с преступностью. В торговых точках устанавливают камеры наблюдения для сбора видеоматериала и наблюдения за поведением покупателей, что весьма полезно для сбора улик и предотвращения преступности.[81] С недавних пор корпорация On-Star, которая является дочерней компанией General Motors, может предоставлять органам правопорядка информацию, получаемую со встроенных в автомобиль датчиков, помогая полиции находить угнанные автомобили; кроме того, она может дистанционно блокировать двигатели угнанных транспортных средств.[82] Полицейское управление округа Нассау (штат Нью-Йорк) использует сеть звуковых датчиков *ShotSpotter*, чтобы с точностью определять источник стрельбы в тех районах, где они установлены.[83] Это примеры тех преимуществ, которые технология Интернета вещей предлагает органам правопорядка для борьбы с преступностью и обеспечения общественной безопасности.

С другой стороны, подобное использование IoT-технологий вызывает беспокойство у некоторых защитников гражданских прав и других заинтересованных лиц. Поводом для беспокойства служит возможность всепроникающего контроля данных, несовершенство законодательства о сохранении и уничтожении данных, методы вторичного использования данных государственными служащими, а также возможность получения доступа к этим данным «плохими парнями». Кроме того, следует учитывать возможность неблагоприятного влияния наблюдения за деятельностью сообществ и обществ, приносящей благо.

Другие ситуации, связанные с обеспечением правопорядка и охраной общественной безопасности, представляются менее явными. Например, при разработке смартфона iPhone 6 с операционной системой iOS 8 корпорация Apple устранила возможность «обходного» доступа к данным, который был возможен на более старых версиях iPhone. Обходной доступ позволял полицейским получать доступ к данным на телефонах пользователей в целях охраны правопорядка. Компания Apple устранила эту функцию в новом iPhone, и теперь смартфон кодирует внутренний контент телефона так, что его почти невозможно взломать, причем Apple не хранит ключи шифрования и, соответственно, не может предоставить к ним доступ.[84] Благодаря этому, доступ к содержимому не может получить никто, кроме владельца телефона. Федеральные органы правопорядка заявляют, что это препятствует борьбе с преступностью,[85] а защитники гражданских свобод считают это победой в деле защиты конфиденциальности данных пользователей.[86] Это противоречие, связанное с шифрованием устройств, касается и других IoT-устройств. Как найти верный баланс между шифрованием IoT-устройств для защиты от атак и законными требованиями по предоставлению доступа к хранящимся в устройстве пользовательским данным органам правопорядка и государственной безопасности?

Ответственность в связи с использованием устройств IoT

IoT-устройства привели к появлению сложных вопросов, касающихся юридической ответственности, о которых следует задуматься. Ключевой вопрос, касающийся IoT-устройств, звучит так: если человеку нанесен вред в результате действия или бездействия IoT-устройства, кто должен нести за это ответственность? На этот вопрос бывает трудно ответить, и во многих случаях мы сталкиваемся с отсутствием законов, которые бы регулировали этот вопрос. Работа IoT-устройств сложнее, чем работа простых автономных продуктов, а это говорит о более сложных сценариях привлечения к ответственности. Пример:

IoT-устройства вполне могут использоваться в целях, не предусмотренных производителями. А производители IoT-устройств не могут предугадать все сценарии возможного использования.

Существует вероятность подключения IoT-устройств и их взаимодействия с другими устройствами непроверенными и непредсказуемыми способами. По мере увеличения интероперабельности эти устройства могут формировать децентрализованные сети, подключаясь друг к другу. Поэтому производителям и пользователям трудно предсказать все возможные недобросовестные способы использования этих устройств.

Устройства могут иметь длительный срок службы, представляя неизвестную угрозу безопасности в будущем. Эти устройства можно взломать и перепрограммировать для нанесения вреда этим или другим устройствам, а также для раскрытия конфиденциальной информации непреднамеренными и неизвестными способами.

IoT-устройства будут интегрироваться в такие автономные системы, как самоуправляемые автомобили, где используются адаптивные алгоритмы машинного обучения для контроля поведения автомобилей в зависимости от сведений, получаемых из датчиков IoT-устройств. Действие этих систем не может быть полностью понято и проверено заранее.

Эти и другие сценарии приводят к появлению различных вопросов. Если какой-либо из этих сценариев приведет к нанесению вреда, справятся ли с ситуацией существующие законы о привлечении к ответственности и разъясняют ли они юридическую ответственность соответствующих сторон? Следует ли пересмотреть законы о привлечении к ответственности с точки зрения «умных» IoT-устройств, которые обучаются от окружения и со временем модифицируют сами себя? Если автономные системы обучаются в результате действий конечного пользователя, а не собственных внутренних алгоритмов, что произойдет в случае ошибки пользователя? Должны ли IoT-устройства быть достаточно «умными», чтобы выполнять инструкции типа «делай, что я говорю»? В какой мере действие существующих законов о привлечении к ответственности при использовании традиционных продуктов распространяется на продукцию, подключенную к Интернету? Какие меры должны быть предприняты нашим сообществом, чтобы информировать законодателей во избежание принятия ими неверных решений на основе массы недостоверной информации и корыстных рекомендаций, которые они получают? И что мы можем сделать, чтобы информировать пользователей и покупателей устройств для достижения понимания ими всех факторов, связанных с их использованием?

Расширение использования IoT-устройств в судебных процессах

Данные, собираемые IoT-устройствами, часто могут служить в качестве улик при различных судебных разбирательствах, и по мере того, как IoT-данные становятся все более распространенными, они будут все чаще использоваться в судебных процессах. Например, американские адвокаты используют данные о месте и времени оплаты проезда по автомагистрали, получаемые из электронных устройств, чтобы уличить неверного супруга в ходе бракоразводного процесса.[87] А в 2014 году жительница Канады использовала данные из своего фитнес-трекера при подаче судебного иска в качестве доказательства нанесения ей вреда.[88]

IoT-устройства с выходом в Интернет также могут устанавливаться в автомобилях с целью получения оплаты от водителей, не выполняющих свои платежные обязательства. Если водитель не осуществит своевременную оплату за аренду автомобиля или взнос по автокредиту, агент по аренде или продаже автомобиля сможет дистанционно заблокировать двигатель автомобиля через установленное в нем устройство, пока водитель оплату не осуществит.[89] Такие IoT-устройства установлены более чем на двух миллионах автомобилей в США.[90]

Подобные сценарии приводят к появлению новых юридических и нормативных вопросов об использовании IoT-устройств. Должны ли производители устройств внедрять такие технологии, как шифрование данных, чтобы ограничить к ним доступ, как это сделала компания Apple со смартфоном iPhone? И наоборот, должны ли производители устройств разрабатывать IoT-устройства так, чтобы облегчить использование данных при судебных разбирательствах? Нужно ли разрабатывать технические условия для IoT-данных, чтобы оптимизировать юридическую цепь обеспечения сохранности данных при судебных разбирательствах? Нужно ли разрабатывать специальные нормы по защите потребителей, касающиеся определенных IoT-устройств?

Функционал IoT-устройств сложнее функционала простых автономных продуктов, что предполагает более сложные сценарии привлечения к ответственности, которые следует рассмотреть.

Общие выводы по юридическим, нормативным и правовым вопросам

Круг проблем юридического, нормативного и правового характера, связанных с Интернетом вещей, весьма широк. Развитие IoT-устройств приводит к появлению новых юридических и нормативных проблем, которых раньше не существовало, и усугубляют многие существующие проблемы. Например, требования по сборке IoT-устройств для лиц с ограниченными возможностями приводят к появлению новых проблем в связи с разработкой новых типов IoT-устройств, но при этом поддерживают существующие стандарты и требования по доступности. [91] С другой стороны, огромное количество беспроводных IoT-устройств, а также радио- и иные помехи, которые они создают, – это пример того, как IoT-устройства усугубляют уже существующие проблемы использования частотного спектра. [92] Вопросы юридического и нормативного характера, касающиеся интеллектуальной собственности (например, утилизация устройств) и владения (например, приобретение в собственность или аренда) – это растущие проблемы, которые также касаются IoT-устройств.

Помимо трудностей при разработке разумных нормативных стратегий для решения IoT-проблем, существуют и дополнительные сложности при принятии решений об объекте системной архитектуры IoT для достижения желаемых результатов. Должны ли нормативные требования применяться к устройствам, потоку данных, шлюзам, пользователям или облачным хранилищам данных? Ответы на эти и другие вопросы зависят от точки зрения, с которой анализируется ситуация. Нормативный анализ IoT-устройств все чаще проводится с общей, нейтральной по отношению к технологиям точки зрения (например, с точки зрения законов и нормативов по защите потребителей).[93] Оценка юридических проблем, касающихся IoT-устройств, с точки зрения защиты от недобросовестных или нечестных практик, направленных против потребителей,[94] может способствовать принятию верных решений о конфиденциальности и безопасности.[95]

И, наконец, решение проблем в данном пространстве и их влияние на общество следует осуществлять с учетом ключевых принципов Internet Society, которые защищают возможности ***подключаться***, ***говорить***, ***предлагать инновации***, ***делиться информацией***, ***выбирать*** и ***доверять***.[96]

ПРИМЕЧАНИЯ К РАЗДЕЛУ

Вопросы законодательства, нормативных требований и прав

78. Проблемы транснациональных информационных потоков, как правило, решаются в рамках региональных и международных инициатив по обеспечению конфиденциальности информации (Руководящие принципы ОЭСР по защите частной жизни, Конвенция 108 Союза Европы, Стандарты АТЭС о неприкосновенности частной жизни и т.д.) и специальных соглашений (система Правил АТЭС трансграничной конфиденциальности, Обязательные корпоративные правила Евросоюза и т.д.). Однако это, скорее, точечный подход, а не всеобъемлющее решение.

79. Большой доктор следит за тобой. *Slate*, 27 февраля 2015 г. http://www.slate.com/articles/technology/future_tense/2015/02/how_data_from_fitness_trackers_medical_devices_could_affect_health_insurance.html

80. *Там же*.

81. Гофорт Грегори, Дженнифер. 5 способов остановить кражу с помощью технологий. *Entrepreneur*, 7 ноября 2013 г. http://www.entrepreneur.com/article/229674

82. Бонд-мл. , Винс. Юристы в погоне за данными в автомобиле. *Automotive News*, 14 сентября 2014. http://www.autonews.com/article/20140914/OEM11/309159952/lawyers-reaching-for-in-car-data

83. Вэйс, Тодд Р. Лучшие полицейские технологии: 5 новых технологий, помогающих полиции бороться с преступностью.*Computerworld*. , 16 февраля 2012 г. Интернет. 3 августа 2015 г. http://www.computerworld.com/article/2501178/government-it/cool-cop-tech--5-new-technologies-helping-police-fight-crime.html?page=2

84. Тимм, Тревор. Ваш iPhone теперь зашифрован. ФБР считает, что это помогает похищать людей. Кому верить? *The Guardian*, 30 сентября 2014 г. http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default

85. *Там же*.

86. Крейг Тимберг. «Apple отказывается разблокировать большинство устройств iPhone и iPad по запросу полиции даже при наличии ордера на обыск». *Washington Post*. Washington Post, 18 сентября 2014 г. http://wapo.st/XGGwDi

87. Крис Ньюмаркер. «EZPass выдает неверных супругов властям». *Msnbc.com*. NBC News.com, 10 августа 2007 г. http://www.nbcnews.com/id/20216302/ns/technology_and_science-tech_and_gadgets/t/e-zpass-records-out-cheaters-divorce-court/ - .Vbp9KnjfbFI

88. Парми Олсон. «Суды начинают использовать показания Fitbit». *Forbes*. Журнал Forbes, 16 ноября 2014 г. http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/

89. Эйми Риччи. «Конфискаторы блокируют двигатели автомобилей на расстоянии». *CBS News*, 25 сентября 2014 г. http://www.cbsnews.com/news/why-the-repo-man-can-remotely-shut-off-your-car-engine/

90. Майкл Коркери, Джессика Силвер-Гринберг. «Пропустили платеж? Попробуйте завести свою машину». *New York Times*, 24 сентября 2014 г. http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/

91. Различные правила госзакупок создают базу для правил обеспечения доступности продуктов информационно-коммуникационных технологий (ИКТ), которые следует рассматривать в контексте совместимости IoT-устройств. В качестве примеров могут послужить стандарты Американской коллегии по доступу (секция 508) и европейский стандарт EN 301 549 V1.1.1.

92. Марк А. Макгенри, Деннис Робертсон и Роберт Дж. Матсон. Электронный шум заглушает Интернет вещей. *IEEE Spectrum*, сентябрь 2015 г. (18 августа 2015 г.). http://spectrum.ieee.org/telecom/wireless/electronic-noise-is-drowning-out-the-internet-of-things

93. Маартен Боттерман. *Доклад о будущем IoT-технологий: открывая новую реальность*. Краткий отчет № D5.2.39. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf

94. Закон об Федеральной торговой комиссии США, кодекс 15, §45(a).

95. Динамическая коалиция по управлению Интернетом вещей (DC IoT) Форума по управлению использованием Интернета предложила этический подход к поиску решений проблем IoT. См. примеры на сайтах: http://www.iot-dynamic-coalition.org/intersessional-meetings/dresden-meeting-2015/ и http://review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-the-internet-of-things-dc-iot-4/

96. “Values and Principles”. *Principles*. Internet Society, 2015 г. http://www.internetsociety.org/who-we-are/mission/values-and-principles

РАЗВИВАЮЩИЕСЯ ЭКОНОМИКИ И ВОПРОСЫ РАЗВИТИЯ

Обеспечение преимуществ IoT в глобальном масштабе

Распространение и влияние Интернета глобально по своей природе, так как он открывает преимущества и возможности как для развитых, так и для развивающихся регионов. В то же время, развивающиеся регионы часто сталкиваются с особыми проблемами, связанными с созданием, развитием, внедрением и использованием технологий, включая Интернет. Разумно ожидать, что это окажется справедливым и для потенциальных преимуществ и проблем Интернета вещей.

В соответствии с основными принципами Internet Society, мы верим, что Интернет должен являться источником повышения возможностей по всему миру независимо от местоположения, региона и экономического развития страны пользователя и что полный спектр возможностей и принципов,[97]

Интернет вещей обещает стать важнейшим инструментом социального развития, в том числе для достижения Целей устойчивого развития ООН.

которые определяют нашу работу и успех Интернета, является глобальным. Начиная с самых ранних дней Интернета, техническое Интернет-сообщество, гражданское общество, государственные организации и представители частного сектора, помимо всего прочего, уделяли особое внимание возможностям и проблемам использования Интернета в развивающихся странах. Следовательно, это должно быть справедливым и в отношении возможностей и проблем использования Интернета вещей.[98]

Возможности экономического развития

В плане возможностей агентство McKinsey Global Institute отмечает, что IoT-технологии имеют значительный потенциал в развивающихся странах. По мнению агентства, к 2025 году не менее 38% ежегодного экономического влияния Интернета вещей будет проистекать из менее развитых регионов.[99] С экономической точки зрения ожидается, что как демографические, так и рыночные тенденции будут определять эти возможности. Например, развивающиеся страны имеют большое количество потенциальных пользователей Интернета вещей (особенно Китай), поэтому центр глобального экономического роста перемещается на территории развивающихся стран, и промышленное применение Интернета вещей (на заводах, фабриках, в сфере транспорта и т.д.) будет определять увеличение рыночной стоимости.[100]

Если ожидания, касающиеся инноваций и применения этих технологий, будут реализованы, то Интернет вещей будет иметь огромный потенциал как важнейший инструмент социального развития, включая достижение целей устойчивого развития ООН.[101] Цели устойчивого развития (ЦУР) – это список из 17 целей, которые охватывают более 100 задач развития для обеспечения достоинства, благополучия и равенства людей всего мира – особенно малоимущих и необеспеченных слоев населения. Они охватывают широкий диапазон фундаментальных проблем развития, включая развитие ресурсосберегающего сельского хозяйства, обеспечение населения энергией и водой, индустриализация, управление наземными и водными ресурсами, а также другие проблемы.

При рассмотрении потенциала «умных» предметов и технологий Интернета вещей, которые должны значительно повлиять на решение проблем развития, эти возможности представляются весьма интересными. Например, применение сенсорных сетей для решения экологических проблем (таких, как качество и использование водных ресурсов, системы канализации, медицина, здоровье, изменение климата и управление природными ресурсами) может оказать значительное влияние на решение проблем, выходящих далеко за пределы сферы управления ресурсами. Данные, получаемые в результате подобного применения, также могут использоваться в исследовательских целях, что может помочь местным ученым и университетам внести уникальный вклад в более широкую область всемирных знаний и побудить местные академические таланты оставаться в родной стране для проведения новых исследований.

Население Земли растет, особенно в странах с переходной экономикой, поэтому проблемы обеспечения населения качественной, безопасной и доступной пищей будут неизбежно усугубляться. Потенциал использования Интернета вещей для борьбы с голодом и развития ресурсосберегающего сельского хозяйства привлекает особое внимание – возможно большее, чем любая другая проблема развития.[102] В свете того, что перед нами остро стоят проблемы управления циклами сельскохозяйственного производства, угрозы болезней, растущей потребности в автоматизированном сборе урожая, развития распределительной логистики и контроля качества, «умные сельскохозяйственные» технологии Интернета вещей, как ожидается, должны улучшить ситуацию с надежностью и эффективностью всей пищевой цепочки.[103, 104]

ВСТАВКА 4

ИНТЕРНЕТ ВЕЩЕЙ И ГЛОБАЛЬНОЕ РАЗВИТИЕ

Интернет вещей (Internet of Things – IoT) используется по всему миру для решения некоторых наиболее острых проблем глобального развития. Соответствующие технологии используются, чтобы решить самые разные проблемы, от борьбы с нищетой до оптимизации управления экологическими системами водоснабжения и канализации, а также чтобы улучшить сферу предоставления услуг и ускорить развитие.

А если учесть, что стоимость датчиков и микропроцессоров уменьшается, а число доступных технологий подключения растет, Интернет вещей можно рассматривать как следующий рубеж по использованию информационно-коммуникационных технологий (ИКТ) в целях развития (ИКТР). В настоящее время 90% мирового населения имеет доступ к сетям мобильной связи, причем две трети населения использует сигнал 3G, обеспечивающий надежный обмен данными; однако в мире существует множество других технологий большого и малого диапазона, которые также предлагают широкий выбор средств для обмена данными. По мере того, как устройства и услуги становятся все более доступными по цене, Интернет вещей будет вносить все больший вклад в развитие общества (ИВР). Например, уже сегодня сети снабжения препаратами против простуды (особенно по транспортировке и распределению основных вакцин), которые используют датчики для отслеживания температуры и местоположения, более безопасны и эффективны и имеют больший процент успешной доставки лекарств до места назначения без повреждений. В деревнях восточной Африки используются ручные водяные насосы, оборудованные датчиками потока воды с модулями 2G SMS, которые могут информировать местные власти, правительственные учреждения и донорские сообщества об уровне потребления воды и тем самым уменьшить время бездействия плохо работающих насосов.

Сельскохозяйственный сектор также пользуется преимуществами от использования Интернета вещей. Более целевое кормление и наблюдение за поголовьем скота стало возможным благодаря использованию именных/номерных меток с чипами радиочастотной идентификации (RFID-чипами). Электрохимические датчики, погруженные в почву, могут измерять уровень солнечного излучения, а также насыщения водой и присутствия основных питательных веществ (например, фосфора и азота). Кроме того, малообеспеченные семьи, живущие на удаленных территориях и в городах и не имеющие доступа к общим системам подачи электричества, используют технологии Интернета вещей в сочетании с автономными солнечными батареями, чтобы снабжать свои дома электричеством. Начальные расходы на покупку солнечных батарей подлежат амортизации и оплачиваются через мобильные системы оплаты, а солнечные батареи передают данные об уровне подзарядки и потребления энергии через каналы передачи данных.

Эти и другие примеры демонстрируют то, как Интернет вещей может использоваться для достижения Целей развития тысячелетия (ЦРТ) и Целей устойчивого развития (ЦУР) ООН. Однако проблемы (особенно связанные с инфраструктурой, техническими возможностями и развитием законодательной базы, способствующими более активному использованию Интернета вещей) остаются нерешенными. Более пристальное внимание потенциалу ИВР поможет увеличить его влияние и эффективность для решения некоторых серьезных проблем развития вашего века.

источник: отчет «Интернет вещей и глобальное развитие» компании Cisco и Комиссии МСЭ/ЮНЕСКО по широкополосной связи в интересах цифрового развития.

Вопросы развивающихся экономик и развития IoT

Чтобы обеспечить глобальность возможностей и преимуществ использования Интернета вещей, нам необходимо рассмотреть особые нужды и потенциальные проблемы стран с переходной экономикой. Вопросы, рассмотренные в предыдущих разделах, касаются не только промышленно развитых стран, но и развивающихся рынков. Однако в странах с переходной экономикой наблюдаются свойственные только им условия, которые приводят к появлению дополнительных вопросов, связанных с получением максимальных преимуществ и решением проблем IoT.

Ниже представлен список проблем (далеко не полный), которые следует рассмотреть:

ИНФРАСТРУКТУРА И РЕСУРСЫ

Инфраструктура связи и Интернета в развивающихся странах быстро расширяются, однако во многих странах остаются пробелы в обеспечении надежного, высокоскоростного и недорогого подключения, в том числе для коммерческого и бизнес-использования. В какой степени Интернет вещей оказывает давление на инфраструктуру и ресурсы Интернета и связи? Подавляют ли текущие проблемы возможности IoT в развивающихся регионах, или IoT может стать двигателем дополнительного развития инфраструктуры? Требуется ли уделить особое внимание управлению спектром, если учесть, что беспроводные технологии поддерживают многие способы применения IoT? Если облачные сервисы и анализ данных благотворно влияют на развитие IoT-услуг, будет ли относительная недоразвитость инфраструктуры информационного центра в развивающихся странах тормозить их использование?

ИНВЕСТИЦИИ

В промышленно развитых странах инвестиции в IoT-исследования и разработку продукции определяются рыночными возможностями для продвижения продукции и услуг. В какой степени ориентированные на рынок инвестиции повлияют на внедрение IoT в развивающихся странах, особенно в сферах, которые явно не обещают гарантированной и быстрой прибыли? С другой стороны, может ли применение IoT в развивающихся странах оказаться более эффективным и недорогим, и могут ли они обогнать технологии остального мира, если здесь используется меньше устаревших систем? Может ли правительство стимулировать разработку инновационных технических решений местными исследователями и отраслями?

ТЕХНИЧЕСКОЕ И ПРОМЫШЛЕННОЕ РАЗВИТИЕ

В какой степени исследователи и предприниматели из развивающихся стран вовлечены в процесс технического развития и применения IoT? Что нужно сделать, чтобы стимулировать участие в разработке технических решений и способов применения в соответствии с нуждами и потребностями этих рынков, уважая при этом культурные традиции и выстраивая на соответствующих уровнях защиту безопасности и конфиденциальности? Какие новые навыки могут потребоваться в условиях переходной экономики для создания, применения и управления IoT-системами? Готовы ли отрасли стран с переходной экономикой воспользоваться преимуществами IoT-технологий? Останутся ли они позади или займут ведущие позиции, обогнав более старые промышленные технологии? Какую позицию могут занять исследователи и отрасли в странах с переходной экономикой, чтобы найти решения местных экономических и социальных проблем, которые напрямую влияют на их общества?

ПОЛИТИЧЕСКАЯ И НОРМАТИВНАЯ КООРДИНАЦИЯ

За последние 10 лет законодатели стран с переходной экономикой добились значительного прогресса в разработке и принятии законов и норм, способствующих развитию Интернета и решающих связанные с ним проблемы. Требования к техническим законодателям в развивающихся странах растут, особенно в условиях быстрого развития и ограниченных ресурсов. И хотя IoT обещает новые возможности, он также ставит перед нами новые проблемы. В каких данных и ресурсах нуждаются законодатели развивающихся стран сегодня, чтобы запланировать решение политических и других вопросов, которые неизбежно возникнут с развитием IoT?

ПРИМЕЧАНИЯ К РАЗДЕЛУ

Развивающиеся экономики и вопросы развития

97. «Ценности и принципы». *Принципы*. Internet Society, 2015 г. http://www.internetsociety.org/who-we-are/mission/values-and-principles

98. Динамическая коалиция по управлению Интернетом вещей (DC IoT) проявила особую активность в изучении влияния и проблем IoT в странах с развивающейся и переходной экономикой. См. соответствующие дискуссии на сайте DC IoT: http://www.iot-dynamic-coalition.org/.

99. Джеймс Маника и др. *Интернет вещей: ценности без рекламы*. McKinsey Global Institute, июнь 2015 г. стр. 4. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

100. Джеймс Маника и др., стр. 4-5.

101. См. список Целей устойчивого развития ООН на сайте: https://sustainabledevelopment.un.org/topics.

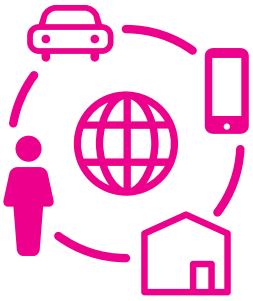
102. Участники Internet Society сформировали специальную группу, чтобы исследовать проблемы в точке пересечения Интернета, IoT и пищевого сектора. См. подробную информацию о специальной группе ISOC «Интернет и пищевые продукты» на сайте: http://internet-of-food.org/

103. Маартен Боттерман. *Доклад о будущем IoT-технологий: открывая новую реальность*. Краткий отчет № D5.2. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf

104. «Цифровые устройства для фермы и новая волна Интернета». *The Guardian*, 20 сентября 2015 г, раздел объединяя будущее. http://www.theguardian.com/connecting-the-future/2015/sep/21/digital-farm-set-for-internets-next-wave

ЗАКЛЮЧЕНИЕ

ЗАКЛЮЧЕНИЕ



Идея объединения компьютеров, датчиков и сетей для отслеживания и контроля устройств витала в воздухе на протяжении десятилетий, однако недавнее слияние ключевых технологий и тенденции на рынке открыли новую реальность «Интернета вещей». IoT обещает ввести нас в революционный, полностью интегрированный «умный» мир, где связь между предметами и их окружением, а также между предметами и людьми становится все теснее и теснее. Перспектива Интернета вещей как вездесущей сети устройств, привязанных к Интернету, может фундаментально изменить представления людей о том, что значит находиться в сети.

Потенциальные сложности значительны, и множество потенциальных проблем может преградить путь этому видению, особенно в сферах безопасности, конфиденциальность; интероперабельность и стандарты; юриспруденции, нормативов и прав, в том числе в развивающихся странах. Интернет вещей поднимает сложный и растущий комплекс технологических, социальных и политических проблем среди самых разных кругов заинтересованных лиц. Интернет вещей существует здесь и сейчас, и сегодня наблюдается потребность в поиске решений связанных с ним проблем и максимального использования его преимуществ с одновременным уменьшением риска.

Internet Society интересуют вопросы IoT, т.к. он представляет растущую проблему того, как люди и различные институты будут взаимодействовать с Интернетом и впускать сетевое соединение в свою личную, социальную и экономическую жизнь. Решения по максимальному использованию преимуществ IoT с одновременной минимизацией рисков невозможно найти, вступая в ожесточенные споры о перспективах IoT против его потенциальных опасностей. Вместо этого требуется активное участие на основе имеющихся данных, наличие диалога и сотрудничество различных заинтересованных сторон для поиска наиболее эффективных путей развития.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Различные организации, объединения и правительства прилагают большие усилия по всему миру, чтобы решить проблемы Интернета вещей. Ниже приведен список дополнительных источников информации. Конечно, этот список далеко не полный. Скорее, это исходная точка для дальнейших исследований.

Организации и альянсы, работающие в области Интернета вещей

AIOTI
Альянс по инновациям Интернета вещей был учрежден Еврокомиссией с целью поддержки развития европейской экосистемы IoT, включая разработку стандартов и норм. https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti

Альянс AllSeen
Индустриальная группа AllSeen, объединяющая 180 участников, продвигает идею широкого распространения протокола взаимодействия AllJoyn между устройствами и системами через IoT. https://allseenalliance.org/

ETSI
Европейский институт телекоммуникационных стандартов (ETSI) занимается разработкой стандартов безопасности данных, управления данными, передачи и обработки данных для подключения миллиардов «умных» вещей в одну коммуникационную сеть. http://www.etsi.org/technologies-clusters/clusters/connecting-things

IEC 62443/ISA99
Комитет промышленной автоматизации и контроля систем безопасности разрабатывает стандарты, технические отчеты и процедуры для внедрения безопасных систем промышленной автоматизации и контроля. http://isa99.isa.org/ISA99%20Wiki/Home.aspx

IEEE (включая P2413)
Институт инженеров по электротехнике и электронике (IEEE) осуществляет специальную инициативу IoT и имеет информационную службу для технического сообщества, занимающегося исследованием, реализацией и использованием IoT-технологий. http://iot.ieee.org/

IERC
Европейский совет по исследованию Интернета вещей координирует текущую деятельность в области IoT по всей Европе. http://www.internet-of-things-research.eu/

Целевая инженерная группа Интернета (IETF)
Это основной орган утверждения Интернет-стандартов, который имеет директорат IoT, координирующий соответствующие усилия среди своих рабочих групп, оценивает спецификации с точки зрения соответствия и отслеживает деятельность, связанную с IoT, в других группах стандартизации. https://trac.tools.ietf.org/area/int/trac/wiki/IOTDirWiki

IIC
Консорциум промышленного Интернета (IIC) объединил усилия с OIC, чтобы ускорить внедрение промышленного архитектурного шаблона для IoT. В 2015 году IIC выпустил эталонную архитектуру для IoT. http://www.industrialinternetconsortium.org/

Форум по управлению использованием Интернета (IGF)
IGF спонсирует динамическую коалицию IoT, которая проводит открытые собрания для обсуждения проблем использования IoT. http://www.intgovforum.org/cms/component/content/article?id=1217:dynamic-coalition-on-the-internet-of-things

Консорциум Интернета вещей
Эта промышленная группа занимается изучением потребителей и просвещением участников рынка для ускорения признания IoT-продуктов и услуг. http://iofthings.org/#home

Альянс IP для «умных объектов» (IPSO)
Альянс IPSO, занимающийся развитием Интернета вещей, продвигает использование протокола IP для подключения «умных объектов» путем информирования, исследований и рекламы. http://www.ipso-alliance.org/

ISO/IECJTC-1
В 2014 году ISO выпустила Предварительный отчет об Интернете вещей, а также Отчет об «умных городах». Группа имеет постоянные комитеты в обеих сферах. http://www.iso.org/iso/internet_of_things_report-jtc1.pdf

Группа «Интернет и пищевые продукты» ISOC
Специальная группа ведет дискуссию о стандартах технической инфраструктуры, которые будут актуальными для пищевой отрасли в будущем. http://internet-of-food.org/

ITU
Международный телекоммуникационный союз (ITU) учредил Глобальную инициативу по стандартам интернета вещей, которая завершила свою работу в июле 2015 года, после чего была сформирована новая Исследовательская группа 20 (Study Group 20), занимающаяся, главным образом, IoT-приложениями. http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx

Альянс MAPI
Альянс промышленников для производительности и инноваций (MAPI) работает над стратегией Индустрия 4.0 в сфере промышленного применения Интернета вещей. https://www.mapi.net/research/publications/industrie-4-0-vs-industrial-internet

OASIS
Компания OASIS разрабатывает открытые протоколы для обеспечения интероперабельности IoT-устройств. Группа выбрала протокол MQTT (Message Queuing Telemetry Transport) в качестве основного протокола обмена сообщениями между IoT-устройствами и оптимизировала протокол MQTT-S-N для беспроводных сенсорных сетей. OASIS учредила три технических комитета Интернета вещей, занимающиеся вопросами MQTT и двух других стандартов: AMQP (Advanced Message Queuing Protocol) и oBIX (OASIS Open Building Information Exchange). https://www.oasis-open.org/committees/tc_cat.php?cat=iot

oneM2M
Мультивендорная компания oneM2M занимается разработкой архитектуры и стандартов межмашинной коммуникации, главным образом, в сферах телемедицины, а также промышленной и бытовой автоматизации. Цель компании – разработка общей платформы управления и контроля M2M для внедрения в аппаратное и программное обеспечение. http://www.onem2m.org/

Online Trust Alliance
Данная группа поставщиков систем безопасности предложила первоначальный вариант платформы для IoT-приложений в сферах безопасности, конфиденциальности и устойчивости систем. https://otalliance.org/initiatives/internet-things

Open Interconnection Consortium
Консорциум OIC занимается разработкой общей коммуникационной платформы, основанной на промышленных стандартах, для беспроводного подключения и управления потоком данных между IoT-устройствами. OIC спонсирует проект IoTivity – систему открытых исходных кодов для взаимного подключения устройств. http://openinterconnect.org/

The Open Management Group
Этот консорциум по разработке технических стандартов занимается несколькими IoT-стандартами, включая протокол DDS (Data Distribution Service), язык IFML (Interaction Flow Modeling Language), а также моделированием надежности, угроз и унифицированных компонентов для систем реального времени и встроенных систем. http://www.omg.org/hot-topics/iot-standards.htm

Open Web Application Security Project
Открытый проект обеспечения безопасности веб-приложений (OWASP) спонсирует проект IoT Top-10 с предоставлением списка наиболее уязвимых для атак областей IoT с целью разъяснения проблем безопасности производителям, разработчикам и потребителям. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

Smart Grid Interoperability Panel
Комитет SGIP учредил инициативу EnergyIoT, концентрирующуюся на новых возможностях Интернета вещей в области энергетики. Энергетический проект OpenFMB объединяет общие энергетические модели данных и передачи данных в IoT-сфере для создания системы Open Field Message Bus. http://sgip.org/focus-resilience

Thread Group
Группа поставщиков решений «умного дома» занимается разработкой общих сетевых протоколов для бытовых IP-устройств (бытовых приборов, средств освещения, систем безопасности и т.д.). http://threadgroup.org/About.aspx

Политика правительства, исследования и координация взаимодействия

Австралия
Государственное объединение научных и прикладных исследований (CISRO) – это австралийское государственное научное учреждение, занимающееся исследованиями и разработками в сфере IoT-технологий. http://www.csiro.au/en/Research/DPF/Areas/Autonomous-systems/IoT

Китай
Правительство КНР выпустило Программу систематического и рационального развития Интернета вещей, отражающую политику Китая в области IoT. http://www.gov.cn/zwgk/2013-02/17/content_2333141.htm

Китай
Министерство промышленности и информационных технологий КНР выпустило 12-й пятилетний план с программой планирования развития IoT-сферы. http://kjs.miit.gov.cn/n11293472/n11295040/n11478867/14344522.html

Европейский союз
Европейская комиссия выпустила «Цифровую повестку дня для Европы: Интернет вещей» и работает со странами-участницами Евросоюза над будущим развитием и применением Интернета вещей. Она также составила списки европейских исследовательских проектов и пилотных проектов в области IoT. http://ec.europa.eu/digital-agenda/en/Internet-things

Европейский союз
Европейская экспертная комиссия по Интернету вещей (EO2514) – это группа экспертов по техническим, юридическим и организационным вопросам использования IoT по всей Европе. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2514

Индия
Министерство коммуникаций и информационных технологий Индии концентрирует усилия на разработке промышленной экосистемы IoT в качестве основной инициативы по преобразованию Индии в развитое цифровое общество и экономику знаний. http://deity.gov.in/content/internet-things

Республика Корея
В 2014 году Министерство науки, ИКТ и будущего планирования Республики Корея предложило «Генеральный план строительства Интернета вещей (IoT) для цифровой революции гиперсвязи» (см. документ на веб-сайте Корейской ассоциации IOT: http://karus.or.kr/uploadFiles/board/KOREA-IoT%20Master%20Plan.pdf).

Сингапур
Сингапурское государственное агентство SPRING, Управление по развитию инфокоммуникаций Сингапура (IDA) и Комитет по стандартизации информационных технологий (ITSC) Сингапурского совета по стандартам (SSC) выпустили План стандартизации Интернета вещей (IoT) для поддержки сингапурской инициативы «Умная нация». http://www.spring.gov.sg/NewsEvents/PR/Pages/Internet-of-Things-(IoT)-Standards-Outline-to-Support-Smart-Nation-Initiative-Unveiled-20150812.aspx

https://www.ida.gov.sg/Tech-Scene-News/Tech-News/Tag?tag=internet+of+things

Великобритания
В 2015 году главный научный советник британского правительства представил доклад, описывающий цели в IoT-сфере: «Интернет вещей: основа второй цифровой революции». https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

Великобритания
Регулирующий орган связи Великобритании Ofcom обозначил несколько приоритетных направлений для развития Интернета вещей, включая область доступности спектра, конфиденциальности данных, безопасности сетей, устойчивости и сетевых адресов. http://stakeholders.ofcom.org.uk/consultations/iot/next-steps/

США
Федеральная торговая комиссия США сформировала Бюро технологических исследований (OTRI) для изучения вопросов конфиденциальности, безопасности, платежей в области IoT и т.д. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

ПРИМЕЧАНИЯ И УВЕДОМЛЕНИЯ

Интернет вещей: краткий обзор
Вопросы и проблемы использования сети Интернет в более глобальном масштабе

Авторы:

Карен Роуз
Старший директор отдела стратегии и анализа Internet Society

Скотт Элдридж
Директор компании Cam & Sprocket LLC и независимый член Internet Society

Лайман Чапин
Директор компании Interisle Consulting Group и независимый член Internet Society

Авторы благодарят сотрудников межорганизационной рабочей группы Internet Society, которые помогли сформулировать концепцию данного материала и предоставляли критические замечания и отзывы на протяжении всей работы: Майкл Кенде, Грехем Минтон, Стив Ольшанский, Робин Уилтон, Грег Вуд и Дэн Йорк. Мы также благодарим следующих сотрудников общества Internet Society за значительный вклад в пересмотр данного материала и неоценимую помощь в виде конструктивных идей: Джойс Догниес, Олаф Колькман, Мегвн Крус, Тед Муни, Кристиан О'Флагерти, Маарит Паловирта, Бастиаан Куаст, Андрей Робачевский, Фил Робертс, Кристина Раннегар, Сэлли Уэнтворт, Фернандо Зарур и Ян Зорц.

Особая благодарность выражается участникам, коллегиям и партнерам Internet Society, которые щедро делились своим временем и опытом, оказывая неоценимую помощь по пересмотру и комментариям предыдущих версий данного материала: Николас Антониелло, Грюнелла Астбринк, Хусейн Бадран, Маартен Боттерман, Винт Серф, Шри Чандра, Глен Дин, Тим Дентон, Патрик Фальтштром, Джон Гаррити, Адрес Гомес, Ричард Хилл, Ховард Ли, Майк О'Рейрдан, Роберт Пеппер, Алехандро Пизанти, Чип Шарп, Берт Виджнен и Пол Уилсон.

Редактор: Кэролин Марсан
Дизайн обложки: Мишель Спеклер

См. подробную информацию на веб-сайте:
https://www.internetsociety.org/iot

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva, Switzerland
Тел.: +41 22 807 1444 • Факс: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA CB20190 USA
Тел.: +1 703 439 2120 • Факс: +1 703 326 9881
Эл. почта: info@isoc.org

report-InternetofThings-20151015-en