Перевод статьи:
Cerf V.G., Ryan P.S., Senges M., Whitt R.S. IoT safety and security as shared responsibility
Business Informatics. 2016. No. 1 (35). P. 7–19. DOI: 10.17323/1998-0663.2016.1.7.19.

Интернет вещей: безопасность и защита как коллективная ответственность

В.Г. Серф
вице-президент, Alphabet Inc.
Адрес: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: vint@google.com

П.С. Райан
директор по стратегии и операциям, Alphabet Inc.
Адрес: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: patrickryan@google.com

М. Сенгес
менеджер исследовательских программ, Alphabet Inc.
Адрес: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: maxsenges@google.com

Р.С. Витт
корпоративный директор по стратегическим инициативам, Alphabet Inc.
Адрес: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
E-mail: whitt@google.com

Что произойдет, если отдельные технические устройства приобретут сетевой интерфейс? Очевидно, что результатом будет беспрецедентное количество «вещей», подключенных к сети Интернет. Менее очевиден ответ на вопрос, что это будет означать для управления Интернетом. В свете концепции Интернета вещей (Internet of Things, IoT) взаимодействующие управленческие структуры уже приспосабливаются к тому, чтобы соответствовать эволюции применений Интернета. Однако, поскольку структура управления продолжает развиваться, безопасность пользователей становится приоритетом для всех поставщиков технических и программных решений. В контексте Интернета вещей в данной статье предлагается определение цифровой безопасности, отличающееся от защиты данных, а также обсуждается то, как управление, затрагивающее различных заинтересованных лиц, может применяться для обеспечения такой безопасности. В работе также рассматриваются вопросы интеграции «старых» отраслей и трансформации управления ими в «мультистейкхолдерную» модель по мере того, как их продукты и услуги становятся онлайновыми. Обсуждается, как тысячи производителей, традиционно производящие не связанные между собой «вещи», адаптируются к роли стейкхолдеров Интернета и как это изменяет наше представление об управлении Интернетом. Особое внимание в статье уделено тому, как это связано с вопросами безопасности, которые становятся все более актуальными в связи с широким распространением Интернет-ориентированных физических устройств.

Авторы выполнили данную работу в академических целях, на основе своего видения рассматриваемых вопросов. Мнение авторов может не совпадать с официальной позицией их работодателя.

Ключевые слова: Интернет вещей, управление Интернетом, безопасность, защита, множественные стейкхолдеры.

Цитирование: Cerf V.G., Ryan P.S., Senges M., Whitt R.S. IoT safety and security as shared responsibility // Business Informatics. 2016. No. 1 (35). P. 7–19. DOI: 10.17323/1998-0663.2016.1.7.19.

Перевод статьи:
Cerf V.G., Ryan P.S., Senges M., Whitt R.S. IoT safety and security as shared responsibility
Business Informatics. 2016. No. 1 (35). P. 7–19. DOI: 10.17323/1998-0663.2016.1.7.19.

Введение

Что происходит, когда обычные автономные устройства и машины начинают использовать сетевые интерфейсы? Определенным очевидным результатом будет беспрецедентное число «вещей», подключаемых к Интернету. Менее очевидным в этом случае будет то, как это отразится на управлении Интернетом. С возникшим феноменом, названным «Интернетом вещей» (Internet of Things, IoT), этот сценарий разворачивается прямо сейчас, и слабо связанные с Интернетом управляющие структуры уже изменяются, чтобы адаптироваться к нему. Начиная со смартфонов, миллионы устройств находятся в режиме онлайн, и в настоящее время охватывают самые разные устройства – от наших автомобилей до видео-охранных и бытовых термостатных систем [8]. Возникает вопрос, как тысячи изготовителей, которые традиционно производили аналоговые, не связываемые с другими физические «вещи», становятся заинтересованными в Интернете, и как это изменяет то, что мы думаем об Управлении Интернетом. Особый интерес представляет то, как решать вопросы безопасности, которые все более бросаются в глаза по мере распространения подсоединенного к Интернету физического окружения. Мы также рассматриваем интеграцию «старой» промышленности и трансформацию управления ими в многостороннюю модель.

У Интернета нет единственного заинтересованного лица и какой-либо единственной категории лиц, которые несут основную ответственность за его управление. Здесь имеет место ответственность, разделенная между всеми заинтересованными лицами. Мы доказываем, что проблемы, которые вносит IoT, будут разрешены с помощью того же многостороннего механизма, который управляет самим Интернетом. Это действительно так, поскольку «вещи», в настоящее время связанные с Интернетом, явно не принадлежат какому-либо одному заинтересованному лицу, и управление через Интернет продолжает оставаться делом разделенной ответственности [3]. Кроме того, существующая система управления должна принимать во внимание машины, которые становятся более «автономными» (т.е. «умными», благодаря обучению машины и т.д.). В этих условиях мы полагаем, что концепция цифровой безопасности, в частности, рассматривается как концепция ответственности, разделенной между всеми группами участников.

1. Переход от цифровой защиты к цифровой безопасности

Свобода в отношении инноваций в своей основе включает ответственность в деле защиты законных интересов пользователей и целостности экосистемы, которая их соединяет. Это предположение особенно оправдано, когда Интернет распространяется в физическом пространстве, и когда продолжает расти количество используемых протоколов следующего поколения и искусственного интеллекта.

1.1 На поле выходят новые игроки

Миллионы новых взаимно соединенных вещей обеспечивают намного больше возможностей в использовании их уязвимости. Эти проблемы возникают в таких платформах, как устройства связанных с Интернетом замкнутых систем телевизионных наблюдений (CCTV). Поскольку устройства современных CCTV – это цифровые камеры, которые обрабатывают большие объемы видеоданных, они используют нетривиальную компьютерную обработку и большие объемы памяти. Во всем мире установлено свыше 245 млн. видеокамер, и их существенная зона обслуживания, осуществляемого через Интернет, недавно привела к различным сервисным атакам [9].

1.2 Как сегодня распределена ответственность

Как сегодня «обитатели» Интернет делят ответственность между собой? Частный сектор здесь «играет свою партию». Все такие компании, как Cisco, Facebook, Google и Verizon, зависят от доверия пользователей и, следовательно, у них имеются сильные стимулы надежно охранять данные, а также детей и близких от опасности мошенничества, выявлять злоумышленников и всякого рода «хищников». Государственные учреждения, как и другие заинтересованные лица, несут значительную ответственность, ввиду необходимости устанавливать законы и правила, наказывать за плохое поведение и принуждать к выполнению законов и правил. Кроме того, группы гражданского общества и неправительственные организации сыграли ключевую роль в разработке Интернета и продолжают анализировать и оценивать практику частного сектора и устанавливать нормы и принципы онлайн-поведения. Очень важно то, что пользо-

ватели Интернета должны нести ответственность и учиться использовать такие инструменты, которые обеспечивают безопасный и защищенный онлайн-опыт.

1.3 Неудобные компромиссы и разделение ответственности

Для некоторых групп участников может оказаться необходимым обмен неудобств на защиту и безопасность. Иллюстрацией может служить использование двухфакторной идентификации. Эта иллюстрация применима к тем пользователям и организациям частного сектора, которые пользуются такой идентификацией. В сети идентификация пользователя обычно включает в себя комбинацию трех факторов: (1) то, что пользователь знает (например, пароль); (2) то, что пользователь имеет у себя (например, USB-ключ, возможно, приложение в телефоне); и/или (3) то, что является личным для пользователя (например, биометрия: отпечатки пальцев или скан радужной оболочки). Большинство современных систем используют просто один фактор, но применение двух (и более) факторов обеспечивает более надежную защиту. При многофакторной идентификации в практику пользователя включается нетривиальное дополнительное неудобство для оказания помощи в приведении доказательств, что пользователь – именно тот, кем он себя называет.

Поскольку трехфакторная идентификация сегодня используется менее часто, дальше будем пользоваться двухфакторной идентификацией. Большинство логинов сопровождается именем пользователя и паролем – формой однофакторной идентификации. В определенных случаях может использоваться второй фактор: это обеспечивается пользователем за счет применения дополнительного кода – СМС, телефонного вызова, USB-устройства или программного приложения. Хотя второй фактор и обеспечивает лучшую защиту, он также может создавать для пользователя некоторые неудобства. Например, если пользователь спешит и для доступа к своему банковскому счету вводит свой идентификатор и пароль, может быть весьма неуместным искать телефон, для того чтобы получить текст с дополнительным кодом. Это может оказаться даже более неудобным, если выданный компанией ключ требуется ввести в компьютер – если у работника с собой нет ключа, и работа может не быть выполнена. Но даже при всех этих неудобствах пользователи все чаще соглашаются терпеть их (и компании все более настаивают на этом), поскольку понимают, что это помогает оставаться в онлайн-безопасности и им самим, и их данным. Как таковое, применение двухфакторной идентификации – хороший пример того, какой вклад пользователь делает в безопасное Интернет-окружение, даже если это делается за счет его личного времени и удобств. Иными словами, те пользователи, которые применяют двух- или трехфакторную идентификацию, сознают свою долю ответственности, которая приходится на них в частном секторе в отношении безопасности их данных.

Важно помнить о разделении ответственности при разборе любого инцидента с защитой. Когда компании Sony не удалось защитить пользовательские данные при серьезном нарушении в 2014 году, компания немедленно заявила об аннулировании своих обязательств по защите пользователя [15]. Не вызывает сомнений, что Sony несет свою долю ответственности за нарушение, но также важно, что правительство, гражданское общество и техническое сообщество должны принять на себя некоторую ответственность за систему, которая в значительной степени не выполнила то, что должна была делать. В случае нарушения со стороны Sony пользователи могут не быть снабжены надежным механизмом восстановления нарушения, допущенного компанией. Например, если пользователи этой компании могли бы иметь двухфакторную идентификацию для своей электронной платежной системы PlayStation, возможно, нарушение данных Sony было бы менее серьезным, или даже незначительным. С практической точки зрения маловероятно, что любое нарушение было бы способно нарушить одновременно защиту ядра и защиту каждого из миллионов отдельных двухфакторных пользовательских устройств.

Возможно, что двухфакторная идентификация не была предусмотрена в качестве варианта для пользователей Sony. В любом случае, для достижения необходимого прогресса остается только признать ответственность всех заинтересованных лиц. Мы полагаем, что политика будет развиваться в направлении того, что такая технология, как двухфакторная идентификация, будет использоваться в качестве наилучшего практического метода, который будет применяться настолько широко, что станет де-факто обязательным стандартом, который требуют пользователи, а также гражданское общество или техническая сообщество. В будущем пользователи обязательно будут требовать эти дополнительные свойства.

Для того чтобы стандарт стал фактическим требованием, стоимость неиспользования стандарта должна быть выше, чем стоимость его использования. Как производятся такие расчеты? Они выполняются различными способами, иногда под давлением со стороны членов своего круга, в других случаях – с помощью судебного постановления или законодательного указа. По аналогии с другими областями, рассмотрим случай проверки на наличие глаукомы специалистом-оптиком во время любой регулярной проверки глаз. Шансы выявления любой отдельной глаукомы очень низки – менее 1%. Однако ее последствия очень серьезны (приводят к слепоте), а стоимость проверки на наличие глаукомы чрезвычайно низка – всего пара долларов. Ясно, что это требует анализа соотношения затраты/прибыль. По этой причине за счет совместного воздействия судебных тяжб, законотворчества и давления со стороны госпиталей сначала де-факто, а затем и де юре, возник стандарт, который требует, чтобы проверку на наличие глаукомы специалист-оптик включал в свои регулярные процедуры. Вот почему, когда пациент проходит регулярную проверку зрения, часто (хотя и не всегда), проводится проверка на наличие глаукомы (например, путем расширения глаз и/или коротких импульсов воздуха). Мы полагаем, что это явление будет применяться в технологиях, которые подобны двухфакторной идентификации и все более доступны, когда становится понятно, что последствия нарушений будут слишком тяжелы для общества.

Конечно, любая компания или организация несет ответственность за защиту своих пользователей и их данных. Эта ответственность не должна быть сведена к минимуму. Однако после разборки конкретных инцидентов многие, кто требовал более строгих законов и лучшего механизма их реализации, демонстрируют сценарий, который относится больше к сенсационности, чем к практической реализации. Конечно, стандарты и законы очень важны. Однако мы не должны позволять, чтобы жесткость наших правил и систем заставляла нас уходить от сосредоточенности на более цельном видении защиты Интернета, при которой не обращается внимание на качество «дверного замка», а охватывается в полной степени роль всего того, что имеется у всех заинтересованных лиц в Интернет-сообществе. Пресса устроила сенсацию в отношении атак на Sony, но лишь незначительное внимание было обращено на те меры, которые компания или пользователи могли бы предпринять для минимизации риска. Оказывается, что Sony могла приобрести у компании DigiCert цифровые сертификаты с двухфакторной опцией для их подтверждения с помощью аппаратного маркера [19]. В этом случае, даже если информация о сертификатах стала бы доступна, двухфакторная опция обеспечила бы «безотказность» со сведением ущерба к минимуму. Это защитная роль относится к разделенной ответственности для создания и поддержания безопасного онлайн-окружения. Ясно, что не все заинтересованные лица все время в одинаковой степени разделяют ответственность, но, вне всякого сомнения, ответственность редко, если не никогда, возлагается на единственное заинтересованное лицо.

1.4 Цифровая безопасность, отличающаяся от онлайн-защиты

Мы предлагаем четко различать концепции цифровой безопасности и онлайн-защиты. Мы считаем цифровую безопасность принципом, защищающим пользователей от ущерба, который может быть вызван системами, все более становящимися полуавтономными и являющимися смесью услуг различных разработчиков. Примером этого могло бы служить применение «восстанавливаемых после отказа» (или, возможно, «отказоустойчивых») решений в случае, когда часть системы перестает функционировать. В нашей модели восстанавливаемые после отказа системы разработаны не с целью защиты от любого нарушения, а в предположении, что нарушения могут быть, а восстановление после отказа обеспечивается за счет определенного решения.

В отличие от этого, онлайн-защита – мера, которая обеспечивает защиту системы от злоумышленников, а не способ, которым действует система для защиты пользователей, когда возникает проблема. Поскольку само по себе восстановление после отказа не является защитой, важна также хорошая защита для предотвращения необходимости в восстановлении после отказа. Это – серьезное отличие от «традиционных» практических мер по защите, которые более терпимы к ошибкам системы при условии, что последствия являются «только» виртуальными и информационными (например, «Тревога! Нарушение защиты!»), а не защищающими пользователей от материального или физического ущерба. С учетом этого другого пути для отличия безопасности от защиты мы предлагаем следующую таксономию:

✦ **Цифровая безопасность** – это защита пользователя в его окружении с помощью технических ме-

ханизмов и мер, которые защищают его от ущерба при неправильной работе устройства.

✦ **Онлайн-защита** – это защита физической сети, операционных систем и контента от воздействия, изменения или функционального ущерба, с использованием комбинации программных и аппаратных механизмов.

В приведенной выше таксономии обе категории могут включать упреждающее действие, а также восстановление после отказа. Устройство открытия двери гаража является примером, в котором первостепенным требованием является безопасность. Обычно гаражная дверь может открываться по сигналу, подаваемому со смартфона или радио-ключа. Если по каким-либо причинам это сделать не удается, важно (с точки зрения безопасности), чтобы дверь могла открываться вручную путем ее отсоединения от средств механизированного управления. Это обычно выполняется с помощью механизма физического высвобождения. Обычно этот механизм доступен только изнутри гаража. Выход из строя управления не удерживает пользователя, и в то же время система находится в безопасности, поскольку дверь не открывается снаружи. В результате пользователь – в безопасности, а гараж – в сохранности.

Можно представить и другие интеллектуальные устройства (такие как термостаты), которые могут управляться и контролироваться дистанционно. Для обеспечения безопасности следовало бы не позволять температуре подниматься выше некоторого максимального уровня. Тот же стандарт также мог бы применяться и к водонагревателю. Даже если послана команда превысить установленные пределы, безотказная конструкция препятствовала бы превышению заданных уровней. Для обеспечения защиты следовало бы обеспечить невозможность или, по крайней, сделать непростым для неуполномоченной стороны управлять или контролировать термостат. Для достижения цели защиты можно было бы использовать двухфакторную идентификацию.

Подводя итоги, отметим, что цифровая безопасность сосредотачивается на конечном пользователе, его интересах и здоровье, в то время как онлайн-защита фокусируется на защите других аспектов сети или самого устройства. Конечно, при некоторых видах неисправностей мог бы быть получен результат, который поднимал бы проблему безопасности, например, в случае злоумышленника, управляющего устройством так, чтобы вызывать возгорание. Различные проблемы защиты определяются с точки зрения IoT на новом уровне из-за повышенной возможности у взломщиков достичь фактического оборудования, используемого для обнаружения, привода в действия и управления. Пока эти устройства находятся в режиме онлайн (например, местное радио, локальная сеть), прямой доступ представляет собой дополнительную опасность. Кроме того, программное обеспечение могло бы быть изменено, чтобы делать все, что предполагается делать для работы устройства, а затем генерировать спам, атаку с целью нарушения нормального обслуживания пользователей или другие опасные действия. Пользователь может не знать о проблеме, если работа устройства не выявляет никакие признаки злонамеренного вмешательства. В отношении безопасности реальная проблема состоит в том, что такие чрезвычайно сложные комплексы IoT (состоящие из аппаратной и программной части и «зашитых» программ) могут иметь дефекты. Как альтернатива, бездефектная система все же могла бы генерировать непредусмотренные наборы сигналов и приводить к результатам, которые препятствовали бы безопасной работе.

1.5 Связывание неразрешенной инновации и разделения ответственности

В условиях неразрешенной инновации любое предприятие способно использовать сеть для доставки новых продуктов и услуг неограниченному множеству пользователей. Такая потрясающая возможность приносит с собой то, что неразрешенная инновация может причинять пользователям вред. Мы предлагаем, чтобы существовал баланс между восприятием «хорошей» и «плохой» неразрешенной инновации. Вместо этого имеется тройное пересечение между разрешенной инновацией, свободой действий и сопровождающей это ответственностью, которую каждый участник делит с целью защиты пользователей. Для общественности в этом пересечении имеется большое пространство для выработки новых решений.

Для обеспечения того, что новаторы могут экспериментировать и создавать новые решения и продукты, было бы возможным содействовать развитию культуры и принятию бета-тестирования для доступа к выигрышным свойствам ранних версий свойств и продуктов. «Бета-тестирование» – это способ поддержки экспериментирования, проводимого его приверженцами, путем предоставления нового набора функциональности в обмен на понимание, что вещь может не работать в полной мере

[5]. Однако важно, что это ожидание ясно и прозрачно сообщается пользователям (и выполняется при поддержке пользователя, идеально – при наличии у него энтузиазма). Более открытый подход, существующий между частным сектором и пользователями в отношении характера их продуктов и возможных рисков, мог бы быть способом ограничить ответственность для новаторов, с сохранением стимулирования экспериментов, и обеспечить, чтобы пользователи были извещены о рисках и были согласны принять их. Такая система может оказаться никогда не быть принятой по любому закону или решению любого суда, но промышленность могла бы объединиться для содействия открытому стандарту для бета-тестирования и системе информирования о ней пользователей. Вещь этого вида в некоторой степени существует на примере американской организации CreativeCommons, публикующей добровольную систему, которую издатели могут использовать для заключения контракта с пользователями для использования их работ.

Как многосторонняя общественность реагирует на призыв к действию, если имеет место глобальный инцидент с защитой Интернета? Прекрасной иллюстрацией этого является «Рабочая группа по Conficker». В 2009 году компьютерная сеть хакеров Conficker оказалась самой изощренной сетью своего времени. В течение недель эта сеть инфицировала миллионы компьютеров, в том числе государственные, деловые и домашние компьютеры, во всех 193 странах. «Рабочая группа по Conficker» (http://www.confickerworkinggroup.org) была собрана быстро (и неофициально) и состояла из участников частного сектора (таких как компании Microsoft и Symantec), академических исследователей и НКО (таких как ICANN и Shadow Server Foundation). В группу также были включены различные правительственные представители.

«Рабочая группа по Conficker» проводила свою работу без официального мандата и действовала вне рамок какой-либо формальной структуры. Это была свободно собранная группа представителей всех секторов, которые были объединены вместе с единственной целью быстрой остановки распространения Conficker. Тот факт, что группа не имела особого мандата, бюджета и особых формальностей, позволил ей сформироваться и действовать быстро и обдуманно. Для остановки одного из вирусных «штаммов» сотрудники «координировали работу более чем со 100 странами и блокировала свыше 50000 доменов в день» в течение менее трех недель [7]. Этот вид мобилизации и ответственности оказался возможным благодаря свободно объединенной и неформальной системы управления, которая была создана для решения конкретной проблемы.

2. Заявка на Интернет Вещей

В течение первых двадцати пяти лет коммерческой деятельности сеть Интернет в основном состояла из управляемых пользователями концевых точек и серверов. Структура сети описывается также как модель «точка-точка», которая означает, что наиболее «интеллектуальная» часть оказывается на краю сети, т.е. в устройстве, которое подключено к ней. Сегодня само физическое окружение «оживляется», и оно растет и процветает в облаке сетевых устройств. Это – Интернет Вещей (IoT): ментальная конструкция или принцип заказа, который мы используем для описания усилий по переходу Интернета на следующий более высокий физический уровень. Действительно, IoT – просто сам Интернет, но с одной отличающейся особенностью: онлайн-деятельность – не только информационная, она включает в себя взаимодействие с «вещами», встречающимися в жизни и часто имеющими физические последствия. Кроме того, эти взаимодействия будут все в большей степени определяться некоторой формой машинного интеллекта, которые позволяет «вещам» координироваться полуавтономно.

IoT определяется как «всепроникающая и самоорганизующаяся сеть соединенных, опознаваемых и адресуемых физических объектов с использованием микропроцессоров» [18]. Развитие IoT описывается созданным недавно компанией Cisco брендом «Интернет Всего». Это звучит всеобъемлюще, так как бренд описывает связь через сеть людей, процессов, вещей и данных. Вещи – это все неодушевленные физические объекты и устройства – датчики, потребительские устройства и активы предприятий, в то время как процессы – это описание того, как люди, данные и вещи работают вместе [6]. Как объяснил Дэвид Килпатрик, «мы распространяем соединяемость Сети к гораздо более широкой всемирной паутине, которая включает в себя магистральные физические объекты мира, позволяя им отвечать на программу, которая делает понятным то, что эти объекты говорят нам» [12]. Таким образом, как считает Нейл Кросс, Интернет может продолжать свой рост по всему миру как «электронная кожа», которая касается всех аспектов жизни: «В следующем столетии планета Земля наденет электронную кожу. Она будет использовать Интернет как подмост-

ки для поддержки и передачи своих ощущений. Эта кожа уже объединена. Она состоит из миллионов встроенных измерительных устройств: термостатов, манометров, датчиков загрязнения, видеокамер, микрофонов, глюкометров, ЭРГ, электроэнцефалографов. Это будут города датчиков и мониторов и исчезающие виды, атмосфера, наши корабли, автомагистрали и флотилии грузовиков, наши разговоры, наши тела – и даже наши мечты» [10].

Однако мы выбираем следующее описание будущего Интернета: он велик, и вещи, использующие его, больше не являются исключительно человеческими. Это может казаться сейчас аксиоматическим, но, когда явление IoT отбрасывается, условия политики будут нуждаться в адаптации для приспособления к перемещению.

2.1 Проблемы политики IoT

В отношении IoT существуют проблемы политики. К счастью, большинство них относится к существующему закону или процессу политики без какой-либо необходимости в новом адаптированном законодательстве. Например, сетевые стандарты, разработанные для IoT, с сопровождающими вопросами относительно способности к взаимодействию и свойству быть собственностью, могут иметь отношение к таким разрабатывающим стандарты организациям, как Институт инженеров по электротехнике и электронике (IEEE), Инженерная группа по развитию Интернета (IETF) и/или другие неправительственные организации. Подобно этому, вопросы генерирования вездесущей соединяемости включают взаимоотношения с национальными и международными органами, назначающими спектр частот.

В связи с возникновением IoT мы отмечаем две новые проблемы главной политики: (1) интеграцию изделий «старой» промышленности и трансформацию их управления в многостороннюю модель и (2) цифровую безопасность, которая не является целиком новой, но становится все более распространенной, поскольку соединяемость продолжает охватывать все новые физические пространства.

2.2 Интеграция изделий «старой» промышленности в сеть многостороннего управления

С одной стороны, традиционные бизнес-компании оцифровывают свои средства производства и нуждаются в обеспечении безопасности и других надлежащих практических методах в отношении своих работников (а также в отношении пользователей своей продукции). С другой стороны, произведенные изделия (или «вещи») теперь могут подключаться к Интернету, и поэтому компании становятся частью существующей экосистемы управления Интернетом. Эта вторая категория известна также как «Промышленный Интернет» (или сети машина-машина, или в Германии «промышленность 4.0»). Перспективы промышленного Интернета – возможности создавать сети создания стоимости в производстве, логистике, техническом обслуживании и бизнесе, которые обеспечивают возрастающий информационный охват, поток, совместное пользование и производительность. В промышленной сфере IoT это в основном частный сектор, который владеет оборудованием и несет ответственность за его защиту. Следовательно, производители и бизнес-компании будут нести ответственность за обеспечение того, что их продукция, работа и условия развития будут безопасными. В этих условиях для установления правил будет важна традиционная роль правительства. Исходя из этого, представляются интересы работников, и практика компаний тщательно изучается профсоюзами. Наконец, судебная система, общественное внимание и давление со стороны своего круга несут ответственность за проведение в жизнь.

Другая проблема существует в отношении введения и интеграции изделий традиционной промышленности в экосистему Управления Интернетом. Это сделать значительно труднее из-за большого объема новых участников, которых IoT приводит с собой, и неоднородности проблем политики. Тем не менее, мы столкнулись с задачей введения методов и получения опыта от многосторонности в условиях управления Интернетом в сферах политического и частного сектора (производства, развития городов, потребительской электроники). Эти сферы традиционно использовали более ограниченный круг среди разнообразия локальных и глобальных участников в их практических методах принятия решений. Естественно, становятся более важными и стимулирующими концепции, подобные конфликтам наслаивания или схематического изображения, так что «борьба» в этой части управления продуктивна и может быть рассмотрена, а затем решена, плеядой многих участников (в нужном слое).

2.3 Роль частной жизни в дискуссиях

С точки зрения пользователя, вопрос, кто контролирует информацию о пользователе и его окружении, является новым, когда это относится к миру соединенных вещей. То, является ли эта информация адекватно защищенной от неправильного использования государством или частными лицами, естественно, вызывает опасения. Вот только один пример: можно ли отказаться от устройств и датчиков, которые помогают включиться в ближайшее окружение? И является ли частная жизнь спорной, только когда объекты встречают субъектов?

Хотя основным в нашей статье является различие между безопасностью и защитой, многие агентства защиты потребителя, которые занимаются безопасностью потребителей, также несут ответственность за защиту частной жизни. Мы здесь не занимаемся этой темой в полном объеме, хотя и полагаем, что IoT, вероятно, для многих агентств по защите потребителя является входом в область управления по многим темам, включая частную жизнь. В Европе, например, действуют несколько директив и нормативов, которые относятся к цифровому рынку и нацелены на широкую защиту прав потребителей, включая частную жизнь. К этим директивам относятся: Директива 2011/83/EU по правам потребителя, Директива 95/46/EC по защите личности в отношении обработки персональных данных, Директива 2000/31/EC по определенным правовым аспектам услуг информационных обществ, Директива 2002/58/EC, касающаяся обработки персональных данных и защиты частной жизни в секторе электронных коммуникаций и многие другие. Хотя анализ важности этих законов и их воздействия на IoT – это тема другого исследования, мы полагаем, что важно выявить некоторые из областей изучения в частной жизни.

Переход от «малых данных» к «большим данным» требует некоторых изменений. Например, не все данные будут персонально идентифицируемыми, а рост объема данных заставит сосредоточиться на окружении, инфраструктуре и поведении других устройств и вещей в Интернете. Некоторые данные могут попасть с серую зону, где могут быть возможны пророчества или разоблачения в отношении личностей. Следует сосредоточиться не на сборе данных, а на том, наносит ли это вред (т.е. зависимость между использованием и сбором). Из-за этого смещения в использовании Интернета концепции, подобные уведомлению и отбору, в будущем будут менее полезными, чем правила «минимизации данных» [2]. В этих условиях распределенный интеллект в сети может выявлять и защищать от угроз, даже когда он может распространять угрозы по всему пользовательскому окружению.

2.4 Рамки политики конкуренции

Подобно самому Интернету, глобальное скопление вещей бросает вызов национальным границам и барьерам. IoT – не единая система, она включает в себя много перекрывающихся сетей, относящихся к открытым, закрытым и частично открытым системам. Многообразие разных архитектур и программных приложений не предполагает никакой централизованной структуры управления; в Интернете большинство пользователей – это частные компании и пользовательская собственность, некоторые являются государственными.

Один из путей анализа рамок политики конкуренции – рассмотрение их сквозь линзу Форума по управлению Интернетом (Internet Governance Forum, IGF). Этот форум действует с 2006 года и собирается ежегодно по приглашению страны-организатора. Консультативная группа из заинтересованных сторон (MAG), руководимая председателем, назначенным Департаментом ООН по экономическим и социальным делам (UNDESA), организует ежегодные встречи, принимающие решения по предлагаемым темам, которые будут включены в повестку дня. Для формулирования вопросов и обмена мнениями о перспективах используются различные форматы.

Форум IGF рассматривал IoT в самых разных случаях. Имеется Динамическая Коалиция Интернета Вещей, но, насколько нам известно, эксперты до сих пор считали, что никакое специальное управление IoT не гарантировано, поскольку это «просто» другое Сетевое приложение. А если это так, то на данной ранней стадии развития IoT следует ли обсуждать ответственность? Мы полагаем, что сейчас для этого самое время, поскольку еще есть возможность «скорректировать траекторию» и сообщить о выборе. Мы полагаем, что дебаты о том, как разделять ответственность за безопасность IoT, должны вестись на всех уровнях и всеми сторонами. Даже при этом мы согласны, что, поскольку преимущества и недостатки мира IoT на ранних стадиях выявить трудно, лица, принимающие решения, должны быть и гибкими, и не принимать решений, которые быстро устареют.

3. Эволюция Управления Интернетом

Поскольку Интернет – разделяемая система, то ответственность за ее управление тоже разделяема. Если выражаться кратко, форма Форума по управлению Интернетом должна соответствовать его функциям. Как же может выглядеть режим разделенной ответственности за безопасность IoT? Мы ранее высказали мнение, что «форум следует за функциями» в условиях Форума по управлению Интернетом [4]. Это означает, что форум IGF обладает способностью выполнять следующие функции: (1) выявлять возникшие проблемы IoT с безопасностью; (2) упрощать создание многосторонних рабочих групп, которые создаются для разработки решений; и (3) контролировать эффективность этих решений, проводить открытый анализ и обсуждение, критику и предложения по изменениям или признанию наличия проблемных явлений.

В Интернете традиционные регулятивные практические методы стараются идти в ногу с инновациями. Более традиционный подход к управлению «сверху вниз» подавил бы выгоды самого пользователя, которые заинтересованные стороны стараются усилить. Это означает, что, не обеспечивая единственного универсального и многостороннего метода управления Интернетом, неформальные практические методы, которые привели сегодня Интернет в поразительное состояние постоянного роста и эволюции, будут сами по себе продолжать приносить новые и инновационные системы управления, примкнувшие «по дороге». Правительства важны, но они не играют исключительную, доминирующую роль, действующую сверху вниз. Вместо этого правительства принимают участие на равных условиях как представители своих соответствующих составных частей. Эти составные части – от частного сектора до гражданского общества и технических экспертов – часто борются с представителями правительств и других заинтересованных сторон по каждому отдельному вопросу и в каждом отдельном случае. С использованием инклюзивного и прозрачного процесса это помогает создавать истинно глобальную сферу управления.

Какова сфера действия каждой из этих групп в области поддержке IoT? Несколько таких ролей включают в себя следующее:

✦ **Государство.** Устанавливать высокий, но преодолимый барьер для защиты граждан, с двумя целями: поддержки (например, защиты потребителя, а также здоровья и безопасности) и образования (например, фишинг требует от потребителя аккуратности, и никакая система не может полностью защитить от него).

✦ **Частный сектор.** Создавать по возможности наиболее безопасную систему и участвовать в обучении тому, как наилучшим образом использовать имеющиеся инструменты. Запрашивать способы вовлечения пользователей в качестве партнеров в обеспечение лучшей безопасности и защиты.

✦ **Гражданское общество.** Представляет перспективы в отношении интересов пользователя и общества. Гражданское общество играет ключевую роль в проверке функционирования системы сдерживания и противовесов для государственных институтов и в поддержке технологических инноваций. Оно также обеспечивает связь между государством и частным сектором. Кроме того, также есть образовательные цели распространения цифровой грамотности, к которым относится обучение пользователей безопасности и защите. Наконец, гражданское общество находится на переднем крае в деле защиты прав человека в опасных частях мира и обучении граждан онлайн-безопасности.

✦ **Техническое сообщество.** Техническое сообщество убеждается, что стандарты правильно продвигаются (например, за счет работы группы IETF) и что в критической инфраструктуре реализуются защиты и надлежащие методы практики (подобно DNSSEC). Хотя каждая группа имеет свой собственный образовательный мандат, техническое сообщество также (совместно с гражданским обществом) использует некоторые подобные образовательные цели для обучения всех групп заинтересованных лиц (и, в частности, пользователей) в деле правильного проектирования и функционирования различных систем.

Как мы полагаем в дальнейшем в отношении смысла безопасности, полезно идентифицировать то, как эти концепции могут быть найдены различными способами в разных слоях Интернета. Здесь мы полагаем, что наиболее удобно рассматривать эволюцию Интернета (и управление им) в виде «слоеной модели» [4]. Как мы наблюдаем в различных частях каждого сетевого слоя, ресурсы (и, следовательно, заинтересованные лица) являются сочетанием частного и государственного секторов. Только логический слой представляет собой ресурс, в основном, являющийся общим достоянием. В результате во всех слоях (за исключением логического) сочетание частных и общественных товаров

означает, что ответственность в вопросах безопасности остается на сочетании частных и общественных действующих лиц. В отличие от этого, логический слой действует в ином режиме управления по сравнению с другими – в таком, который является причиной этих материальных различий. Здесь ответственность в вопросах безопасности в целом лежит на подходящем многостороннем сообществе, осуществляющим управление (а не распределенном среди всех заинтересованных лиц). Мы основываемся на слоеной модели, применяемой ниже к IoT.

3.1 Место IoT в существующей модели управления

Как вопросы управления, относящиеся к IoT, связаны с управлением остальной частью Интернета? На *рис. 1* мы построили модель, которую мы ранее предложили, но модифицировали ее для включения некоторых отобранных заинтересованных лиц, которые непосредственно связаны с управлением IoT. Как можно увидеть из приведенного ниже описания, наиболее важная зона деятельности в управлении IoT будет находиться в слое контента.

В инфраструктурном слое, расположенном в нижней части *рис. 1*, находится физическая основа сети. Права пользования, полюса и зоны, используемые совместно с другими провайдерами, иногда описываются как «клубные блага», обеспечиваемые частными ISP (провайдерами услуг Интернета), и это сходится с инфраструктурой, предоставляемой коммунальными предприятиями (для обеспечения электроэнергией, водой, дорогами и светом). Практика управления в физическом слое определена относительно хорошо, даже если инновации сталкиваются с традициями (например, регулирование услуг, подобных предоставляемым станцией HAPS). Расположенный над инфраструктурным слоем логический слой демонстрирует более содержательную историю моделей управления разносторонними участниками с активными группами, подобными ICANN, IETF, IEEE и другим. В адаптации этих групп к конкретным заинтересованным сторонам IoT должны участвовать соответствующие институты.

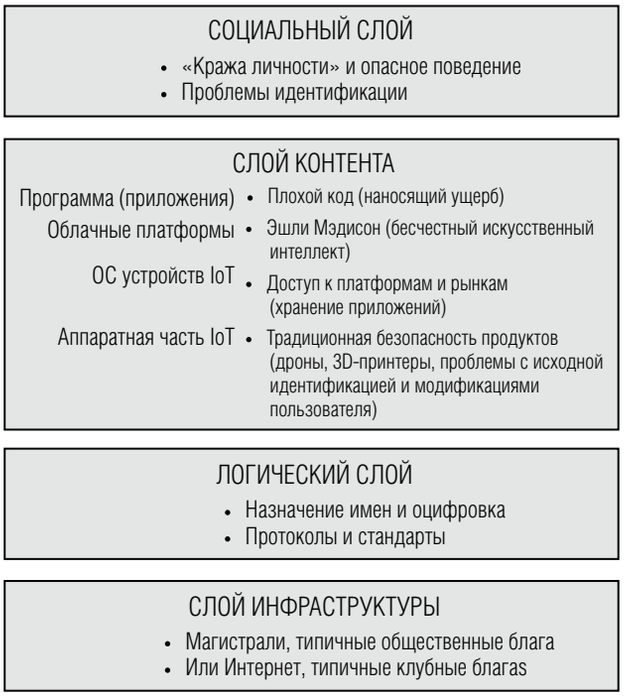

Рис. 1. Слоеная модель Управления Интернетом, адаптированная к Интернету Вещей

Большинство проблем, связанных с управлением IoT, окажется в слое контента и выше него. Из-за наличия этой тенденции те институты, которые в настоящее время занимаются управлением в этом слое, будут нуждаться в усилении, чтобы заняться добавлением устройств IoT в систему управления. С учетом IoT мы предпочитаем называть этот слой «слоем пользователя и взаимодействия», поскольку есть намерение охватить те виды деятельности, которые включают «традиционную» веб-паутину, датчики и устройства. Мы ожидаем, что многие правительства решат, что добавление приемных и исполнительных устройств к сети может потребовать усложненного анализа, когда дело идет о безопасности пользователя.

Поскольку вопросы обеспечения безопасности потребителя становятся более важными, мы можем наблюдать более активное участие множества агентств по защите потребителя в центре управления Интернетом. Здесь в отношении IoT не возникает никаких новых проблем с безопасностью. Очевидно, что потребители будут продолжать делать глупости, подобные сушке волос, сидя в ванне. На некотором уровне даже этот вид проблем будет менее важен при более «разумных» устройствах (например, устройство сушки с датчиками, которые выключают устройство, когда становится слишком влажно), но всегда будет иметься возможность обсудить, где находятся «демаркационные линии» в деле «совместной ответственности» производителей для изготовления устройств, которые ожидают ошибок со стороны пользователя, и самих пользователей, которые должны пользоваться устройствами ответственным образом.

3.2 Механизмы полицентрического управления

Недавно на логический слой было обращено большое внимание из-за исследования механизмов полицентрического управления, которые установил нобелевский лауреат Элинор Остром [14]. Один из многих вкладов, которые сделал Остром в своей работе, – это указание на то, что сложность в полицентрических системах управления – не то же самое, что хаос. Полицентрическое управление характеризуется организационной структурой, когда многочисленные независимые действующие лица совместно определяют свои взаимоотношения с другими лицами на основе общей системы правил. Нет единственного участника, управляющего будущим Интернета, вместо этого все участники должны действовать в рамках своей компетенции («полицентрическим» путем) и отвечают за свою зону ответственности. Эти участники энергично продолжают действовать в духе взаимозависимого сотрудничества и управления таким же образом, как и действовал сам форум IETF при разработке большинства стандартов для Интернета.

3.2.1 «Базар» в Управлении Интернетом

Один из наилучших примеров того, как может быть разработана технология в условиях управления со слабыми связями, предоставил компьютерный программист Эрик Реймонд. В его работе «Кафедральный собор и базар» [16] отмечаются различные подходы к компьютерной технике: «кафедральный собор», который представляет собой иерархию «сверху-вниз», и «базар», представляющий собой плоский, более демократический (хотя и хаотический) процесс в разработке программ. Это полезный способ анализа философии развития Интернета по сравнению с другими телекоммуникационными технологиями (например, Bell Labs). По сути дела, метод «базара» для написания программ не похож на то, как работает Википедия: система открыта и подвержена воздействию в соответствии с замечаниями любого, кто имеет определенное мнение. Центральным является следующий тезис Реймонта: «при достаточном количестве глаз все ошибки становятся неглубокими», что, по сути, означает, что широкое распространение и обсуждение программных продуктов обеспечивает их улучшение.

Эквивалентом базара в организациях разработки стандартов является группа IETF – открытая структура, основанная на добровольных началах в деле создания стандартов без какой-либо формальной корпоративной «индивидуальности», где инженеры работают над центральной функциональностью, которая обеспечивает передачу пакеты информации по Интернет. Все проекты IETF свободно доступны, и все процессы IETF полностью публикуются в Интернете. Возможно даже, что чтение веб-сайта IETF может быть несколько затруднительным, но только из-за того, что публикуется слишком много информации. Публикации имеются в любом формате и ожидается, что любой может принять участие в процессе IETF. Как указывает Харалд Алвестранд, работа группы IETF основана на полностью открытом процессе, который означает, что любое заинтересованное лицо может принять участие в работе, зная, что решается, и подать свой голос по рассматриваемой проблеме. Часть этого принципа – обязательство составлять документы, списки адресатов нашей рабочей группы, список присутствующих и протоколы заседаний, открыто выложенные в Интернет [1].

Составленная по аналогии с пространством открытых стандартов, группа IETF – истинная система, при которой положение участников определятся их способностями. Если член сообщества IETF решит, что инженерные идеи имеют ценность, эти идеи принимаются и включаются в комплект стандартов по Интернету. С другой стороны, те идеи, которые устарели или контрпродуктивны, отклоняются. Как заявил Дэвид Кларк из Массачусетского технологического института, «мы отвергаем королей, президентов и голосование; мы верим в грубый консенсус и выполнение кода» [11]. В отличие от этого, многие государственноцентричные системы, построенные по принципу «сверху вниз», полагаются на назначении государствами и официальными комитетами, как это происходило в мире при разработке стандартов по модели PTT.

3.2.2 Безопасность как совместная ответственность

Важно, что не только в Интернете используется разделяемая ответственность. Еще один пример – способ организации самих людей в деле охраны домов и окрестностей. Здесь государство играет свою роль через создание правовых преград для преступлений и их реализацию через деятельность полиции, а также установление стандартов и

правил безопасности. Частный сектор также принимает участие – через частную охрану, системы тревожной сигнализации, защитные ограждения и т.д. Гражданское общество играет свою собственную роль через механизмы программ соседского наблюдения и коллективных действий отдельных соседей. Кроме того, поднят вопрос образования и выбора пользователя – например, некоторые выбирают вариант запирания дверей, другие – нет; некоторые выбирают вариант использования засовов, другие – нет.

3.3 Отображение IoT на текущую систему управления

В последнем разделе рассмотрим средства управления, которые мы хотим разработать, особенно те, которые касаются безопасности IoT. Перед тем, как обсудить особенности хорошей системы управления, позвольте уточнить то, что мы рассматриваем как цель в отношении будущих технологий и, в частности, IoT. Мы придерживаемся пользовательско-центристской концепции в технологии, которая означает, что Интернет Вещей должен содействовать развитию человека и повышать благосостояние пользователей. Вся технология – это средство поддержки научных достижений и инноваций не только ради их самих, но и для оказания поддержки в интересах людей Информационному Обществу и более богатому, более справедливому управлению и экономическим условиям. Лоуренс Лессинг провел исследования по этой теме, различая технологии доступа (к знаниям и услугам) и технологии управления (дающие возможность институтам лучше контролировать пользователей и управлять ими) [13].

Если технология управляется пользователем, то какого рода опыт пользователи получат, когда IoT станет господствующей тенденцией? На абстрактном уровне большинство выгод от IoT создается через применение систем. Например, в «умном» городе объединенные в сеть датчики и сигналы регулирования движения ведут к более эффективному дорожному движению, в «умных» домах температурные датчики и интеллектуальные распределенные системы отопления и охлаждения приводят к экономии энергии, а подобные сети сельскохозяйственных датчиков обеспечивают более точную ирригацию и внесение удобрений, приводящие к более высоким урожаям и более устойчивому развитию.

При анализе ориентированного на потребителя сектора IoT мы можем обнаружить существенно разные и быстро развивающиеся группы ответственности, поскольку эта область будет включать знания о все более «умных» бытовых изделиях. Как отмечено ранее, эти роли могут все в большей степени выполняться агентствами по защите потребителя и за счет усилий гражданского общества, сфокусированных на пользователе. Хотя ответственность за безопасность в более развитой инфраструктуре не всегда легко определять, имеется, по крайней мере, относительно четкое право

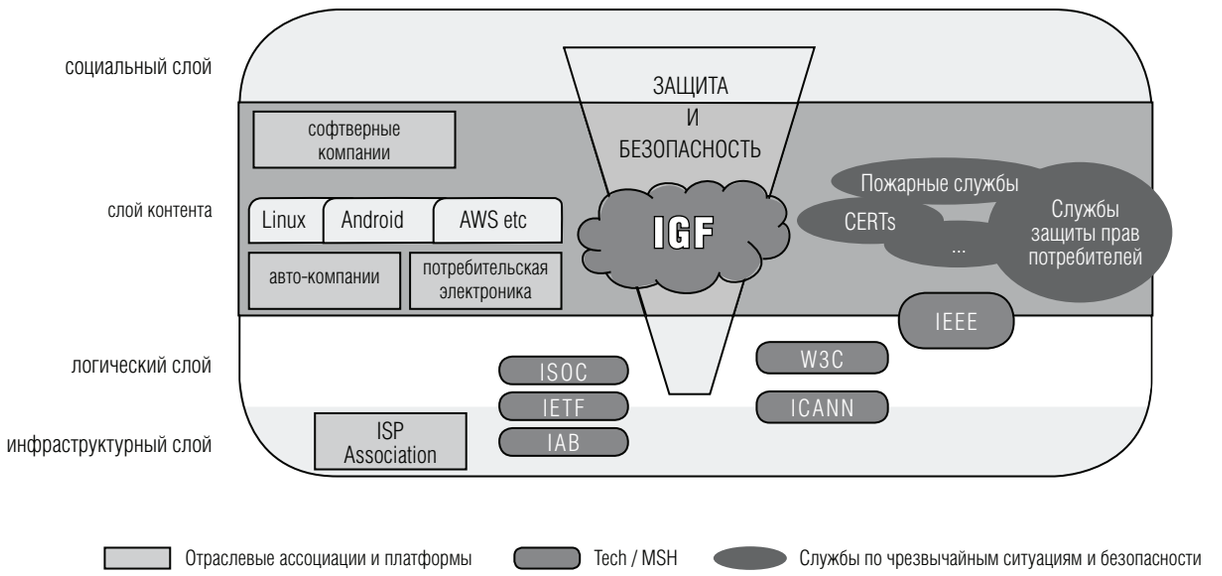

Рис. 2. Экосистема управления безопасностью IoT

собственности и, следовательно, контроль рассматриваемой системы (например, дороги, завода и т.п.). Однако в пространстве пользователей множество соединенных устройств и их взаимодействие может создать для безопасности новые угрозы. Кроме того, конечные применения все больше включаются в наращивание сети и доскональное изучение размещения продукта. Кроме того, просьюмеры – потребители, которые производят и потребляют средства и которые сдают на прокат свои устройства – будут продолжать увеличиваться, и, таким образом, эта тенденция усложнит задачу передачи информации об изъянах в безопасности изделий.

На *рисунке 2* мы отобразили мир управления IoT в той модели, которая была представлена ранее. Группы заинтересованных лиц, таких как автомобильные компании, агентства по защите потребителя и общественной безопасности, будут все больше проявлять себя в сфере управления. Эти и другие группы будут играть все возрастающую роль (1) в разработке и определении стандартов безопасности; (2) в обеспечении того, что продукты и услуги безопасны для применения; и (3) в разборе опасностей, после того как они возникнут.

Подход, описанный выше, представляет дополнительные группы внутри каждого из слоев, чтобы показать, в каком слое те агентства, которые занимаются проблемами IoT, могли бы связываться с коллегами. Как и в других аспектах управления Интернетом, эта конструкция ведет к динамичной, вплетенной и гипертекстовой сети информационных связей между заинтересованными сторонами, которые согласны совместно развивать и реализовывать решения. Этот неформальный и децентрализованный метод, по нашей оценке, является более эффективным и адекватным, чем другие (более традиционные) подходы, подобные попытке развивать и санкционировать гипотетическую «Угрозу кибербезопасности» или гипотетическую «Угрозу безопасности Интернету Вещей». Среди многих причин, этот подход обеспечивает более быстрые обновления, больше экспериментов с новыми решениями и более высокую гибкость при рассмотрении уникальных культурных, контекстных и политических условий. Эти виды предложений по угрозам не являются нелепыми. Мы наблюдали на Всемирной конференции по международной электросвязи (WCIT-12) борьбу 193 стран в отношении того, как реализовывать (или не реализовывать) меры защиты Интернета с помощью договоров. Попытки, подобные наблюдавшимся на этой конференции, и другие подобные события наверняка будут продолжаться [4].

Имеется несколько заинтересованных институтов, которые достойны упоминания благодаря той роли, которую, как мы ожидаем, они играют в безопасности IoT. К ним относятся Группа компьютерной скорой помощи (CERT) и Группа реагирования на инциденты с компьютерной защитой (CSIRT). Первые группы CERT начали действовать почти 30 лет назад, и сегодня по всему миру имеется сеть групп, а одним из основных видов их деятельности является разборка инцидентов с защитой/безопасностью Интернета. Группы CERT занимаются технологической деятельностью в кибермире, и эта деятельность сравнима с работой групп по борьбе с пожарами или природными катастрофами в физическом мире. Обязанности как групп CERT, так и других групп, занимающихся общественной безопасностью, могут быть расширены с включением в них аварий IoT, поэтому их база финансирования должна включать в себя всех традиционных игроков частного сектора, которые обеспечивают соединяемость в своих изделиях.

Заключение

Наступление эпохи Интернета Вещей дает огромные возможности в изучении весьма реальных проблем в сфере защиты правовых интересов пользователей. Улучшившееся понимание различий между сетью, операционными системами вещей, прикладным программным обеспечением и их применением (особенно когда речь идет о защите и безопасности пользователей) позволит создать набор солидных практических методов для многообразных заинтересованных сторон как в виртуальном, так и в физическом мире.

Конечно, остаются без ответа многие вопросы. Какие виды ответственности широкая публика унаследует благодаря использованию Интернет-устройств для защиты других от опасного поведения и злоупотреблений (например, в некоторых юрисдикциях по закону вокруг плавательного бассейна требуется ограда)? Будет ли концепция небрежности и причинной обусловленности изменяться в условиях Интернета Вещей? Каковы последствия отказа от своевременного обновления критичного для безопасности программного обеспечения? Эти и другие вопросы, определенно, возникнут, поскольку популяция Интернет-устройств увеличивается, становясь неотъемлемой частью нашей повседневной жизни. ■

Литература

1. Alvestrand H. A mission statement for the IETF // IETF, Request for Comments 3935. 2004. [Электронный ресурс]: https://www.ietf.org/rfc/rfc3935.txt (дата обращения 01.02.2016).
2. Andrade P.L., Hemerly J., Recalde G., Ryan P. From Big Data to big social and economic opportunities: Which policies will lead to leveraging data-driven innovation's potential? The Global Information Technology Report 2014: Rewards and Risks of Big Data // INSEAD, Cornell University, the World Economic Forum. 2014. P. 81–86.
3. Cerf V.G., Ryan P.S., Senges M. Internet Governance is our shared responsibility // I/S: A Journal of Law and Policy for the Information Society, 10 ISJLP 1 (2014). 2014. [Электронный ресурс]: http://ssrn.com/abstract=2309772 (дата обращения 01.02.2016).
4. Cerf V.G., Ryan P.S., Senges M., Whitt R.S. A perspective from the private sector: Ensuring that forum follows function // Beyond Netmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem / W.J. Drake, M. Price, eds. Center for Global Communication Studies, Annenberg School for Communication at the University of Pennsylvania. 2014. [Электронный ресурс]: http://ssrn.com/abstract=2489348 (дата обращения 01.02.2016).
5. Chesbrough H., Van Alstyne M. Permissionless innovation // Communications of the ACM. 2015. Vol. 58. No. 8. P. 24–26.
6. Tomorrow starts here // Cisco press release. 10 December 2012. [Электронный ресурс]: http://goo.gl/vlKOfJ (дата обращения 01.02.2016).
7. Conficker Working Group: Lessons Learned. June 2010 (Published January 2011). [Электронный ресурс]: http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf (дата обращения 01.02.2016).
8. Faddell T. Nest CEO Tony Fadell on the future of the Internet // Wall Street Journal, 26 April 2015. [Электронный ресурс]: http://www.wsj.com/articles/nest-ceo-tony-fadell-on-the-future-of-the-internet-1430104501 (дата обращения 01.02.2016).
9. Gayer O., Wilder O., Zeifman I. CCTV botnet in our own back yard // The Incapsula Blog, 21 October 2015. [Электронный ресурс]: https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html (дата обращения 01.02.2016).
10. Gross N. The earth will don an electronic skin // Bloomberg Business Week, 30 August 1999.
11. Hoffman P. The Tao of IETF: A novice's guide to the Internet engineering task force. 2012. [Электронный ресурс]: http://www.ietf.org/tao (дата обращения 01.02.2016).
12. Kirkpatrick D. Why an Internet of everything event? 'It's the world waking up' // Techonomy, 3 May 2013.
13. Lessig L. The future of ideas: The fate of the commons in a connected world. Vintage Books, 2002. 384 p.
14. Ostrom E. Beyond markets and states: Polycentric governance of complex economic systems. Nobel Prize Lecture, 8 December 2009. [Электронный ресурс]: http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/ostrom_lecture.pdf (дата обращения 01.02.2016).
15. Pettersson E. Sony to pay as much as $8 million to settle data-breach case // Bloomberg Business, 20 October 2015.
16. Raymond E.S. The cathedral and the bazaar. V. 3.0. 2000. [Электронный ресурс]: http://www.catb.org/esr/writings/homesteading/cathedral-bazaar/ (дата обращения 01.02.2016).
17. Ryan P., Falvey S. Trust in the clouds // Computer Law & Security Review. 2012. Vol. 28. No. 5. P. 513–521.
18. Schindler H.R., Cave J. Towards a dynamic and trustworthy Internet of things // Rand Europe Research Brief, 88-9742-EC. 2013.
19. Westby J. Instead of a real response, perennially hacked Sony is acting like a spoiled teenager // Forbes, 17 December 2014. [Электронный ресурс]: http://www.forbes.com/sites/jodywestby/2014/12/17/sony-earns-cyber-troglodyte-award/#2fc4f7f96942 (дата обращения 01.02.2016).
20. Whitt R.S. A deference to protocol: Fashioning a three-dimensional public policy framework for the Internet age // Cardozo Arts & Entertainment Law Journal. 2013. No. 689. P. 754–756.