Дэн Йорк: «В ближайшей перспективе вопросы безопасности не смогут замедлить развитие интернета вещей»

Дэн Йорк,

Старший контент-стратег в *Обществе интернета (ISOC)*, председатель *Альянса по безопасности VoIP (VOIPSA).*

Стремительное развитие интернета вещей меняет привычный нам мир и повседневную жизнь, одновременно стирая грань между онлайн и оффлайн деятельностью. Вместе с удобствами приходят и неудобные вопросы о безопасности все большего количества подключенных к интернету устройств, данных, генерируемых с их помощью, сети передачи этих данных и т.п. В октябре 2015 года «Общество интернета» (ISOC) опубликовало доклад The Internet of Things (IoT): An Overview, в котором в числе освещен ряд угроз и вызовов, связанных с повсеместным развитием и внедрением технологий интернета вещей. Мы поговорили с Дэном Йорком, старшим контент-стратегом ISOC о том, чем грозит интернет вещей, какие вопросы он ставит перед обществом в целом и отдельным пользователем, государством, бизнесом и техническим сообществом.

— Какое место в Вашей компетенции и сфере интересов занимает «Интернет вещей»?

— Я работаю в ISOC уже четыре года. Сначала я занимался вопросом внедрения ключевых решений для более безопасного и доступного интернета, сюда относятся модули безопасности службы доменных имен (DNSSEC), протоколы

безопасной маршрутизации, IPv6 и т. д. То есть я занимаюсь вопросами безопасности и коммуникациями в этой области.

Тема интернета вещей всегда меня интересовала. С увеличением числа подключенных к интернету устройств — гаджетов, смартфонов, носимых устройств, таких как *Apple Watch*, и т.п. — безопасность сетей все больше становится поводом для беспокойства. Со временем ноутбуки, смартфоны и другие устройства стали более защищенными. Но сегодня к интернету подключены и холодильники, и видео-няни, и любые другие вещи. Только посмотрите, как их много! Моей дочери 6 лет, и я помню, когда видео-няня была, условно говоря, рацией. Сейчас они подключены к интернету, имеют поддержку IP-протокола, ведь потребитель хочет, отправившись на работу, смотреть за своим ребенком. Во-первых, это устройство подключено к интернету, оно отправляет ваши данные, видеопоток, на сервер, к которому вы имеете доступ через телефон. Данные проходят через несколько узлов, и это поднимает вопрос о безопасности на транспортном уровне. Зашифрованы ли данные на пути между домом и сервером, между сервером и смартфоном? Во-вторых, есть проблема безопасности самого устройства. Может ли недоброжелатель попасть в вашу сеть, подключиться к устройству и через него заглянуть в ваш дом изнутри? Недавно появились сообщения о холодильниках, которые использовались в ботнет-схемах: злоумышленник нашел способ подключиться к интерфейсу «умного» холодильника, установил там вредоносную программу, чтобы впоследствии использовать его в качестве «компьютера-зомби» в DDoS-атаках.

— Кажется, это Винт Серф сказал: «Мой самый страшный кошмар — это тысячи холодильников, которые взламывают Bank of America».

— Точно. Знаете, одна из трудностей заключается в обновлении ПО. Например, помните, недавно в США провели эксперимент, в ходе которого журналист сделал так, чтобы хакеры на камеру взломали *Jeep Cherokee*, за рулем которого он сидел? В машине была подключенная к интернету мультимедийная система. Возвращаясь к теме безопасности в интернете вещей, эта мультимедийная система не была изолирована от остальных систем в автомобиле. Хакеры смогли проникнуть внутрь машины через беспроводную сеть, к которой была подключена мультимедийная система, взломали ее и получили контроль над автомобилем. При этом в подключенной к интернету машине, очевидно, не было средств контроля безопасности, а система управления не была отделена.

Другая проблема заключается в обновлении этих устройств. Когда нужно обновить ПО в *Jeep Cherokee*, вам придется либо отвезти машину к дилеру, или самостоятельно загрузить обновление на флешку и установить его на автомобиль. Сколькие люди захотят заниматься этим самостоятельно? Есть небольшие вещи, такие как термостат *Nest* или подключенные к интернету лампочки, которые можно включать удаленно. Но будут ли люди заниматься обновлением системы безопасности на таких устройствах?

Есть и другая крайность — *Tesla* недавно выпустила обновление для автомобилей, которое устанавливает на них автопилот. Один мой знакомый на прошлой неделе написал в соцсети, что как раз загружает это обновление для

своей машины. После этого он отправился в 2,5-часовую поездку, и все это время машина ехала сама, за исключением пары минут, когда на одном сложном участке на автостраде в Флориде ему пришлось вести самому. Все остальное время он только говорил автомобилю, куда ехать, и тот ехал в соответствии с проложенным по GPS-навигатору маршрутом. Но это обновление проходило через Wi-Fi. Если сравнить с машинами *Chrysler*, которые обновляются через USB-устройства, *Tesla* оказывается еще более интернет-интегрированной и подвержена еще большему количеству угроз безопасности.

Все это возвращает нас к вопросу доверия. Использование таких технологий возможно, только если мы доверяем безопасности интернета. Меня беспокоит сама идея беспилотного автомобиля, когда я думаю, сколько существует способов взломать его. Но в то же время, я хорошо представляю себе пользу от таких машин. Однажды я вернулся в Коннектикут ночью и слишком устал, чтобы вести машину. Поэтому мне пришлось остановиться в отеле, который был в 1,5 часах езды от моего дома, чтобы немного поспать. В мире, где есть беспилотные машины, я мог бы просто сказать: «Отвези меня домой», и при условии доверия системе я скорее бы оказался дома, со своей семьей.

— По вашему мнению, проблемы безопасности могут замедлить развитие интернета вещей в мировом масштабе?

— В ближайшей перспективе, я думаю, вопросы безопасности не смогут замедлить этот процесс, потому что человечеству хочется «запрограммированных» удобств. С точки зрения рынка, производители сейчас заинтересованы в том, чтобы занять максимально большой сектор рынка. Я думаю, в какой-то момент произойдут крупные инциденты, связанные с информационной безопасностью, которые заставят людей задуматься и приведут к вмешательству правительств. Раз сейчас производители не обращают особого внимания на вопросы безопасности, могут быть вовлечены другие игроки, которые повлияют на рынок. Регулирование на разных уровнях может привести к затратам, которые заглушат инновации. Из-за этого мы считаем, что производителям следует больше внимания уделять вопросам безопасности уже сейчас.

— Кроме того, безопасность сама по себе — это бизнес.

— Это так. Если компания не обращает внимания на безопасность, в какой-то момент в защите найдутся серьезные бреши, а это повлияет на доверие к продукту и к компании. На конференции DEFCON в Лас-Вегасе в этом году было представлено много технологий, имеющих отношение к интернету вещей. Это серьезное поле деятельности для людей, занимающихся информационной безопасностью, будь они «белыми» или «черными» хакерами. Они занимаются этим потому, что очень много незащищенных устройств выходит на рынок. Отчасти для такой аудитории был проведен эксперимент с *Jeep Cherokee* в этом году. Но был также и эксперимент с удаленным взломом снайперской винтовки, когда могло быть немного скорректировано направление наведения прицела. Так что думать, что безопасность таких устройств не будет проверена на прочность, достаточно наивно, потому что это неизбежно. Вышел еще один доклад о

проблемах безопасности видео-нянь, результаты были направлены в соответствующие компании. Это было исследование, проведенное «белыми» хакерами, но на их месте могли бы оказаться менее этичные люди.

— В том, что касается интернета вещей, решения по обеспечению информационной защиты больше сконцентрированы на бытовых устройствах, или уже есть те, что относятся к бизнесу, индустриальным объектам, например, к критической инфраструктуре?

— Действительно, интернет вещей существует на разных уровнях, и вызовы на этих уровнях отличаются — и в смысле безопасности, и в смысле защиты персональных данных. Интересно посмотреть на архитектурные модели используемых дома, на работе и где бы то ни было устройств, которые связываются с центральным хабом, который в свою очередь перенаправляет сигнал обратно на серверы. Есть несколько разных видов архитектурных решений, при использовании которых возникают разные вопросы к безопасности и защите конфиденциальности. В целом, через эти серверы можно узнать о внутренней инфраструктуре компании. При развертывании этих систем, необходимо принимать решения и по вопросам безопасности, и эти варианты не всегда продумываются. Когда мы стремимся получить все преимущества новых технологий, нужно удостовериться, что они должным образом защищены, а для этого должен быть определенный уровень доверия.

— Справедливо ли говорить, что сейчас усилия направлены на создание единообразия в смысле стандартизации или поиска решений, которые работали бы не только в определенной узкой нише, но в целом кластере?

— Как мне кажется, сейчас можно наблюдать большое количество разрабатываемого проприетарного программного обеспечения, того, что называют «закрытые экосистемы». Это происходит из-за того, что фирме-поставщику проще самостоятельно определить направление развития и иметь в своем арсенале набор решений. Сейчас начинают формироваться разные альянсы и консорциумы, представляющие разных поставщиков и объекты из их закрытых экосистем. Проблема в том, что, когда предлагается инновационное решение, как правило, проприетарное, в какой-то момент его назовут «деловым интересом» и представят новый стандарт, очерчивающий проблему совместимости. На мой взгляд, сейчас нам нужно посмотреть, куда движется рынок, когда на рынок поступает огромное количество продуктов, борющихся за покупателя. В какой-то момент компании и потребители могут высказаться против привязанности к единственному поставщику или консорциуму из-за локализованного стандарта единообразия. Сейчас развиваются разные стандарты на разных уровнях и платформах. В рамках Инженерного совета Интернета (IETF), например, несколько групп работают над стандартами для интернета вещей на транспортном уровне. В Международном союзе электросвязи (ITU) разрабатывают стандарты, связанные с радиопередачей.

— Но насколько глобальными могут быть стандартизация и регулирование, когда разные страны, очевидно, захотят иметь собственное

законодательство на этот счет со своей собственной сертификацией. Могут ли в итоге появиться некие региональные кластеры?

— Да, я думаю, здесь может сказаться вопрос разрозненности стандартов. Это в целом проблема для интернета в глобальном смысле, давление идет из разных регионов и стран, где стремятся ввести собственные меры контроля и связанные с интернетом стандарты. Это, кстати, не так очевидно, как в случае с ICANN, где все так или иначе возвращается к DNS и основано на открытых интернет-стандартах, то есть, стандартах IETF. В интернете вещей приходится иметь дело со встроенными операционными системами, с радио, а стандарт IEEE имеет отношение к некоторым физическим интерфейсам. Далее, есть стандарты IETF в сетях с протоколами IP, IPv6. Так что здесь существует целый ряд стандартов, из-за чего регулирование становится довольно мудреным.

— А не было ли сколько-нибудь значимой попытки объединить это все?

— Нет, но были группы-посредники между разными организациями по стандартам по разным тематикам. Я лично в этом не участвовал. Помечу себе, это могло бы стать отличной темой для обсуждения.

— Что касается протокола IPv6, насколько задержки в его распространении могло бы замедлить или уже замедляет развитие интернета вещей?

— Это, без сомнения, проблема, которая может замедлить развитие протокола. В Европе блоки IPv4 уже распределены, как и в Северной Америке и в Азиатско-тихоокеанском регионе. Это пересохший источник реки. Сейчас мы обсуждаем емкость реки, в то время как вода из нее медленно уходит. Порой это ставит меня в тупик во время бесед с представителями компаний-производителей. Когда я говорю об IPv6, они отвечают что-то вроде: «Нам неохота об этом думать». Я спрашиваю: «Вы понимаете, что вы пытаетесь развернуть миллиарды новых устройств, для которых у вас нет диапазона адресов?». К счастью есть и те, кто понимают важность вопроса.

— Давайте перейдем к другой стороне вопросов безопасности. Когда речь идет об устройствах и проблеме конфиденциальности, компании предлагают изменить пользовательские настройки приватности. Но какое реальное значение ни имеют?

— Разного рода озабоченность возникает вокруг конфиденциальности в интернете вещей в связи с растущим объемом передаваемых данных. Один из вызовов в данном случае связан с тем, что, загружая, например, приложение для смартфона, вы видите условия использования и соглашаетесь с ними. Возьмем теперь «умный» холодильник или лампочку. Где у них пользовательским интерфейс, чтобы поставить галочку? Его просто нет. Так что варианта с моделью, в которой есть условия использования, с которыми можно было бы согласиться, не существует. Это неприменимо к средам со встроенными сетевыми системами и отсутствующими пользовательскими интерфейсами. Не знаю, есть ли простой ответ на этот вопрос.

— Кроме того, все сложнее и сложнее отказаться от какого-то сервиса не только технически, но и из-за того, что все мы живем не в пустом пространстве, а в социуме, в обществе мы связаны различными отношениями. Мне представляется ситуация, где отказаться нельзя потому, что нельзя уйти из некоторой окружающей среды, в которой ты живешь, если только ты не живешь в лесу.

— Это так. И это возвращает нас к вопросу о том, какой частью приватности мы готовы пожертвовать, чтобы получить удобство определенного сервиса. Если я хочу иметь удаленный доступ к своему дому или офису, мне стоит признать, что все эти сервисы строят свои бизнес-модели на монетизации данных, циркулирующих между домом и офисом, центральным хабом и устройством.

— Кроме того, недавние решения в рамках соглашения Safe Harbor между Европой и США могут вывести эти споры на новый уровень, например, о передаче данных. У вас есть представление, куда все это может привести?

— В самом деле, это интересное решение Европейского суда. До «Общества интернета» я работал в компании-поставщике «облачных» решений. Мы столкнулись ровно с этой проблемой — европейские потребители не хотели, чтобы их персональные данные хранились на серверах, находящихся в США, где действует Закон о борьбе с терроризмом в США (Patriot Act). Создается интересная ситуация. Мы много обсуждаем не требующие разрешений инновации, когда не нужно запрашивать разрешение у кого-либо, чтобы запустить собственный сервис. Где бы ни был запущен такой сервис, доступ к нему возможен из любой точки в мире. Теперь, если в рамках своего инновационного сервиса вам приходится хранить данные пользователей, вам придется удостовериться, что данные европейских пользователей хранятся на европейских серверах, данные российских пользователей — на российских серверах, и мы снова возвращаемся к проблеме фрагментации.

— В России был принят закон, по которому персональные данные россиян должны храниться на территории Российской Федерации, он вступил в силу 1 сентября 2015 г.

— Это вопрос того, какую поддержку находят инновации, движимые ростом интернет-экономики. Похоже, что теперь я не смогу предложить в России свой сервис, если только не придумаю, как быть с персональными данными российских пользователей моего продукта, который я написал с парой друзей в своей спальне, потому что у нас появилась потрясающая идея, которая может стать новым фейсбуком. Теперь, чтобы запустить этот продукт в России, я должен иметь возможность разместить данные на российском сервере. Все это не вписывается в концепцию интернета вещей. Если я захочу продавать в России «умные» лампочки, все данные, поступающие от российских пользователей, мне нужно будет каким-то образом хранить в российском дата-центра, который каким-то образом должен будет быть соединенным с моим дата-центром, который может находиться в Европе, в Северной Америке или где угодно.

Это серьезный вызов для бизнеса. Для компании, в которой я раньше работал, большой проблемой стала необходимость устанавливать отдельные центры обработки и передачи данных и оставлять соответствующие зазоры между кодом и всем остальным. Только для того, чтобы быть уверенным в том, что данные европейских пользователей находятся на европейских серверах. Это повлекло за собой дополнительные расходы, разработку дополнительного ПО и т.п.

— Сейчас многие компании в своих отчетах о прозрачности (transparency reports) раскрывают информацию о поступающих к ним запросах от правоохранительных органов относительно пользовательских данных, которые эти компании получают. Появлению этого тренда во многом помогли разоблачения Сноудена, после которых многие компании решили выпускать такой отчет, чтобы сохранить доверие пользователей. С учетом развития интернета вещей, насколько жизнеспособен этот тренд отчетности?

— Это действительно стало бы испытанием для компаний. Например, предположим, что в ходе расследования правоохранительным органам понадобится информация о том, были ли вы дома в какой-то день. Вы утверждаете, что были, а они могут затребовать в качестве свидетельства данные с вашего холодильника, показывающие, сколько раз он открывался в тот вечер. И внезапно может оказаться, что, хотя вы утверждаете, что вы сидели дома, ужинали и пили пиво, холодильник показывает, что ни разу дверца не была открыта за весь вечер. А датчики света показывают, что в доме не горел свет. Тогда ваше алиби не работает! С другой стороны, насколько можно доверять этим записям данных? Можем ли мы быть уверены, что они не были скомпрометированы кем-либо или изменены? Может, кто-то проник в вашу систему и скорректировал данные так, что холодильник показывает, что вас дома не было, хотя на самом деле вы там были? Это вопросы к безопасности тех больших систем из вещей, с которыми приходится работать. Можно ли быть уверенным, что правоохранительные органы получат приемлемый доступ, если само понятие «приемлемый» отличается в разных культурах? Европейское понятие «приемлемого доступа» для правоохранительных органов отличается от американского, которое, в свою очередь, отличается от русского. Очевидно, что в некоторых странах проблема конфиденциальности данных имеет гораздо более длительную историю, а в других такие ожидания не обязательно существуют. Это вопрос того, как мы можем обеспечить необходимый уровень безопасности и сделать это так, чтобы не заблокировать все возможности для развития и повышения удобства.

— Каково ваше мнение по поводу споров о шифровании в системах связи? Будет ли это работать с распространением интернета вещей? Все еще ведутся споры о том, должно ли шифрование в системах связи быть по умолчанию сквозным, и, как вы знаете, правительства некоторых стран приводят аргументы в пользу предоставления им доступа к бэкдорам для осуществления эффективной правоохранительной деятельности. В то же время, технические специалисты утверждают, что или бэкдоры будут для всех, или их не будет ни для кого, здесь не может быть никаких преференций.

— В «Обществе Интернета» мы имеем четкую позицию на этот счет — это одна из тех особо принципиальных позиций, которые мы заняли в поддержку заявления Совета по архитектуре Интернета. Все интернет-протоколы должны шифроваться по умолчанию. Мы изначально продвигали эту позицию из-за крупномасштабной электронной слежки со стороны государств заявив, что коммуникации, подразумевающие конфиденциальность, особенно нуждаются в шифровании. Конечно, среди нас есть такие, кто считает, что шифрование должно обязательно быть сквозным, есть те, кто больше внимания обращает на обеспечение невмешательства государственных акторов в транспортировку данных по сети. Это возвращает нас к вопросу о балансе законных требований правоохранительных органов на получение приемлемого доступа к информации. Понимаете, если мой ребенок попадет в беду, я захочу, чтобы правоохранительные органы использовали все возможности, чтобы найти злоумышленника. Снова этот вопрос об общественном балансе интересов. С точки зрения шифрования, мы хотим, чтобы продукты использовали зашифрованные протоколы. Это должно стать правилом разработки таких устройств, и правоохранительные органы должны пересмотреть свои методы работы в связи с этим. Мы слишком долго жили под постоянным наблюдением, теперь нужно понять, как защитить себя. Это касается не только отдельных лиц, но и корпораций и государств, которые всегда стремились добыть чужие данные разными способами.

— Сейчас на различных уровнях предпринимаются усилия по разработке правил поведения государств в киберпространстве — например, в Группе правительственных экспертов ООН, в ОБСЕ, в ШОС, даже *Microsoft* как представитель корпоративного сектора пытается разработать подобные принципы.

— Мы развиваем еще и такую модель, которую мы называем «коллаборативная безопасность» (collaborative security). Ее смысл в том, что ни одно государство самостоятельно не сможет решить подобные проблемы безопасности. В этой сфере нужно работать сообща. Некоторые правительства, включая российское, призывают к принятию международного договора, который обеспечивал бы глобальную безопасность, но под силу ли одним только правительствам привести его в жизнь? А ведь к тому времени, когда такой договор может быть принят, он уже будет устаревшим из-за технологической революции. Некоторые из этих вопросов мы прорабатывали с поставщиками маршрутизаторов в проекте Взаимного соглашения по правилам обеспечения безопасности маршрутизации (MANRS). Это необязывающее, добровольное соглашение между компаниями, которые договариваются о «надлежащей гигиене данных». Это модель «коллаборативная безопасность», ответственное поведение, как мы это называем.

В целом, как мне кажется, на вопросах безопасности и конфиденциальности не стоит замыкаться. Если обратиться к выгоде потребителя, выгоде бизнеса, экономической выгоде, то вырисовывается совсем другая картина. Я раньше скептически относился к концепту беспилотного автомобиля, но один друг сказал мне: «Я не очень хорошо вожу по ночам, у меня плохое зрение. Мне бы хотелось иметь беспилотный автомобиль, чтобы ночью я мог отправляться в более

длительные поездки». И тут я стал думать, что интернет вещей вполне способен изменить жизнь людей к лучшему. Я думаю, перед нами как обществом стоит вопрос о приемлемом уровне доверия к интернету вещей и также «интернету всего», чтобы воспользоваться теми возможностями, которые они дают.