Опасный IoT

Татьяна Золотова

Вопрос безопасности набирающих популярность интеллектуальных платформ, управляющих «умными вещами», заставляет бизнес-сообщество призвать государство к регулированию этого сегмента: ввести сертификацию, выработать критерии и стандарты безопасности для абонентского оборудования, подключаемого к Сети.

В марте 2018 года на круглом столе «Как обезопасить подключенные абонентские устройства», организованном издательством «Телеспутник», представители производителей оборудования и эксперты по информационной безопасности (ИБ) обсудили проблемы цифровой экономики и перехода на умное оборудование. Вопрос безопасности IoT-решений оказался непраздным не только для участников круглого стола, но и для всех игроков рынка.

Имя им легион

По данным исследования аудиторского агентства KPMG, к 2020 году во всем мире более 50 млрд устройств будут подключены к Интернету. Эксперты IoT Analytics подсчитали, что в 2017 году насчитывалось 450 IoT-платформ — на 25% больше, чем в 2016 году. Специалисты консалтинговой фирмы Berg Insight вычислили, что на 300 проектов с применением мобильных технологий (рассматривались масштабные проекты с 2004 по 2016 год в разных регионах мира, — *прим. «Теле-Спутника»*) приходилось более 156 млн активных абонентов IoT-сервисов. По итогам 2018 года расходы на технологии Интернета вещей составят $772,5 млрд (рост на 14% по сравнению с 2017 годом), в 2020 году — $1 трлн, сообщается в исследовании IDC. Оборудование станет самой большой статьей расходов в этом году: $239 млрд будут направлены в основном на приобретение модулей и датчиков, строительство инфраструктуры и обеспечение безопасности. К примеру, в апреле 2018 года Microsoft объявила, что вложит $5 млрд в инициативы на рынке Интернета вещей в течение ближайших четырех лет.

Ежегодная конференция «Лаборатории Касперского» наглядно показала серьезность наличия уязвимостей в безопасности большинства подключаемых к Интернету девайсов. Согласно данным, озвученным на мартовском саммите Security Analyst («Саммит экспертов по информационной безопасности», SAS 2018) в Канкуне аналитиком «Лаборатории Касперского» Денисом Макрушиным, опасности подвержены более чем 8,4 млрд IoT-устройств, которые уже функционируют на рынке. Речь шла как о газовых насосных станциях, торговых центрах, так и об интеллектуальных системах для частных домов.

Увеличивается количество как хакерских атак, так и их способов. «С каждым годом функциональность вредоносного программного обеспечения (ПО) увеличивается. Преступникам доступны те же прогрессивные технологии, что и производителям решений безопасности и сервис-провайдерам. Злоумышленники активно используют машинное обучение, компьютерное зрение и другие современные технологии для взломов систем и платформ умного дома, беспроводных точек доступа, подключенных устройств», — сообщил директор проектного направления Group-IB Антон Фишман.

Так, в апреле 2018 года эксперты Menlo Security зафиксировали волну кибератак на финансовые и ИТ-организации в США и на Ближнем Востоке. Нападение ведется новым многоступенчатым методом, использующим уязвимость одного из продуктов Microsoft: сотрудники компаний получают письма с файлами Microsoft Word, в документах спрятаны специальные HTML-теги, отвечающие за загрузку вредоносного ПО FormBook. Активированная вредоносная программа запоминает порядок нажатия клавиш, крадет содержимое буфера обмена, считывает пароли, может самостоятельно загружать файлы, завершать и перезагружать работу системы. Причем антивирусные программы не замечают такую цепочку вредоносных действий.

Хакеров может вовсе не интересовать конкретное подключенное устройство, у них в арсенале большое количество методов сбора ботнетов (множество подключенных к Сети и зараженных вредоносными программами устройств IoT). Можно, к примеру, отсканировать диапазон IP-адресов, найти окно уязвимости, заразить и войти в эту ботнет. Начальник отдела ЗАО «МНИТИ» (Московский научно-исследовательский телевизионный институт) Михаил Смагин на примере телевизоров приводит пример, как для масштабных нарушений может использоваться всего одно подключенное устройство: «Современный телевизор — практически компьютер, который можно использовать в интересах злоумышленника. Это активация рекламы, майнинг криптовалют, использование в DDoS-атаках, слежка через встроенные видеокамеры за конкретными личностями».

Еще один аспект, помогающий взламывать подключенные к Сети устройства, отмечают собеседники «Теле-Спутника»: в большинство массовых умных вещей нецелесообразно встраивать мощные процессоры, так как они могут серьезно повысить стоимость абонентского оборудования. При этом ограниченная вычислительная мощность и небольшой объем памяти затрудняют применение сложных криптографических алгоритмов. В итоге устройства остаются уязвимыми.

«Кроме того, за умными вещами стоят IoT-платформы, которые контролируются совершенно конкретными людьми со своими интересами», — уверяет президент Ассоциации российских разработчиков и производителей электроники (АРПЭ) Иван Покровский. «Было бы наивно полагать, что чайник, наделенный искусственным интеллектом, может перехватить управление домом и даже вытеснить человека из его жилища, как это сделал герой рекламного ролика Сбербанка Mr. Чайник. Угрозу представляют не умные чайники, а недоверенные системы Интернета вещей, через которые злоумышленники могу влиять на нас. Есть факты кибератак на сетевое и серверное оборудование, которые совершались через систему Интернета вещей», — поделился он.

Кто виноват

Возникает вопрос: кто отвечает за возникающие окна уязвимостей в IoT? В списке «виноватых», считают участники круглого стола, несколько представителей. Это и пользователи, которые упрощают работу злоумышленникам, используя дефолтные и устанавливая легкие пароли, не проверяют оборудование на вирусы, подключаются в общественных местах. «Абоненты не предъявляют к конечным устройствам требований безопасности», — отмечает директор по стратегическим проектам и коммуникациям холдинга GS Group Андрей Безруков. «Пользователю необходимо объяснять, зачем он должен выбирать между защищенным и незащищенным оборудованием, каковы последствия использования небезопасных устройств», — дополняет Антон Фишман.

В ответе за безопасность и производители оборудования. Раньше большая часть бытового оборудования (телевизоры, телефоны) имела вшитое ПО без возможности модификации, производители оборудования могли обновить программу только в своих сервис-центрах. Теперь разработчики могут обновлять прошивки на расстоянии. «Созданы платформа и программно-аппаратные средства, которые позволяют дистанционно с сервисного центра выйти на любое устройство, модифицировать его функции, снять с него всю необходимую информацию. Дальше в погоне за новыми сервисами смастерили троянского коня: чтобы привлечь потребителя к Smart TV, сначала ввели условный Skype, встроили телекамеру, включили функции управления жестами, распознавания по лицу. Были созданы все необходимые условия, чтобы это устройство из троянского коня превратилось в полноценного шпиона», — говорит заместитель генерального директора МНИТИ, руководитель секции по приемному оборудованию Ассоциации разработчиков и производителей аппаратуры телерадиовещания (АРПАТ) Константин Быструшкин. По сути, потребители оказались в полной зависимости от производителя оборудования.

Участники круглого стола задались вопросом — должны ли отвечать за безопасность подключенных устройств операторы и сервис-провайдеры? «Безопасность вряд ли когда-то будет коммерческим драйвером B2C-сегмента. С другой стороны, больше в этом заинтересованы операторы, и это может быть некоторым драйвером продаж корпоративных решений», — полагает Андрей Безруков.

По мнению заместителя генерального директора SAP CIS Юрия Бондаря, к которому «Теле-Спутник» обратился за экспертным комментарием, к теме безопасности подключенных к Сети устройств и сервисов необходимо привлечь четыре стороны: государство, производителей (разработчиков) оборудования, провайдеров облачных платформ и потребителей.

Государство может выступать неким арбитром, который выработает правила игры на рынке безопасности, в первую очередь разграничит и соотнесет между игроками рынка меру ответственности за безопасность IoT-устройств. Производитель, как правило, не обладает компетенциями в разработке систем и механизмов безопасности, исторически его основное направление — это создание оборудования. Провайдер облачных платформ предоставляет сервисы и услуги, выступая посредником между производителями и потребителями. Пользователь в итоге несет на себе все риски незащищенных устройств и вынужден самостоятельно разбираться с возникающими в этом направлении проблемами — эту ситуацию необходимо изменить.

Компании направляют инвестиции на развитие самих технологий, и мало кто задумывается о том, что этим решениям необходимы инструменты защиты от кражи информации, взлома оборудования. Отдельно стоит отметить оценку экономических рисков от подобных инцидентов, — настаивает Юрий Бондарь.

Беззащитный IoT

Согласно п.1 ст.41 ФЗ «О связи» все технические средства в сети связи общего пользования подлежат обязательному подтверждению соответствия установленным требованиям. Документ предусматривает два вида подтверждения соответствия: декларирование и сертификацию.

Сертификации в обязательном порядке подлежат технические средства, указанные в «Перечне средств связи» (Постановление Правительства РФ от 25.07.2009 №532). Оконечного оборудования в этом перечне нет. Получается, что все бытовые предметы и системы, подключаемые к сети передачи данных, подлежат лишь обязательному декларированию.

Порядок декларирования установлен «Правилами организации и проведения работ по обязательному подтверждению соответствия средств связи» (Постановление Правительства РФ от 13.04.2005 №214). Согласно п.10 Правил заявитель (юридическое лицо или индивидуальный предприниматель, обратившиеся с заявлением о проведении обязательного подтверждения соответствия средства связи) при декларировании соответствия выбирают установленные требования, которым соответствуют средства связи; заключает с испытательной лабораторией (центром) договор о проведении испытаний, передает экспертам образцы и техническое описание на русском языке; направляет на регистрацию в Федеральное агентство связи (Россвязь, отвечает и за сертификацию) экземпляры декларации о соответствии. Впоследствии Приказ Минкомсвязи РФ от 29.07.2015 №288 разрешил декларировать соответствие любой организации или предпринимателю, имеющему с производителем договор, в котором указано, что производитель берет на себя обязательства обеспечить соответствие продукции установленным требованиям.

Информационная безопасность IoT также затрагивалась и в проекте программы «Цифровая экономика». Как сообщал осенью 2017 года информационный портал CNews, проект плана мероприятий на 2018—2020 годы программы по разделу «Информационная безопасность» содержал предложения по поддержке разработок в сфере IOT, киберфизических систем и больших данных. Для межмашинного взаимодействия киберфизических систем планировалось разработать систему национальных стандартов, единственно допустимых для применения в России.

После предполагалось создать систему добровольной сертификации в области киберфизических систем, а также испытательных лабораторий и инфраструктуры для подтверждения соответствия такой сертификации в рамках национальных и международных стандартов. Появление центров сертификации позволило бы присваивать статус «IoT Ready» для программно-аппаратных комплексов (ПАК) отечественного производства. Для киберфизических систем планировалось разработать отечественную свободную операционную систему, которая стала бы основой для разработки надежных, безопасных и эффективных устройств для IoT, в том числе «умных вещей», коммуникационных и интеграционных устройств.

Рабочая группа по направлению «Информационная безопасность» программы «Цифровая экономика», возглавляемая генеральным директором группы компаний InfoWatch Натальей Касперской, высказалась критично по отношению к большинству из данных инициатив.

В конце марта 2018 года вышло распоряжение №528-р «О бюджетных ассигнованиях на реализацию первоочередных мероприятий программы “Цифровая экономика Российской Федерации”». Согласно документу, по направлению информбезопасности Минкомсвязь получит 350,1 млн рублей на финансирование АНО «Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий». На эти деньги будут проведены анализ устойчивости, рисков и угроз безопасного функционирования единой сети электросвязи, а также исследования по теме «План разработки стандартов обеспечения информбезопасности сетей связи общего пользования».

Также планируется определить целевые значения информбезопасности Рунета и создать национальный удостоверяющий центр для устойчивого взаимодействия устройств в российском сегменте Интернета, корневой сертификат которого является доверенным для международных удостоверяющих центров и основных операционных систем. Минпромторгу предстоит модернизировать системы критериев для определения ПО, а также телекоммуникационного, компьютерного и серверного оборудования российского происхождения.

Каких-то конкретных шагов по защите IoT-платформ и устройств не прописано. «Между тем рынку необходима единая стандартизация по безопасности подключенного к Интернету оборудования и различных платформ Интернета вещей», — говорит Антон Фишман. Он объясняет, что эта стандартизация должна быть проверена экспертами по безопасности, протестирована временем и принята в качестве обязательной для всех игроков рынка. Пока этого нет, каждый поступает, как хочет.

С коллегами соглашается Юрий Бондарь: единого стандарта по безопасности, который бы регулировал подход к информации и ее защите, не существует. Есть компании, например «Лаборатория Касперского», которые в российской среде создают системы защиты для промышленных и персональных подключенных устройств. «Пока это единичные компании, еще не сформировался рынок защиты подключенных устройств. А для этого должна появиться обратная связь от пользователя, отражающая потребность в дополнительных мерах безопасности», — говорит представитель SAP CIS.

Участники круглого стола «Теле-Спутника» уверены, что для решений Интернета вещей необходимо создавать многоуровневые системы безопасности, включая защиту узлов, хранилищ, сети и экосистемы в целом. Пока же отсутствует даже определение безопасности для абонентского оборудования, не прописаны регламенты и требования. Константин Быструшкин из МНИТИ уверен, что в нормативных документах должны в числе

прочих быть прописаны следующие параметры: что делать и как доказать, если ущерб нанесен «умными вещами». «Особенно когда такие устройства подключены к федеральным ресурсам типа портала госуслуг», — дополняет Андрей Безруков.

Безопасность — обязанность государства

Иван Покровский из АРПЭ уверен, что облачные технологии совместного использования должны соответствовать требованиям доверенности. В первую очередь это касается облачных систем обработки данных и управления, к которым подключаются абонентские устройства и другие объекты, сопряженные с концепцией IoT. «Чтобы обеспечить необходимый уровень доверенности и парировать постоянно появляющиеся новые киберугрозы, у государственного регулятора должен быть доступ к разработчикам и процессу разработки. Это практически невозможно при использовании решений зарубежных вендоров», — настаивает глава ассоциации.

Андрей Безруков задается вопросом: смогут ли операторы и сервис-провайдеры быть уверены, что они обеспечивают безопасность пользователя при использовании иностранного оборудования и софта? Он отметил, что в GS Group при производстве систем умного дома для защиты отдельных элементов используется проприетарное ПО собственной разработки.

Иван Покровский соглашается, что на российском рынке абонентских устройств преобладает продукция зарубежного производства, но проблема не столько в оконечных устройствах и в месте их производства. Антон Фишман приводит в пример политику распространения обновлений Google и Apple. Apple одним обновлением распространяет «заплатки» и исправления для всех устройств, Google же выпускает обновление для своей платформы Android, а дальше Samsung, Lenovo и другие вендоры вынуждены вносить изменения в свои прошивки и распространять отдельно обновления для своих устройств.

«Все процедуры признания оборудования российским опираются на методики расчета добавленной стоимости и расчеты доли российских компонентов. Это развивает компетенции бухгалтеров и юристов, которые готовят расчеты и проходят необходимые процедуры подтверждений, но это не создает спрос на доверенные решения и не развивает соответствующих инженерных компетенций», — рассуждает Иван Покровский.

Константин Быструшкин отмечает, что если ПО будет на 100% отечественным, информационную безопасность при использовании импортной элементной базы гарантировать нельзя, так как, к примеру, в микросхемах могут быть аппаратные «закладки», реализующие незадекларированные функции. «Оборудование в нашей стране на 95% иностранное: из 60 наименований изделий, которые покупают потребители, только одно-два производятся в России. Мы продаем вооружение, а бытовую технику все еще покупаем. И причина в том, что нет собственной элементной базы», — подчеркивает председатель экспертного совета АРПАТ Калью Кукк.

Участники круглого стола пришли к мнению, что, возможно, стоит разработать некое доверенное приложение или систему, устанавливаемую поверх IoT-программ, сервисов и решений, которые встраиваются в оконечное абонентское оборудование. «Такие системы могут отслеживать правомочность действий и блокировать их, если, к примеру, устройство начинает выходить на некий сайт, который не прописан в IoT-программе, или выполнять нелогичные действия. Это технически снимет значительную часть проблем с безопасностью решений Интернета вещей», — считает Константин Быструшкин.

При этом к такой системе должны быть применены единые требования, распространяемые на все зарубежные решения, которые реализуются на территории РФ. Константин Быструшкин привел в пример глобальную навигационную спутниковую систему (ГЛОНАСС), которую с 2017 года необходимо устанавливать на все транспортные средства, ввозимые в нашу страну. В апреле 2018 года Министерство транспорта РФ опубликовало проект приказа, который с 1 января 2022 года обяжет оснащать ГЛОНАСС и самолеты. Новые требования вводятся по поручению президента России Владимира Путина «по результатам проверки развития и использования ГЛОНАСС в интересах модернизации экономики и развития регионов страны».

Все в наших руках

Очевидно, что новые технологии делают жизнь людей лучше и проще. Различные умные устройства, подключенные к Сети, проникают в наши дома и офисы. Полноценными компьютерами теперь являются не только традиционные десктопы, ноутбуки, планшеты и смартфоны, но и телевизоры с ТВ-приставками.

И если риски, с которыми сопряжено использование мобильных гаджетов, очевидны, а методы борьбы с ними известны, то об обеспечении безопасности использования устройств, лишь только недавно наделенных возможностью подключения к Сети (телевизоров, ТВ-приставок, систем умного дома, IP-камер и других), массовые потребители пока не задумываются.

В то же время абонентские подключенные устройства могут нести неменьшую угрозу для безопасности пользовательских данных. Также злоумышленники могут использовать умные устройства не против их владельцев, а для организации глобальных распределенных атак, например на банки и госучреждения. Таким образом простые пользователи становятся невольными соучастниками киберпреступлений.

Ситуация усугубляется тем, что подавляющее большинство абонентских устройств и компонентов, из которых они состоят, производится за рубежом. В России даже нет законодательных требований к обязательной сертификации такого оборудования. Мы можем только догадываться, какие незадекларированные возможности и уязвимости «зашиты» в устройства, которые нас окружают, и кто ими может воспользоваться. С учетом текущей геополитической ситуации это вызывает особую тревогу.

Российскому отраслевому сообществу с обязательным привлечением государства необходимо выработать шаги по изменению столь неблагоприятной ситуации. Основными из них должны стать: наращивание производства российского оборудования и компонентной базы и, как следствие, увеличение доли отечественной продукции на рынке абонентских устройств, создание четких критериев доверенности решений, предназначенных для распространения в России.

До тех пор, пока эти меры не будут приняты, говорить о том, что российские пользователи находятся в безопасности, не приходится. ■