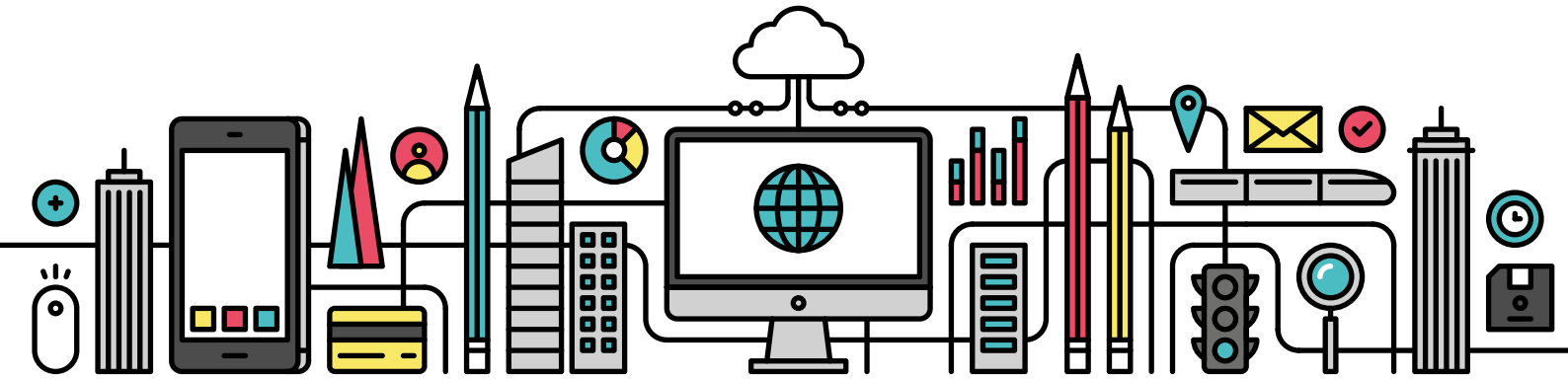


Каких хлопот потребует IoT

Спикеры ИТ-компаний (в отличие от игроков рынка систем безопасности) считают, что время интернета вещей (IoT) уже наступило. Просто пользователи никак не хотят в это поверить. Как результат — работа по развитию IoT и IIoT (промышленный интернет вещей) не идет дальше пиара на модных аббревиатурах. Журнал RUБЕЖ выяснил, в чем причина дисконнекта между технологией и ее внедрением.

Подготовили: Станислав Тарасов, Римма Ремизова

Александр Владимиров
руководитель отдела перспективных разработок ООО ГК «РОСОХРАНА»

Основная преграда для массового внедрения — экономическая. Если начать с элементарного аппаратного уровня: модуль передачи данных (проводной или беспроводной) стоит немало. И оснащение им любого устройства неизбежно приведет к пропорциональному повышению стоимости.

По стандартам: уже достаточно давно провайдеры и дистрибьюторы активно рекламируют для применения в любых устройствах IoT-технологию LoRa, принадлежащую американской корпорации. Если для тех же счетчиков ЖКХ технология вполне применима, то для устройств систем безопасности — неприемлема хотя бы из-за существенной задержки при доставке извещений. Для систем безопасности больше подходит технология UNB, которая, к сожалению, не так активно продвигается.

Но обе эти технологии требуют колоссальных инвестиций для разворачивания сетей с «нуля». В этом плане большим толчком для развития IoT должен стать коммерческий запуск сетей LTE-M и NB-IoT. Операторы сотовой связи находятся в более выгодном положении для перспектив развития предоставления услуг IoT — сети с глобальным покрытием уже есть, их нужно только модернизировать.

Алексей Кычкин
директор по науке INSYTE Electronics (ООО «ИНСАЙТ ЭЛЕКТРОНИКС»)

Концепция интернета вещей предусматривает M2M (межмашинное) взаимодействие отдельных цифровых устройств, в том числе встроенных в оборудование и технику, посредством единой инфокоммуникационной вычислительной сети. На сегодня реальных кейсов

IoT issues / By Stanislav Tarasov, Rimma Remizova

Speakers of IT companies (unlike safety market players) believe that the time for IoT has come. But users won't believe it. As a result — work on IoT and IIoT goes no further than market exercise on modern abbreviations. The RUBEZH magazine found out what is the reason of disconnection between the technology and its implementation.

полноценного внедрения IoT немного. Достижениями могут похвастаться в основном страны Западной Европы, США, Япония, Корея, Китай и другие страны с высоким уровнем развития цифровых технологий передачи информации. В России кейсы с полноценным внедрением IoT-решений мало известны, однако общую готовность можно считать высокой.

Ключевыми, но не основными факторами, препятствующими массовому внедрению, можно назвать отсутствие сетевой инфраструктуры и низкий уровень автоматизации. Для примера можно отметить, что реальная потребность промышленности и ЖКХ России в IoT-устройствах пока невелика, сказывается преобладание традиционных форм управления. Но в ближайшие годы видится резкий скачок потребности.

Системы безопасности внутри интернета вещей, особенно для промышленных приложений, несомненно, будут проходить процедуры сертификации и постоянные проверки. Системы безопасности вне IoT, естественно, сохранятся. Они будут иметь менее развитую функциональность, но более высокую надежность.

Денис Гасилин

директор по маркетингу АО «РАМАКС Интернешнл»

Международные аналитические агентства считают, что мировой объем IoT-рынка на конец 2017 года составил порядка $160-180 млрд. К 2020 году рынок превысит $1 трлн, а к концу 2024-го ожидается рост приблизительно до $4,3 трлн. Причем IIoT, по моим прогнозам, в целом является не менее перспективным к росту направлением. Он будет расти темпами, минимум соизмеримыми с потребительским сегментом интернета вещей, если не опережая его.

>60 млрд ₽

составит объем российского рынка IoT и межмашинных коммуникаций по итогам 2017 года

Аналитическая компания J'son&Partners Consulting

Что касается России, то сошлюсь на данные аналитической компании J'son&Partners Consulting, согласно которым по итогам 2017 года объем российского рынка IoT и межмашинных коммуникаций превысил 60 млрд рублей. Ожидается, что по итогам 2022 года его объем достигнет почти 90 млрд рублей, а структура претерпит значительные изменения: доля услуг в области передачи данных и аппаратно-программных комплексов снизится с 70% до чуть более 40%, а доля облачных сервисов, наоборот, вырастет практически в пять раз.

По данным PricewaterhouseCoopers, суммарный эффект для российской экономики от внедрения интернета вещей может составить до 2025 года порядка 2,8 трлн рублей. Это очень серьезные показатели. При этом скачок в развитии сделают компании из электроэнергетической отрасли и ритейла. Видоизменится также транспортно-логистическая отрасль, получит новое направление для развития и модернизации своего бизнеса банковская сфера.

IoT в России сейчас — это 20-25 млн устройств. По данным J'son&Partners Consulting, к 2020 году число подключенных устройств может достичь чуть ли не 50 млн. Главным драйвером роста выступает высокая конкуренция на рынке, стимулирующая внедрение новых технологий для анализа и управления покупательским и клиентским спросом.

Препятствием для развития IoT в России является отсутствие правового поля, позволяющего правомерно использовать те или иные технологии.

Игорь Хереш

директор по развитию бизнеса АО «Группа Т-1»

Внедрение технологий IoT тормозят риски кибербезопасности и разрозненность протоколов и стандартов работы IoT-устройств. Глобальный вопрос безопасности передачи данных и удаленного управления устройствами не решен, и о том, когда это случится, сказать сложно. Массовой та или иная технология становится, когда ее используют крупные заказчики. Однако чтобы это случилось, технология должна быть «обкатана» на небольших сегментах. Сегодня же далеко не все готовы брать на себя ответственность за возможные ошибки.

Что касается частотных стандартов передачи данных, то, к сожалению, на данный момент фактически каждый производитель имеет свой проприетарный протокол. Хочу верить, что уже в скором времени основные игроки рынка придут к единому стандарту и будут сфокусированы на качестве фактически оказываемых сервисов для клиента, а не на закрытости своих протоколов.

Ирина Яхина

директор по технологиям Hitachi Vantara (ООО «Хитачи Вантара») в North EMEA

Одной из главных трудностей при реализации проектов в области IoT может стать отсутствие профильных специалистов. Руководитель также должен понимать, что процессы внедрения IoT-решений могут инициироваться «снизу», поэтому его цель — выстроить взаимодействие внутри проектной команды. Тогда процесс внедрения IoT-системы будет идти эффективнее, а результаты принесут большие преимущества.

Главное, на чем строится интернет вещей, — это данные компании. Соответственно, еще на этапе подготовки внедрения IoT в организации руководителям необходимо продумать, как создать надежную систему защиты своих данных. Она обязательно должна включать три аспекта: обеспечение конфиденциальности, сохранение целостности (в процессе перемещения данных по сети), аутентификацию. Для совершенствования технических решений разработчикам систем безопасности нужно совместно определить стандарты и спецификации, которые обеспечат взаимодействие средств безопасности с другими высокотехнологичными устройствами и системами.

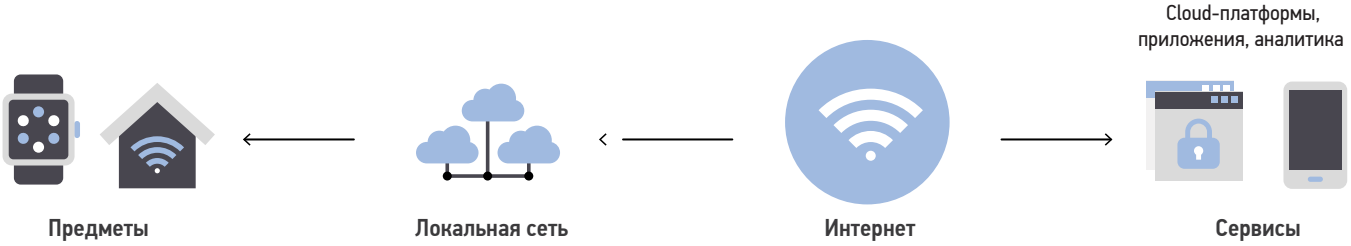
Поскольку IoT становится все более востребованным, логично ожидать, что будут совершенствоваться и способы обеспечения безопасности. Это, возможно, даст какой-то новый толчок развитию на рынке систем безопасности, однако вряд ли только из-за интернета вещей нас будут ждать революционные изменения в этой сфере.

Яков Гродзенский

руководитель направления информационной безопасности ООО «Системный софт»

Один из основных моментов, мешающий внедрению интернета вещей в России, — все еще недостаточное финансирование, как с точки зрения поддержки государства в рамках «Умного города», так и на промышленных предприятиях в области IIoT. Суммы, выделяемые на техноло-

Архитектура IoT



гии интернета вещей растут в процентном отношении, однако пока не доходят до размеров, приемлемых для массового внедрения.

Владимир Ласовский

менеджер по развитию бизнеса Orange Business Services (ООО «Эквант»)

У нас имеется множество кейсов внедрения в разных странах для заказчиков из разных отраслей — под нашим управлением находится более 17 млн датчиков по всему миру. В России мы выходим на первые пилотные внедрения. На данный момент заказчики, с которыми мы общаемся, перед массовым развертыванием решений хотят видеть доказательства его работоспособности и эффективности. После этого следует стадия ограниченного внедрения на «боевой» инфраструктуре. А затем уже можно говорить о полноценном коммерческом проекте с его тиражированием.

Обычно мы используем уже созданное оборудование разных вендоров, как российских, так и зарубежных, в зависимости от того, что наилучшим образом подходит в каждом конкретном случае — решения интернета вещей всегда индивидуальны. Тем не менее в нескольких случаях приходится использовать оборудование, разработанное специально под конкретные запросы. В одном из проектов из-за большого территориального применения решения мы опирались на стандарт GSM, но при необходимости рассматриваем любые существующие протоколы передачи данных — от LoRaWAN до Maritime VSAT.

Сергей Павлов

технический директор Artezio (ООО «АРТЕЗИО», группа компаний «ЛАНИТ»)

Появление IoT-систем практически не повлияло на расстановку сил на рынке систем безопасности. Большинство IoT-решений фокусируется на простом информировании пользователей о происходящих инцидентах.

Только специальные подразделения ведомств, отвечающих за предупреждение ущерба, предлагают так называемые «профессиональные» системы безопасности. Это менее информативные решения, без уведомлений и SMS, которые обеспечивают быстрое реагирование на инциденты. Данные с устройств приходят на пульт охраны, и при попытке проникнуть в квартиру или офис на место выезжает команда быстрого реагирования. При пожаре срабатывает система тушения либо поступает сигнал в ближайшую пожарную часть.

Но в будущем IoT может кардинально изменить рынок систем безопасности. Новые программные платформы для управления IoT-устройствами легко масштабируются и позволяют подключать «умные» устройства нового типа — предупреждающие ущерб.

Вениамин Липский

основатель и финансовый директор проекта Kviku (ООО МФК «ЭйрЛоанс»)

Рынок интернета вещей в России ежегодно увеличивается более чем на 20%. Этот процесс постепенно усиливается за счет массовой цифровизации крупных компаний и корпораций. Действительно, развитию рынка интернета вещей способствуют госструктуры, которые пытаются идти в ногу со временем и внедрять некоторые сервисы в нашей стране.

> Одним из сдерживающих факторов развития интернета вещей остается отсутствие внятной позиции государства

Мы наблюдаем возросший интерес к этому рынку и со стороны бизнеса. Аналитики отмечают прирост инвестиций в сферы, которые формируют соответствующую экосистему: развитие услуг связи, разработка новейшего программного обеспечения и необходимого оборудования.

Одним из сдерживающих факторов развития интернета вещей остается отсутствие внятной позиции государства, которая могла бы выражаться в виде принятых стандартов, необходимых для регулирования всех процессов по построению цифровой экономики. Но какая-то работа сейчас в ведомствах в этом направлении идет. По крайней мере мы слышим об этом от руководителей основных ведомств на форумах и конференциях, посвященных «индустрии 4.0».

В ближайшие 4-5 лет при отсутствии глобальных экономических шоков и курсовых изменений рынок интернета вещей в России должен превысить $10 млрд.

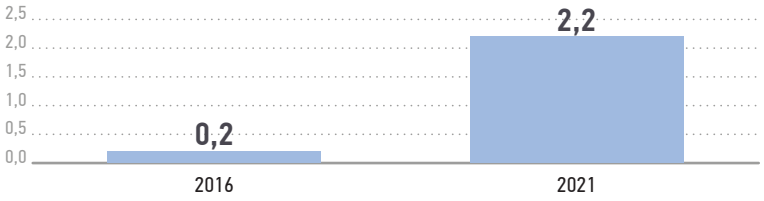
Алексей Виноградов

генеральный директор Lockerbox (ООО «АКХ»)

Главная проблема для IoT — отсутствие единого и общепринятого стандарта связи между оборудованием. Барьером также является и неудовлетворительный уровень сигнала для подобных приборов. Даже в столице

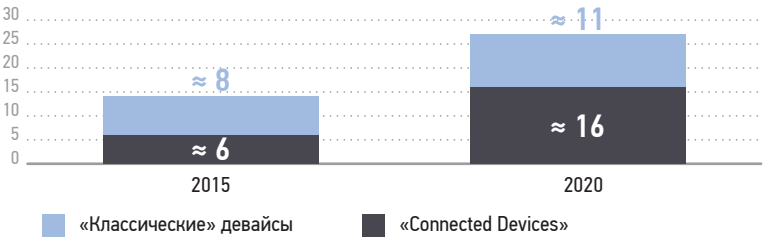
Прогноз развития IoT

Ожидается рост трафика M2M в среднем на 70% в год, ЭБ в мес.



Количество «Connected Device» вырастет в 4 раза

Приблизительное количество устройств в миллиардах



Источник: Machina Research; Cisco; Ericsson

существуют точки, где связь функционирует недостаточно стабильно, а подключить оборудование к локальной сети клиента не всегда возможно.

С точки зрения рисков, то это два ключевых типа угроз: управление доступом к устройствам извне и обеспечение целостности данных. На мой взгляд, именно по этому пути будет развиваться рынок безопасности, т. е., с одной стороны — улучшение системы аутентификации, чтобы избежать «вторжения» извне, а с другой стороны — шифрование потоков данных, которые поступают на устройства и с устройств по сети.

Григорий Кузнецов

руководитель лаборатории системной интеграции кафедры Телекоммуникационных систем Московского Института Электронной Техники (МИЭТ), руководитель Сетевой академии Cisco МИЭТ

Интернет вещей сегодня внедряется во всех известных отраслях, начиная с транспорта и заканчивая здравоохранением. При этом массовому внедрению интернета вещей особо ничего не мешает, т.е. каких-то крупных технологических причин я не вижу. Этот переход можно сравнить с любой технологической революцией.

Там, где это реально нужно, где интернет вещей дает реальную прибыль, он активно внедряется. Два года назад устройств, подключенных к интернету, было 18 млрд, а сейчас их уже примерно 28 млрд. И мы не говорим, что это только смартфоны и компьютеры. Это различные вещи, которые с ними взаимодействуют. Есть прогноз, что к 2020 году число устройств достигнет примерно 50 млрд.

Мы для передачи данных руководствуемся стандартами LoRa и LoRaWAN. Первый — технология физического и канального уровня, а в LoRaWAN есть еще шифрование, которое обеспечивает безопасность. Эти технологии позволяют передавать данные по радиоканалу. Нужны эти стандарты для того, чтобы позволить устройствам тратить меньше энергии и передавать информацию на большие расстояния.

Изменит ли интернет вещей расстановку сил на рынке систем безопасности? С учетом большого количества трафика должны разрабатываться и появляться решения, которые позволяют защищаться. Сейчас может получиться, что крупные игроки на рынке систем безопасности разработают новые продукты. Но из того, что я наблюдаю, они не хотят выделять это в какой-то вид новых кейсов. Они просто пытаются адаптировать существующую систему безопасности для защиты устройств и трафика интернета вещей. Даже если какие-то маленькие стартапы найдут новые технологии, те компании, у которых есть деньги, просто выкупят их и получат в свой актив. Мне кажется, что расстановку сил на рынке систем безопасности это не изменит.

Александр Вахтин

управляющий телекомкомпанией ООО «Телеком-Биржа»

Развитию IoT в промышленности мешают отсутствие бюджетов на такие проекты, отсутствие стандартов и адекватных систем кибербезопасности, которые бы позволили построить реальные IoT-продукты на базе платформ, а не решения квази-IoT.

Сейчас можно использовать только отраслевые стандарты, т. к. новые только планируются к разработке. Полезно также использовать референсную архитектуру и методологию создания IoT-решений, они международные и созданы на основании лучших практик зарубежных вендоров. Отечественные компании (например, «Стриж») делают свои решения и протоколы, но это может быть тупиковый вариант с точки зрения совместимости систем и расширения линейки поддерживаемых устройств.

Евгений Ойстачер

старший партнер компании EKF (ООО «Электрорешения»)

В Москве и Казани уже появился ряд операторов связи, развернувших сети для удаленного управления устройствами (датчиками, контроллерами и др.), а также цифрового учета ресурсов. К этим сетям уже подключены тысячи приборов учета расхода холодной и горячей воды, потребления энергии и газа.

На российском рынке также представлены решения для дистанционного мониторинга газовых котельных, позволяющих осуществлять эксплуатацию без непосредственного присутствия обслуживающего персонала. Все это стало возможным благодаря использованию самых передовых IoT-технологий.

Однако примеры внедрения таких решений пока единичны, а предлагает их ограниченное количество компаний. Данные исследования J'son&Partners Consulting свидетельствуют о том, что глубина проникновения IoT в России на конец 2017 года составляла всего 0,35% от общемирового уровня.

Основной тормоз массового внедрения — психология потребителя. У конечного пользователя пока отсутствует

понимание ценности IoT. И конечно, чем современнее технология, тем, как правило, она дороже. Например, обычный счетчик учета электроэнергии стоит от 600 рублей, а «умный» — от 3,5 тыс. до 10 тыс. рублей. Здесь необходима большая просветительская работа, чтобы донести покупателю (это и сбытовые, и управляющие компании, и потребители) выгоду, которую он получит при установке нового прибора.

Что касается крупных промышленных предприятий, то пока большинство инженеров воспринимают IoT как «новый вариант» АСУ ТП (автоматизированные системы управления технологическими процессами. — Прим. ред.), и, если на этом производстве он уже есть, они не понимают, зачем еще что-то внедрять и «дополнительно» автоматизировать.

Виктор Мазурик

директор по маркетингу и монетизации инноваций Блока R&D АО «ЭР-Телеком Холдинг»

На сегодняшний день рынок интернета вещей в России только начинает развиваться, происходит его становление. В России реализованы точечные проекты на основании технологии LoRaWAN, существуют локальные сети нескольких компаний на уровне одного города, нескольких районов в городе или нескольких домов. В основном это кейсы в ЖКХ, локальные пилотные проекты в промышленности, но, как правило, они не публичны. Кейсов масштабного внедрения в нескольких регионах на основе единой сети от одного оператора пока нет.

Для стимулирования внедрения и использования решений и сервисов в области интернета вещей необходимы слаженные действия всех участников цифровой экосистемы. Государство должно обеспечивать гибкое регулирование и создавать стимулы для развития инновации. Бизнесу, в свою очередь, необходимо пересмотреть отношение к рискам, быть готовым к экспериментам и быстрому самообучению, проявлять открытость для построения межотраслевой системы взаимодействий с другими игроками. Только благодаря отсутствию ограничений со стороны регулирующих органов и при равенстве доступа компаний к технологиям интернета вещей возможно создание конкурентной среды, в результате чего рынок интернета вещей может стать реальным драйвером цифровой экономики страны.

Александр Коломиец

руководитель отдела маркетинга компании Rightech

Распространению IoT препятствуют три серьезные проблемы. Во-первых, отсутствие специалистов — 95% разработчиков не обладают достаточной квалификацией для работы с системами интернета вещей, а оставшиеся 5% заняты в глобальных корпорациях и недоступны для малого и среднего бизнеса.

Во-вторых, сроки — разработка IoT-системы для конкретного бизнеса «с нуля» требует работы 7-15 дорогостоящих высококвалифицированных разработчиков (которых, как мы помним, на рынке в принципе мало) и занимает более 2-3 лет. Из-за громоздкости и продолжительности 80% таких проектов остаются незавершенными или заканчиваются неудачей — и даже в случае успешного запуска доработки и правки также будут отнимать много времени. Современному бизнесу так долго ждать нельзя — конкуренты и рынок уйдут далеко вперед.

В-третьих, многообразие видов подключаемых устройств — при каждом обновлении используемых датчиков владелец бизнеса вынужден тратить время на доработку своей IoT-системы.

Тем не менее бизнес с работающей IoT-системой, бесспорно, имеет огромные возможности для развития. Автоматизация процессов, сокращение затрат на контроль и обслуживание и минимизация издержек — все это позволяет существенно сократить расходы и увеличить прибыль. А значит, интернет вещей будет притягивать все больше и больше бизнес-единиц.

В то же время переход бизнеса на IoT значительно повышает степень его уязвимости. Под угрозой сами устройства, их программное обеспечение, каналы передачи данных, протоколы и системы обработки данных. В результате появился целый пласт уязвимостей, которые еще никем не изучены. Поэтому комплексных решений для безопасности IoT-систем со 100%-ной гарантией защиты пока не существует.

Екатерина Кравченко

руководитель департамента сетевых продуктов Aruba, Hewlett Packard Enterprise (ООО «Хьюлетт Паккард Энтерпрайз»)

Интернет вещей из технологии будущего постепенно превращается в технологию настоящего, и Россия — не исключение. В нашей стране внедрение IoT уже помогает оптимизировать деятельность компаний в самых разных отраслях, а инвестиции в технологию увеличиваются с каждым годом. Так, по данным исследовательской компании IDC, в 2021 году они превысят $9 млрд, а это в три раза больше, чем в 2016 году.

У IoT-технологии огромный потенциал и почти нет минусов, кроме разве что высокой стоимости. Но этот недостаток с лихвой компенсируется оптимизацией процессов и впечатляющим экономическим эффектом, измеряющимся сотнями миллиардов рублей.

У IoT-технологии огромный потенциал и почти нет минусов, кроме разве что высокой стоимости

Развитие IoT замедляют юридические и стандартизационные барьеры, отсутствие благоприятной регуляторной среды — распространение новых технологий традиционно тормозится длительностью процессов регистрации и внедрения. Очевидно, что необходима доработка законодательства в этой области. Что касается стандартов, то в сфере информационных технологий их необходимо привести в соответствие с новыми реалиями, адаптировать к новым технологическим условиям.

Распространение интернета вещей также немыслимо без совершенствования механизмов защиты IoT-решений от кибератак. Таким образом, IoT действительно окажет свое влияние на рынок систем безопасности, способствуя его развитию.

В России на крупнейшей хакерской конференции в этом году будет проходить конкурс по взлому системы электроснабжения двух жилых домов

Екатерина Медведева

специалист в области систем безопасности, Новосибирский общественный фонд Сибирский экспертный центр (СЭЦ) «МОДЕРНИЗАЦИЯ»

В настоящее время реальными помехами внедрения интернета вещей являются проблемы отсутствия технологической инфраструктуры в регионах и отдельных местностях. Действительно, ключевым для работы интернета вещей является высокое и стабильное качество связи, особенно работающее бесперебойно на самом объекте. На сегодня проникновение интернета в России составляет около 72%, однако качество покрытия серьезно разнится от региона к региону. Бесперебойность работы связи на объекте и на устройстве пользователя, вне зависимости от его местонахождения, — прямой залог развития IoT в нашей стране.

Немаловажно также, чтобы система регулирования строительства (в качестве задела для формирования «умных домов») уже содержала в себе элементы обеспечения IoT. Сейчас идет работа по стандартизации IoT (Ассоциацией интернета вещей), что может в дальнейшем вылиться во включение норм в СНиП и ГОСТы в области строительства, заранее обеспечивая инфраструктуру для работы IoT в сфере безопасности, информирования о парковках, управления доступом в здания и квартиры и прочее.

Можно отметить: интегрированные в рамках IoT системы безопасности все еще малодоступны и мало востребованы для рядовых жителей, в то время как организации уже видят в таких системах будущее, особенно если их можно прямо интегрировать с системами управления доступом и логистическими системами.

Алексей Парфентьев

ведущий аналитик ООО «СёрчИнформ»

Понятия безопасности в потребительском сегменте IoT сейчас не существует. Защищать «умные» устройства — задача производителей, но они заняты продажами, и в результате пользователи даже не знают об угрозах информационной безопасности. Возможно, ситуация изменится, если у вендоров появится стимул придерживаться требований к защите IoT-устройств. Например, введутся штрафы со стороны регуляторов.

В свою очередь в промышленном IoT совсем другая картина. Здесь уже есть правовое поле в виде Доктрины информационной безопасности, закона 187-ФЗ «О безопасности критической информационной инфраструктуры РФ», а также требования ФСТЭК и отраслевых регуляторов. Кроме того, и это принципиальное отличие от потребительского IoT, критические объекты понимают риски, заинтересованы устранять их и планомерно делают это.

Учитывая актуальную с 1 января 2018 года уголовную ответственность за несоблюдение правил информационной безопасности, можно ожидать, что уровень безопасности в IIoT повысится. В то же время следует понимать, что промышленный интернет вещей — это скорее про «умные» процессы, а не устройства. Усовершенствование этих процессов затратно и длительно, внедрение обычно требует масштабной реконструкции инфраструктуры, а цена выхода из строя слишком велика. Отсюда неспешная, но однозначно положительная динамика.

Георгий Цедилкин

генеральный директор компании ANP Ceges Technology

IoT родился и развивается как следующая эволюционная ступень систем автоматического управления (*АСУ ТП. — Прим. ред.*), которые получили возможность беспроводного сбора данных и управления. При этом IoT наследует и проблемы систем управления, связанные с кибербезопасностью — до начала массовых хакерских атак сейчас ни один клиент не будет платить на 20-25% больше только за то, что его беспроводной датчик «защищен».

Но на самом деле угроза уже перестала быть абстрактной: сегодня известны случаи хакерских атак на промышленные объекты. В России на крупнейшей хакерской конференции в этом году будет проходить конкурс по взлому системы электроснабжения двух жилых домов. Что может сделать злоумышленник с IoT? Подключившись к незащищенным каналам связи, он может составить профиль поведения каждой квартиры в доме и это продать.

Ситуация усугубляется тем, что рынок насыщается подобными системами и пока нет экономического стимула для изменения трендов. Немногие компании используют в своих разработках и шифрование канала, и смену ключей, и смену частоты передачи и другие способы повышения безопасности. Но даже они не внедряют дорогостоящие процессы безопасной разработки кода (SDLC), не прибегают к практике вознаграждения за выявление уязвимостей (bagbounty) и не заказывают исследования безопасности своих решений. А профессиональные исследователи ежегодно находят десятки критических уязвимостей у международных производителей оборудования автоматизации.

Илья Апполонов

руководитель группы IoT в компании ICL Services

Большинство известных нам внедрений IoT относится к сфере производства, распределения и потребления энергии, по всей цепочке от производителя до конечного потребителя. Это и системы «умных счетчиков» и «умные» системы распределения, системы поддержки регламентного технического обслуживания энергетического оборудования. В числе компаний, внедряющих такие технологии, — «Интер РАО-Электрогенерация», ПАО «Россети», АО «Концерн Росэнергоатом», многие УК начинают переходить на системы АСКУЭ, использующие в своей архитектуре подходы IoT.

Если говорить про IoT в целом, то массовому внедрению мешает отсутствие качественных отечественных решений, которые были бы дешевле по сравнению с зарубежными аналогами. Второй момент — это отсутствие понимания со стороны бизнеса всех выгод от внедрения решений IoT и того, как можно будет вернуть сделанные вложения. Таким образом, участникам рынка России на данный момент нужно больше весомых и очевидных доводов в пользу внедрения IoT-решений.