03 февраля 2016

Национальные особенности IoT

Комментарий Андрея Мелузова, руководителя департамента ИТ-аутсорсинга ГК «КОРУС Консалтинг», в рамках обзора журнала Connect о специфике IoT в России.

Тема Интернета вещей (Internet of Things – IoT) постепенно захватывает умы российских пользователей. Развитие этой индустрии у нас отличается от аналогичных процессов в других развитых странах. Дело в том, что на Западе под IoT подразумевается потребительская электроника, которая управляется через интернет-сервис, а в России часто говорят и о корпоративном, и даже о государственном IoT.

Особенности

Сразу следует отметить, что IoT – технология не новая. Это утверждает Андрей Мелузов, руководитель департамента ИТ-аутсорсинга ГК «КОРУС Консалтинг»: «Различные датчики и системы мониторинга были и раньше, но благодаря развитию сервисов, связанных с BigData, таких как проведение online-аналитики поступающей информации, прогнозирование событий на базе машинного обучения, подготовка сложной отчетности, стали доступны бизнесу сравнительно недавно». Поэтому, чтобы отличить предыдущее поколение промышленной автоматизации от современного IoT, будем называть первое M2M, поскольку те технологии в основном были

ориентированы на взаимодействие между машинами. А признаками корпоративного IoT являются наличие облачного сервиса и технологии «большой» аналитики, которые и создают новое качество.

На Западе M2M развивается достаточно давно и успешно. Чтобы расширить сферу применения интеллектуальных устройств на персональные продукты аналитики и придумали термин IoT для описания потребительской электроники. По мнению Евгения Власова, менеджера проектов в сфере IoT дизайн-центра электроники Promwad, «на Западе активно развиваются медицинские IoT-устройства (фитнес-трекеры, измерители пульса и давления), системы «умного дома», маркетинговые и информационные системы, построенные на протоколе iBeacon компании Apple. В России такого рода устройства – скорее развлечение для «гиков», чем продукты массового использования». Таким образом, на Западе главная идея использования термина IoT – привлечь разработчиков к созданию персональных интеллектуальных устройств и набора связанных с ними сервисов.

В России, опоздавшей на промышленную автоматизацию M2M, под IoT часто подразумевают именно корпоративные устройства, объединенные сетью и имеющие подключение к Интернет. Например, Алексей Сабанов, заместитель генерального директора компании «Аладдин Р.Д.», утверждает, что «развивающиеся и планируемые известные проекты в Москве, Санкт-Петербурге, Казани и Тольятти пока касаются только одного направления M2M – «Умный и безопасный город». Аналогичные сведения и у Игоря Рудыма, менеджера по развитию экосистемы Интернета вещей компании Intel: «Если говорить о рынке автоматизации, то Россия внедряет много передовых технологий, таких как мониторинг транспорта, умные парковки,

умное освещение. Новые реализуемые проекты уже изначально включают часть умного функционала Интернета вещей. Например, в жилых домах сбор данных по коммунальным услугам ведется автоматически». Таким образом, в России речь идет в основном о развитии второго поколения M2M – корпоративных систем датчиков и исполнительных устройств, объединенных с помощью интернет-сервиса.

Еще одной особенностью российского рынка, по словам Валерия Андреева, заместителя директора по науке и развитию ЗАО ИВК, является «попытка сотовых компаний протолкнуть сетезависимую реализацию Интернета вещей в качестве стандарта, т. е. намертво привязать IoT к своим сетям. Это тупиковая ветвь для нашего рынка. Во-первых, данный вариант не обеспечит уровень информационной безопасности, достаточный для серьезных применений новой технологии. Во-вторых, такая реализация сделает IoT недоступным там, где нет качественного покрытия сотовых сетей. В-третьих, мы попадем в еще большую зависимость от зарубежных производителей оборудования 5G». В качестве альтернативы Валерий Андреев предлагает использовать для организации IoT-сервисов технологию на основе MOM (Message Oriented Middleware – промежуточного ПО, ориентированного на передачу сообщений) с гарантированными сервисами защиты, доставки и контроля логики обработки информации. Такие сервисы будут работать через любые сетевые протоколы, но, главное, для них есть российские варианты реализации.

Прогнозы

От понимания термина IoT зависят и оценки рынка по количеству устройств, которые дают различные аналитики. По утверждению Алексея Сабанова, «прогнозы от Gartner и ITU практически совпадают и составляют примерно 25 млрд устройств M2M в 2020 г. к использованию в сегментах «умный дом», автоматизации зданий, транспорта, ЖКХ, государственных услуг и медицины (в порядке убывания)». Вячеслав Медведев, ведущий аналитик отдела развития компании «Доктор Веб», приводит другие цифры: «Согласно прогнозу IDC количество подключенных к Интернету устройств увеличится с 10,3 млрд в 2014 г. до 29,5 млрд в 2020-м». Константин Соловьев, исполняющий обязанности председателя правления платежной системы «Лидер», верит еще более оптимистичным прогнозам: «По экспертным оценкам, в настоящее время в мире существуют порядка 10 млрд активных устройств, а к 2020 г., как ожидается, их число возрастет до 60 млрд. Общество постепенно переходит от Internet Of Things к Internet Of Everything (Интернет всего)». Судя по термину IoE, эта оценка дана аналитиками Cisco. Таким образом, цифра Gartner – это M2M-автоматизация, IDC говорит, видимо, о персональных IoT-устройствах, а для Cisco важно оценить объемы сетевого трафика, поэтому они считают вообще все устройства.

Анализ того, насколько российский рынок IoT отличается от мирового, провел Максим Андреев, директор по бизнес-приложениям компании КРОК: «По данным IDC в 2014 г. объем мирового рынка Интернета вещей составил около 650 млрд долл. и до 2020 г. будет расти в среднем на 17%. Тем временем российский рынок IoT (включая оборудование, технологии и услуги), по подсчетам аналитиков J'son & Partners Consulting, в 2010 г. насчитывал более 100 млн долл., а к 2020 г. может вырасти до 1 млрд долл.». Таким образом,

Россия к 2020 г. будет занимать меньше 0,1% мирового рынка IoT.

Слабое развитие технологий IoT в России Дмитрий Потемкин, главный архитектор департамента защиты инфраструктуры компании «Андэк», связывает с психологическими и экономическими причинами: «В России за последнее время появилось несколько компаний-стартапов. Эти компании уже известны на мировом рынке, однако массовый российский пользователь крайне далек от заинтересованности в подобных системах. К тому же IoT часто неотделим от облачных технологий, а в РФ с этим пока все не так хорошо, в отличие от Запада. Поэтому и российские стартапы стараются в первую очередь выйти на западный рынок, поскольку это сулит им быстрое получение прибыли». Константин Соловьев также ссылается на психологические проблемы развития IoT: «Развитию IoT-индустрии в нашей стране и мире может мешать и отношение потребителя, ведь IoT – это потеря приватности. Уже сейчас ваш банк или сотовый оператор знают о вас больше, чем ваша жена».

Безопасность

Излишняя осведомленность владельцев IoT-сервисов является фактором, который сильно тормозит развитие. Потенциальные пользователи боятся, что IoT-устройства будут так же уязвимы, как компьютеры и смартфоны, и поступающие новости подтверждают их опасения. Так, Вячеслав Медведев отмечает, что «случаи взлома устройств для контроля за детьми, смартфонов, систем управления уже отмечены в прошедшем году. Как правило, «умные» устройства имеют выход в Интернет, поддерживают беспроводной доступ и рассчитаны на пользователей, не имеющих знаний в области безопасности. К

сожалению, «умные» устройства слишком легко «перевербовать». В России проблемы с развитием пользовательской IoT-индустрии могут возникнуть, в частности, из-за строгого законодательства. Евгений Власов предполагает, что «многие IoT-проекты сложно внедрить в розничную торговлю в связи с Федеральным законом “О персональных данных”». Хотя как раз использование идентификатора устройства вместо имени – легкий способ избавиться от обработки персональных данных.

Впрочем, законодательство еще больше влияет на корпоративные IoT-сервисы. Олег Левенков, руководитель инновационных проектов компании «Аладдин Р.Д.», сетует: «Особое значение в системах IoT, разрабатываемых по государственному заказу, имеет обеспечение безопасности решений и аттестации систем на соответствие требованиям регуляторов информационной безопасности. Например, в системах «Платон», «ЭРА-ГЛОНАС» существуют свои требования к используемым компонентам и технологиям и к способам их применения при построении систем. Согласно нормативным актам для каждой автоматизированной системы разработчиками создавалась модель угроз и нарушителей, в которой комплексно учитывались возможности потенциальных нарушителей по несанкционированному воздействию на объекты соответствующих систем. Между тем, проблема безопасности IoT, в частности, решений в сегменте промышленности и медицине, в подавляющем большинстве случаев не решается на основе системного подхода. Это происходит в силу того, что решения создаются зарубежными поставщиками, которые не готовы развивать отечественный рынок и стремятся продавать готовые типовые решения, которые могут не соответствовать требованиям законодательства

России. Потребителям и заказчикам таких систем обязательно нужно привлекать опытных и авторитетных интеграторов для построения систем IoT и экспертные организации для оценки безопасности проектных решений». Таким образом, требования российских регуляторов создают, с одной стороны, определенный барьер для использования иностранных IoT-устройств и связанных с ними сервисов на территории России, с другой – условия для создания более безопасных сервисов.

Следует отметить, что в России есть определенные наработки в области промышленной автоматизации, которые можно использовать, в частности, для создания IoT-инфраструктуры. Валерий Андреев указывает, что «давно существуют зрелые и проверенные практикой отечественные реализации MOM, которые можно взять за основу. Только подход на базе промежуточного ПО с интегрированными сервисами ИБ позволяет создать управляемую безопасную инфраструктуру для любых сценариев автоматического взаимодействия информационных устройств, вплоть до самых ответственных: дронов, промышленных роботов, носимых медицинских датчиков и др.». Таким образом, у российских производителей еще есть шанс создать безопасные IoT-сервисы, которые смогут конкурировать с иностранными решениями именно по безопасности предлагаемого функционала.

Материал опубликован в журнале Connect от 01.02.2016.