Развитие IoT-рынка

Несмотря на серьезное отставание России от Запада по части Интернета вещей (Internet of things – IoT), о котором говорят все аналитики, IoT уже прочно вошел в нашу жизнь и бизнес. Пожалуй, сегодня это одна из наиболее часто обсуждаемых тем на конференциях и в СМИ. В 2016 г. развитие сегмента IoT шло вполне уверенно; что ожидает данную технологию в 2017 г., а также какие вызовы стоят перед IoT сегодня, редакция узнала у экспертов отрасли.

– Как вы оцениваете текущее состояние и перспективы рынка IoT-решений в России?

Андрей Рычков,
руководитель платежной системы "Центральная касса"

– Рынок Интернета вещей в России находится в зачаточном состоянии. Массового применения решений нет, но уже идет публичное обсуждение, как можно использовать технологии в повседневной жизни. По сути, сейчас формируется общественный заказ: рынок пытается определить, что нужно покупателям, даже если они еще сами об этом не знают.

Павел Новиков,
руководитель группы исследований безопасности телекоммуникационных систем Positive Technologies

– Тема IoT-устройств сейчас популярна как никогда. Активное использование IoT в быту повышает комфорт и личную эффективность владельца. На российском рынке представлено множество IoT-решений от иностранных компаний-производителей, но для них не существует единого стандарта управления и безопасности. Устройства разных производителей невозможно заставить работать друг с другом. К примеру, пользователь вынужден скачивать несколько приложений, чтобы управлять умными розетками и лампочками в своей квартире.

Зачастую все эти IoT-устройства содержат критические уязвимости, которые легко эксплуатировать злоумышленникам. Один из ярких примеров уязвимостей IoT – нашумевшая история с ботнетом Mirai, в котором основную массу составляли Web-камеры с учетными данными типа admin:admin. Наши исследования в этой области подтверждают, что получить видео или фото с чужой Web-камеры не составляет труда, в том числе распространенных именитых производителей.

Ситуацию смогут выправить комплексные решения от крупных производителей, которые позволят связать воедино несколько устройств и в том числе защитить их.

Марат Гуриев,
директор по работе с госучреждениями Samsung Electronics

– IoT можно назвать самой горячей частью любого рынка, поскольку он приблизительно с равной скоростью развивается в каждом из своих восьми наиболее известных направлений: дом, освещение, здание, город, предприятие (индустрия), ритейл, автомобили, здравоохранение. Предполагаю, что в текущем году своими пилотными проектами рынок IoT-решений доберется до объектов внедрения во всей перечисленной восьмерке. Есть две специфические особенности успешных IoT-решений: они должны быть компактны и быстро окупаемы. А значит, это сфера активности малого и среднего бизнеса. Поэтому в конце года можно будет наблюдать множество краудфандинговых решений на базе смартфонов, планшетов, мобильных приложений, а также разнообразных датчиков, подключаемых к облачным сервисам. И, разумеется, все эти устройства должны быть оснащены серьезными средствами информационной безопасности.

– Что должно произойти в сфере технологий, чтобы Интернет вещей стал обыденным делом?

Андрей Рычков,
руководитель платежной системы "Центральная касса"

– Они должны стать дешевле и одновременно с этим полезнее для человека. Потребитель должен понимать ценность решений Интернета вещей.

Виталий Кузнецов,
управляющий партнер Office Anatomy

– Интернет вещей – один из глобальных трендов. По различным экспертным оценкам, к 2020 г. 16–30 млрд IoT-устройств будут подключены к сетям по всему миру. Только в Европе число таких устройств, по прогнозам, может

увеличиться в четыре раза. В России темпы развития Интернета вещей намного медленнее. Для активного роста необходимо повсеместное развертывание сетей стандарта 4G и впоследствии – 5G. Также важны такие факторы, как защищенность и безопасность сетей. Для решения этой задачи необходимы новые технологии, обеспечивающие безопасность данных. Дальнейшая миниатюризация датчиков и сенсоров IoT-устройств и разработка новых технологий в области энергозависимости могут также способствовать росту Интернета вещей.

Павел Новиков,
руководитель группы исследований безопасности телекоммуникационных систем Positive Technologies

– IoT-решения стали обыденным делом в личном пространстве пользователя, городской среде и на крупных предприятиях. Осведомленность о технологиях ежедневно растет и, соответственно, растет количество пользователей IoT-устройств. Не стоит сомневаться, что в ближайшие годы IoT основательно проникнет в наш быт, занимая новые ниши в повседневной жизни.

Людмила Сухоставец,
руководитель отдела маркетинга Rubetek

– Если говорить о технологиях, важным вопросом является создание "идеального" протокола передачи данных. Даже самые распространенные протоколы – Wi-Fi, Bluetooth, Z-wave, ZigBee – имеют как преимущества, так и недостатки. Рынок IoT в большинстве случаев сегодня представлен "локальными" решениями с ограниченной функциональностью.

Поэтому все ждут внедрения единого стандарта, который объединит элементы IoT в единую систему, что станет мощным толчком в развитии отрасли. Большие надежды производители возлагают на беспроводные технологии Bluetooth 5.0 и Wi-Fi HaLow, выход которых планируется в конце текущего года. А пока наиболее прогрессивные компании в сфере IoT используют сразу несколько протоколов, что позволяет создать открытую систему и объединить множество устройств.

– Какие вызовы сейчас стоят перед IoT?

Николай Сергеев,
генеральный директор ГК "РТЛ Сервис"

– В России сейчас отсутствует универсальная интеграционная платформа для применения IoT на промышленных предприятиях, что не позволяет объединить данные из различных IoT-систем и получать аналитику в общепринятом формате. Разработку в этом направлении ведет компания "Ростелеком", но еще рано говорить о промышленной эксплуатации создаваемой ей платформы.

Создание гибких аналитических систем для обработки данных, получаемых от различных IoT-систем, и подготовки типовых управленческих решений.

Удешевление стоимости систем IoT, в первую очередь стоимости внедрения их систем. В условиях сложной экономической ситуации компании не идут на внедрение дорогой системы без понятного экономического эффекта. Снижение стоимости даст толчок росту количества пилотных внедрений, что позволит получить данные об экономическом эффекте и может спровоцировать дальнейший рост количества установок IoT-систем.

Сейчас системы IoT содержат множество функций, без возможности их разделения на отдельные продукты или модули. Например, система содержит в себе контроль протечек, контроль открывания дверей, контроль температуры, влажности воздуха и управления климатическим оборудованием. А клиенту требуется только контроль протечек или только контроль открытия дверей. Предложение концепции модульности IoT-решений позволит клиентам постепенно наращивать их функционал, закрывая в первую очередь самые важные для него задачи.

Дмитрий Огородников,
директор центра компетенций по информационной безопасности компании "Техносерв"

– Одной из приоритетных задач IoT сегодня является обеспечение безопасности конечных пользователей. К концу 2020 г. необходимость закрывать уязвимости в IoT приведет к росту расходов на обеспечение их безопасности до 20% от годового бюджета на безопасность против менее 1% в 2015 г.

И в этом нет ничего удивительного. Требования современного бизнеса в первую очередь предъявляются к "красивой обертке" и скорости вывода продукта на рынок. При таком подходе очень часто страдает производительность и надежность новых продуктов, а про безопасность, как правило, просто забывают, реализуя какие-то базовые механизмы, либо сознательно оставляют ее "на потом". При этом "масла в огонь" добавляют зачастую отсутствующие процессы безопасной разработки программного обеспечения.

Согласитесь, крайне неприятно увидеть в Интернете запись происходящего в собственном доме или получить неожиданный продуктовый заказ из супермаркета от "взбесившегося" холодильника, или потерять страховку из-за зубной щетки, которая сообщила в страховую компанию, что вы не чистите зубы. Но, впрочем, все это покажется несущественным, когда к миру IoT станут подключаться роботы с возможностью изменять окружающие предметы и, хуже того, чем-либо управлять.

Такое положение "вещей" в первую очередь вызвано отсутствием общих стандартов, протоколов, архитектур этих систем и их взаимодействием. Беглый взгляд на документы RFC RFC 7452 (Architectural Considerations in Smart Object Networking)[1] и RFC 7397 (Report from

the Smart Object Security Workshop)[2] показывает, что основные принципы построения Интернета вещей только начинают разрабатываться, а многое находится на уровне определений и рекомендаций – "вы должны об этом подумать сами".

Вместе с тем подключение таких устройств, как сенсоры и особенно исполнительные механизмы (Actuator), несет в себе абсолютно новые риски, а именно риски некорректного управления объектами технологических процессов или жизнеобеспечения.

Если проанализировать большинство из известных атак на объекты АСУ ТП, мы придем к выводу, что почти все они были направлены на контроллеры PLC и изменение режима работы этих устройств. Но эти контроллеры не подключаются напрямую к сети Интернет, поэтому атакующие были вынуждены атаковать управляющие системы для последующего контроля конечных устройств PLC. Но Интернет вещей создается по принципу "все, что может подключаться, должно быть подключено", и именно к сети Интернет. При такой концепции без единых стандартов, как вы понимаете, риски возрастают многократно.

Андрей Рычков,
руководитель платежной системы "Центральная касса"

– Технологии необходимо удешевить и стандартизировать. Сейчас большинство решений очень дорогие. Но такой путь проходят многие инновации. Вспомните, поначалу ABS устанавливался только в автомобили премиальных марок. Теперь даже у недорогих моделей есть антиблокировочная система. По сути, ABS – это базовый стандарт автомобилей, как карандаш с ластиком наверху.

Причем скорость внедрения и распространения новых технологий будет увеличиваться. Если раньше на это требовались десятилетия, то теперь все намного быстрее.

Уверен, так будет и с Интернетом вещей. Если сейчас умные предметы приобретают только самые продвинутые, то с удешевлением технологий они будут все активнее появляться в наших домах.

Петр Травкин,
руководитель направления Big Data компании Hitachi Data Systems

– Возможность снизить затраты за счет прогнозирования поломок и своевременного обслуживания оборудования – одна из востребованных задач Интернета вещей. Особенно это будет крайне востребовано в условиях промышленного производства и добычи полезных ископаемых. Каждый из датчиков IoT, установленных на оборудовании, выполняет свою функцию: измеряет вибрацию, температуру (самого аппарата и помещения, в котором он находится), уровень света, шума и прочее. Эти данные обновляются несколько десятков раз в секунду. Будут ли эти технологии использоваться на нефтяных вышках, заводах, сборочных конвейерах или где-либо еще – для всех отраслей принцип получения прогнозной аналитики одинаков. Информационные системы "запоминают", при каких обстоятельствах совершилась предыдущая поломка: к примеру, когда уровень температуры окружающей среды и объекта различался более чем на пять градусов, – и когда в следующий раз температурные нормы подойдут к критической отметке, датчики предупредят специалистов о возможной неисправности. Немаловажно и то, что машины сами учатся предсказывать поломки: создают соответствующие алгоритмы на основе прецедентов или заложенных в программу данных.

Алексей Талаев,
руководитель департамента прогнозной аналитики и оптимизационного планирования ИТ-компании Navicon

– В России потенциал IoT раскроется в сфере решений для дистанционного мониторинга в промышленности. Здесь важно настроить системную работу с информацией (без аналитических инструментов бизнес способен эффективно использовать только 1% собираемых с датчиков данных) и наладить тесную интеграцию IoT с интеллектуальными инструментами аналитики (AI и Machine Learning), а также с облачными решениями вендоров.

Наконец, в России до сих пор не сформирована инфраструктура "Индустриального интернета". Сейчас в стране используется более 300 решений для передачи данных IoT, а сам сектор нормативно не регулируется. Нужно, во-первых, создать универсальную платформу и единый протокол IIoT, во-вторых – разработать единые стандарты и нормативные документы.

Владимир Ласовский,
менеджер по развитию бизнеса в области Интернета вещей Orange Business Services Россия и СНГ

– Основной вызов, который стоит сегодня перед развивающимся Интернетом вещей, – это безопасность умных устройств, которой пренебрегают многие пользователи. 90% ИБ-экспертов считают IoT главной угрозой безопасности в 2017 г. Устройств с доступом к сети появляется все больше, и каждое из них – потенциальная частичка разрастающихся ботнет-сетей. Основная опасность состоит в том, что ботнет-вирусы живут несколько лет и их крайне тяжело обнаружить. Самые громкие DDoS-атаки в 2016 г. связаны именно с Интернетом вещей. Источниками атак становятся многочисленные роутеры, камеры

[1] *https://tools.ietf.org/html/rfc7452.*
[2] *https://tools.ietf.org/html/rfc7397.*

и видеорегистраторы. При этом один час простоя обходится компаниям в $40 тыс. Средняя атака длится 6–24 часа, убытки доходят до $500 тыс.

Другой вызов – разрозненность существующих IoT-проектов и отсутствие универсальных стандартов взаимодействия датчиков между собой и с внешней средой. Наконец, еще одна проблема – необходимость модернизации магистральных ВОЛС в связи с появлением все большего количества проектов в сфере Интернета вещей.

– Каковы, на ваш взгляд, приоритетные задачи для развития в России рынка Интернета вещей?

Екатерина Медведева,
специалист по стратегическому маркетингу, АстроСофт

– Для развития в России приоритетных направлений Интернета вещей – умного города и промышленного Интернета вещей – необходима инфраструктура. Ее развитием на базе имеющихся ресурсов могут заниматься операторы сотовой связи и крупные телекоммуникационные компании, например "Ростелеком". Такая задача подтягивает за собой еще один важнейший вопрос – обеспечение ее безопасности. В данном контексте отечественное программное обеспечение становится ключевым элементом системы безопасности. Во-первых, это обеспечивает независимость национальной технологической базы, а во-вторых, зарубежное ПО все еще остается уязвимым для кибератак. Одна из крупнейших кибератак произошла осенью 2016 г., когда заражение IoT-устройств стало причиной мощной DDoS-атаки на DNS-провайдера Dyn. В результате атаки нарушилась работа интернет-сервисов на всем Восточном побережье США, работа клиентов провайдера Dyn оказалась парализована. Уже можно наблюдать увеличение активности отечественных разработчиков ПО, недавно активно освещалась в прессе инновационная российская разработка операционной системы реального времени ОСРВ МАКС. Форсировать этот позитивный тренд могла бы поддержка отечественных разработчиков и создание базы для обмена знаниями и технологиями на национальном уровне.

Павел Новиков,
руководитель группы исследований безопасности телекоммуникационных систем Positive Technologies

– Мы переступили порог взрывного роста использования устройств IoT. В ближайшие годы прогнозируется многократный рост количества этих устройств, но что еще важнее – они будут вовлечены во многие "слабо информатизированные" области жизнедеятельности и бизнеса, в том числе затрагивающие обработку критической информации: информацию о здоровье, платежные операции, информацию о местоположении, физическую безопасность и безопасность человеческой жизни. В связи с этим приоритетная задача производителей IoT-решений – повышение защищенности этих устройств, учитывая аспекты информационной безопасности как при разработке, так и при внедрении элементов IoT-решений.

Борис Труш,
директор компании ООО "Единые Электронные Системы"

– На данный момент расширение и модернизация систем безопасности в городах России является приоритетным шагом к развитию IoT-технологий. Уже существует множество технологий, которые позволят сделать более безопасными улицы города. В прошлом году было множество споров о рентабельности вложения средств в системы безопасности с Интернетом вещей. На мировом рынке IoT расширяется не только благодаря потребительскому спросу на гаджеты, но и благодаря государственным программам безопасности, увеличению числа камер слежения, датчиков и терминалов, способных собирать и анализировать данные. Это дает надежду на то, что электронная промышленность будет набирать обороты, чтобы наполнять проекты современными устройствами, способными видеть, слышать, запоминать.

Яков Гродзенский,
руководитель направления информационной безопасности компании "Системный софт"

– Одной из основных задач для развития IoT в России остается решение проблем информационной безопасности. Дело в том, что главными векторами развития Интернета вещей в нашей стране будет не потребительская электроника, а промышленность, энергетика и сельское хозяйство – отрасли, в которых применение IoT-решений даст реальный прирост производительности труда и ресурс для усиления конкурентоспособности экономики. В промышленном Интернете вещей риски взлома существенно выше: одна атака может стоить компании миллионы и даже миллиарды рублей, поэтому без отлаженных механизмов защиты не обойтись. Другие задачи – развитие экосистемы Интернета вещей, создание законодательной базы со стороны государства и поиск инвестиций для пилотных IoT-проектов.

Андрей Рычков,
руководитель платежной системы "Центральная касса"

– В первую очередь на данном этапе для рынка Интернета вещей в России важна пропаганда. Сейчас у людей не сформировалось видение необходимости применения IoT-решений.

Один из самых простых примеров – счетчик электричества или воды, который сам передает показания электроснабжающей организации. У человека одной заботой меньше, ему уже не нужно держать в голове, что каждый месяц надо показания записывать и отправлять. Одновременно с этим такой

счетчик повышает точность передачи показаний. Но люди не побежали стройными рядами менять установленные у них счетчики. Потому что нет окончательного понимания полезности такого решения и конечной ценности. Люди должны понимать, что конкретная проблема решается и для них это не накладно, просто и понятно.

Илья Апполонов,
руководитель по развитию направления IoT компании ICL Services

– Следует прежде всего разделить все решения в области IoT на два сегмента: потребительский Интернет вещей и индустриальный Интернет вещей. По факту это две совершенно разные области, и их нужно рассматривать отдельно.

Если говорить о задачах для развития рынка, то они разнятся для этих сегментов. Для потребительского сегмента решающими факторами является доступность и стоимость решений (как программной части, так и самих устройств). Учитывая, что подавляющее большинство IoT-решений предлагаются зарубежными брендами, на оба фактора можно повлиять, налаживая официальные дистрибьюторские каналы поставок решений в нашу страну. Чем больший масштаб поставок будет достигаться, тем дешевле и доступнее будут решения. Если говорить о таком факторе, как спрос, то здесь СМИ играют свою роль уже сейчас, подогревая интерес аудитории с помощью огромного количества статей, видео, описаний реальных примеров использования и т.д.

В индустриальном Интернете вещей задачи несколько иные. В данном сегменте приживаются только решения, которые способны хотя бы на момент защиты бизнес-кейса показать потенциал значительного снижения расходов для внедряющей компании либо значительного повышения выручки. Данный аспект обуславливает намного более вдумчивый выбор IoT-решений и их оценку, при этом стоимость самого решения играет не столь значимую роль, а доступность вообще не является ограничивающим фактором.

Для приобретения и внедрения индустриального IoT-решения бизнесу нужно четкое понимание выгод в сравнении со стоимостью. Как показывают маркетинговые исследования, даже западный рынок IoT-решений не обладает таким уровнем зрелости, при котором заказчик сам может оценить свои слабые места в текущей деятельности и связать их усиление с внедрением IoT-решения, т.е. никто не придет к вам как интегратору и не скажет: "Мне нужно IoT-решение, чтобы снизить затраты на техподдержку и убытки от простоя оборудования". Инициатива предложения такого рода решений на рынке индустриального Интернета вещей должна быть исключительно со стороны интеграторов, которые должны обладать опытом решения задач бизнеса через внедрение IoT-решений. На данный момент опытом внедрения полномасштабных индустриальных IoT-решений обладают единицы.

Таким образом, задачами для развития российского рынка индустриальных IoT- решений является обучение и повышение уровня зрелости как интеграторов, так и заказчиков в лице компаний. Интеграторам, конечно, следует начать с работы с текущими заказчиками и попробовать взглянуть на их текущие задачи и проблемы с точки зрения провайдера IoT-решений, а заказчикам, в свою очередь, научиться выстраивать свои стратегии с учетом технологий IoT. При возникновении такой общей "понятийной платформы" между провайдерами и заказчиками рынок индустриального IoT начнет развиваться намного динамичнее.

Павел Новиков,
руководитель группы исследований безопасности телекоммуникационных систем Positive Technologies

– Помимо умного дома активное развитие получили решения класса умный город, при этом зачастую горожане не замечают этих изменений. Они уже применяются для регулировки светофоров, городского освещения, информационных табло, в камерах фиксации дорожно-транспортных нарушений. Также IoT получил распространение в области сельского хозяйства, промышленности и т.д. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru