«Вавилонская башня» Интернета вещей

Игорь КИРИЛЛОВ

Концепция Internet of Things активно обсуждается в ИТ-сообществе последние несколько лет. Однако до сих пор в отрасли нет единой точки зрения относительно того, что же это, собственно, такое. Каждый производитель, ратующий за внедрение IoT, имеет на сей счет собственную точку зрения.

Изначально Интернет был сетью взаимодействия между людьми посредством компьютеров. По крайней мере до 1990 года это было именно так, а потом, как говорят, некий Джон Ромки (один из разработчиков TCP/IP) подключил к этой глобальной сети тостер. Сам того не подозревая, инженер стал идейным вдохновителем нового направления в ИТ, которое через девять лет получило название «Интернета вещей». Еще через примерно такой же промежуток времени — в 2009 году — оказалось, что число устройств, подключенных к Интернету, превысило показатель населения планеты, не говоря уже про число одушевленных пользователей Сети. С тех пор этот разрыв только увеличивается, а человечество начало всерьез задумываться о том, как извлечь максимальную пользу из всего этого «зоопарка», а главное, не выпустить его из-под контроля.

Бешеные деньги

Прогнозы развития рынка IoT поражают воображение. Так, по данным Cisco, уже в прошлом году к Сети было подключено 25 млрд устройств, а к 2020 году их количество удвоится (правда, IMS Research говорит «лишь» о 22 млрд к тому же сроку). Такая разница в оценках, скорее всего, свидетельствует о различной методике подсчета устройств и определения того, что же такое IoT. Строго говоря, ПК, смартфоны и планшеты, формирующие сегодня львиную долю рынка во всех отчетах о рынке IoT, к этому понятию не относятся, потому что управляются человеком, представляя собой лишь интерфейс для «Интернета людей».

В то же время технологии сугубо межмашинного взаимодействия были известны и успешно применялись уже много лет назад под общим названием M2M (machine to machine). По идее, концепция IoT должна не только объединить оба эти подхода («Интернет машин» и «Интернет людей»), но и вывести их на новый глобальный уровень взаимодействия и возможностей. Идея Internet of Things охватывает все сферы современной жизни — быт, образование, бизнес, медицину, транспорт, промышленность, экологию и т.д. Список можно продолжать практически до бесконечности. Неудивительно, что говоря о рынке IoT, в будущем аналитические компании оперируют триллионными суммами. Так, по данным IDC, расходы в области Internet of Things в 2020 году составят более $7 трлн. Как заявил на одной из конференций в 2013 году тогда еще генеральный директор Cisco ***Джон Чемберс***: *«Интернет вещей» станет крупнейшей составной частью ИТ-рынка в ближайшие 10 лет, реализация этой концепции принесет $14 трлн выручки»*.

Куда идет IoT?

Несмотря на явный прорывной характер, «Интернет вещей» — это вовсе не революция в ИТ-сфере. Скорее, это логичный эволюционный шаг в условиях накопив-

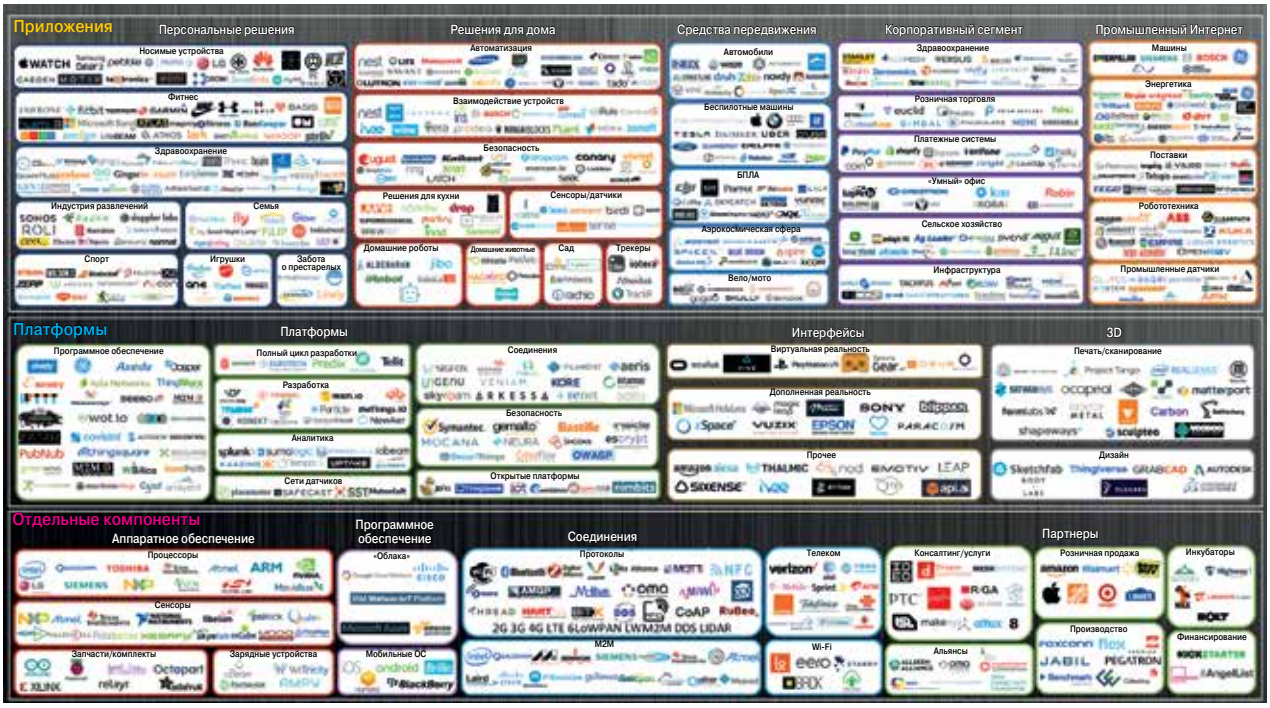

Рис. 1. Мировая «экосистема» IoT по версии mattturck.com (март 2016 года)

шейся критической массы технологий. Отдельные составляющие IoT сосуществовали бок о бок много лет, но лишь в конце первого десятилетия нового века стало понятно, что все это богатство можно собрать воедино для получения синергетического эффекта.

Благодаря чему это стало возможно? Здесь сыграли свою роль несколько факторов. Во-первых, удешевление электронных компонентов, особенно различных датчиков и микроконтроллеров, цены на которые за последние несколько лет снизились в десятки раз. Второй момент — развитие «облачных» технологий (как программных, так и аппаратных составляющих), с помощью которых участники «Интернета вещей» могут эффективно взаимодействовать между собой. Но главное — данные, полученные с отдельных устройств, могут эффективно обрабатываться, анализироваться для получения качественно новой информации. Третий момент, необходимый для развития IoT — это, конечно же, повсеместное распространение сетей широкополосной радиосвязи (Wi-Fi, 3G, LTE, LTA Advanced и т.д.), которых в мире появляется все больше с каждым годом. Без них «Интернет вещей» был бы обречен на «нишевость» и крайне медленное развитие. Есть и другие факторы (например, появление и развитие т.н. программно-конфигурируемых сетей, SDN), но эти три, по нашему мнению, являются определяющими.

Поскольку терминология в отрасли еще не устоялась, сегодня можно встретить разные определения не только для самой концепции IoT, но и различные точки зрения на то, какие основные сферы она охватывает. Наиболее показательным нам видится разделение, предложенное Harward Business Review, в рамках которого развитие «Интернета вещей» идет в пяти разных направлениях (**рис. 1**):

- носимые устройства (Connected Wearables);
- «умный» дом (Connected Homes);
- подключенные автомобили (Connected Cars);
- «умный» город (Connected City);
- промышленный Интернет (Industrial Internet)

Наибольшие деньги сегодня вкладываются в первые три. О характере развития технологий и спроса на них могут рассказать крупные приобретения компаний на рынке, которые состоялись в последнее время. Например, производитель спортивной экипировки Under Armour (США) приобрел две компании Endomondo и MyFitnessPal за $560 млн. Google заплатил $3,2 млрд за Nest Labs, которая разрабатывает отдельные элементы решений для «умного» дома. British Gas купил сервис мониторинга домашнего энергопотребления AlertMe за $100 млн. Производитель автомобильных шин Continental выложил почти $700 млн за компанию Electrobit (ПО и другие разработки для подключенных автомобилей). Список можно продолжать очень долго — число таких сделок растет. Особенно перспективны носимые устройства, поскольку, благодаря датчикам телеметрии, они непосредственно затрагивают такие огромные рынки, как медицина и массовый спорт.

Очень популярной в последнее время стала идея автомобилей, подключенных к Сети. Где-то рядом и «умный» городской транспорт. Что касается промышленного Интернета, то здесь IoT является логичным эволюционным шагом в сфере автоматизации производства. В области энергетики «Интернет вещей» воплотился в виде «умных» энергосетей (т.н. Smart Grid). Также развивается концепция и в области сельского хозяйства.

Похоже на то, что возможности «Интернета вещей» ограничены лишь нашей фантазией, потенциал этой перспективной концепции и связанных с ней технологий будет раскрываться в течение многих лет. Мы только в начале большого пути, но даже на этом этапе реальные возможности IoT впечатляют (на эту тему написано уже немало восторженных статей). Но задача нашей

публикации не столько в популяризации IoT, сколько в критической и объективной оценке данной концепции, попытка которой дана в дальнейших разделах. Начнем с хорошего — с реализованных проектов.

IoT — в массы. Опыт мировых проектов

Хотя «Интернет вещей» воспринимается сегодня у нас в стране как некая футуристическая идея, в мире появляется все больше проектов IoT. Многое проходит незаметно, поскольку рост числа внедрений не носит явного «взрывного» характера — это скорее эволюционный процесс, который начинается с индустриальных предприятий, а затем переходит и в другие сферы экономики.

Например, знаменитый бренд Harley Davidson автоматизировал свое производство, используя решения компании ***SAP***. По этому же пути пошел и порт города Гамбург, где с помощью решений для «Интернета вещей» было организовано управление большим логистическим хабом.

Похожие решения имеются и в транспортной отрасли. Один из наиболее интересных проектов реализован для итальянской железнодорожной компании TrenItalia. Датчики, установленные на эксплуатируемых составах, позволяют компании непрерывно отслеживать состояние технологического оборудования, прогнозировать потребность в ремонтных работах и оперативно оповещать диспетчеров о необходимости замены того или иного элемента. Как ожидается, такой подход позволит транспортной компании сэкономить в будущем 8–10% на техническом обслуживании.

В сельскохозяйственной отрасли интересным примером использования IoT является т.н. «умный трактор», который обрабатывает почву с учетом ее химического состава и особенностей каждого участка. С размещенных в почве датчиков он собирает данные о температуре, влажности, содержании тех или иных микроэлементов, а затем передает для обработки в «облачную» платформу. Выявив в результате анализа недостаток удобрений на каком-то участке, система инициирует их дозаказ и закупку у поставщика, доставку (с помощью логистической компании) и последующие действия, вплоть до внесения удобрений в почву на конкретном участке поля.

Есть примеры и в энергетической отрасли. Так, компания Alliander (Нидерланды) в режиме реального времени получает информацию с датчиков и следит за уровнем потребления энергии как в крупных компаниях (заводы и фабрики), так и среди частных потребителей. Одна из важнейших задач — мониторинг объемов энергопотребления и моделирование поведения энергосети, которое поможет выявить слабые места, запланировать ремонт или модернизацию. В качестве платформы здесь используется SAP HANA.

Рис. 2. Датчики системы Invisible Tracck, устанавливаемые на деревьях, помогают защитить дождевые леса Бразилии от неконтролируемой вырубки

«Интернет вещей» также является неотъемлемой составляющей концепции «Умный город». Например, уже сейчас в Нью-Йорке с помощью специальных датчиков контролируется система вывоза мусора, а в Бостоне каждый водитель, использующий специальное мобильное приложение, может сообщить о неисправности дорожного полотна или аварии, тем самым помогая городским службам оперативно на них реагировать.

Активно используется IoT в энергетической и авиационной отрасли. Это позволяет вывести бизнес компаний на совершено новый уровень. Так, например, Rolls-Royce теперь предлагает клиентам свои знаменитые авиационные двигатели в аренду. При этом оплачивается не само устройство, а определенное количество часов эксплуатации. Поставщик гарантирует работоспособность двигателей в течение оплаченного времени. Для того чтобы это стало возможным, на каждом двигателе установлено множество датчиков IoT, отслеживающих состояние устройства в реальном времени. Собранные данные анализируются и на их основе принимаются решения о ресурсе двигателя или необходимости сервисного обслуживания. Подобную схему предлагает и Boeing для некоторых моделей своих самолетов, а также General Electric для мощного электрогенерирующего оборудования.

О возможностях, которые открывают технологии IoT для оборонного сектора, можно, наверное, написать не одну книгу. Отметим лишь, что отдельные элементы концепции активно используются, например, ВМС США для построения систем освещения подводной обстановки (СОПО), основной целью которых является обнаружение подводных лодок неприятеля в заданных районах. Концепция развивается примерно с 90-х годов прошлого столетия, а первые сведения о ее реальном применении приходятся на первые годы XXI века. Суть метода заключается в построении сети мощных излучателей и приемопередающих устройств с антеннами (которые могут устанавливаться на кораблях, подлодках, автономных буях, да и просто на морском дне). Благодаря современным системам связи, в т.ч. спутниковым каналам, вся эта структура работает как одно гидролокационное устройство с большой эффективной площадью покрытия. Собранные данные передаются в центральный командный пункт в режиме реального времени. Как считается, такой подход позволяет обнаружить любую, даже самую малошумную, атомную подлодку. Кардинальным отличием СОПО от более ранних проектов, например SOSUS (стационарная гидроакустическая сеть ВМС США, действовавшая во времена холодной войны), является возможность развертывания системы «по требованию» — в нужный момент и только в необходимом районе, причем штатными ресурсами.

Но IoT — это не только промышленность или оборона; подобные решения могут помочь в решении и более глобальных вопросов, например экологического характера. Так, проект Invisible Tracck (в названии нет ошибки) предлагает защищать дождевые леса Бразилии с помощью сети автономных миниатюрных датчиков (**рис. 2**), устанавливаемых на деревьях в охраняемых природных зонах.

В случае фиксации незаконной вырубки леса природоохранным подразделениям автоматически отправляется сигнал тревоги с указанием точных координат инцидента. Правда, параллельно с установкой этих устройств приходится организовывать и территориальную сеть радиосвязи, но, как говорят разработчики, цель в данном случае оправдывает затраченные усилия — с помощью Invisible Tracck удалось существенно сократить объемы незаконной вырубки лесов.

Более локальный пример. В американском Бостоне работает проект BigBelly, представляющий собой не что иное, как сеть мусорных баков, каждый из которых оснащен датчиками, прессом для отходов и солнечными батареями. Такие урны самостоятельно анализируют степень своего заполнения и передают сведения в обслуживающую компанию, которая, в свою очередь, может планировать оптимальные маршруты мусороуборочной техники. В результате такого подхода оказалось, что во многих местах города отходы можно забирать в несколько раз реже (поскольку баки там наполняются значительно медленнее, чем предполагает план).

Нерешенные [пока] проблемы

О том, почему «Интернет вещей» — это хорошо, мы поговорили, но на обратной стороне новой перспективной концепции скрывается еще много нерешенных вопросов. Казалось бы, если IoT — это так здорово, почему мы все еще не живем в окружении «умных» вещей и даже не приближаемся к этому идиллическому автоматизированному миру? Большинство экспертов сходятся во мнении, что за «Интернетом вещей» будущее, но каким оно будет — все еще неясно, скорее всего, не таким, как нам видится на данный момент.

Одной из ключевых и, в общем-то, самой безобидной из потенциальных проблем является необходимость перехода на протокол IPv6, ведь свободные адреса IPv4 закончились еще в феврале 2010 года. Хотя, конечно, благодаря ухищрениям Интернет-провайдеров пользователи не ощутили дефицита, но с IoT так не получится — повсеместное внедрение IPv6 с его почти неограниченным количеством возможных адресов является обязательным условием, учитывая то, что число устройств, подключаемых к Сети, будет исчисляться десятками миллиардов.

Вроде бы и проблемы тут никакой нет — надо взять и перейти. Но, как показала практика традиционного Интернета, за почти семь лет после распределения последнего свободного пула адресов IPv4 переход на новую версию протокола все еще происходит очень медленно — его доля в общей структуре мирового трафика в 2015 году, по различным оценкам, составляла немногим более 10% (по 2016 году данных нет, но даже если сегмент вырос до 15% или 20%, это все равно довольно скромный результат).

Но если насчет необходимости поддержки IPv6 все производители солидарны, то вот касательно других важных протоколов взаимодействия пока единства нет. Попытка объединить «все» на базе концепции Internet of Things пока что не имеет внятного решения. Ведь различные составляющие концепции пришли с очень разных рынков, каждый из которых развивался по своему пути. Например, в области бытовой электроники разрабатывались собственные стандарты и подходы, которые принципиально несовместимы, например, со средствами промышленной автоматизации. Транспорт, торговля, медицина, телекоммуникации, системы безопасности и т.д. — все это «отдельные миры» со своими законами и правилами, которые для надлежащего использования IoT теперь предстоит привести к общему знаменателю. Необходимо также включить в «Интернет вещей» огромное количество «старых» устройств. Эта проблема характерна, в частности, для промышленной автоматизации, где имеется огромный массив контроллеров и датчиков, установленных десятилетия назад. Менять их, естественно, никто просто так не будет — это огромные затраты, а значит, нужны технологии и протоколы, способные сопрячь устройства предыдущих поколений с новыми системами.

Более того, каждый крупный производитель естественно стремится развивать (и, по возможности, навязывать другим) собственные технические подходы и стандарты к реализации «Интернета вещей», ведь кто владеет стандартами — владеет миром. Борьба подходов вполне естественна, учитывая, какую потенциальную выгоду несет рынок IoT в будущем. Но в то же время сейчас ни одна компания не способна стать технологическим монополистом, а значит, необходимы альянсы, и они создаются.

Одним из наиболее известных объединений такого рода сегодня является Open Connectivity Foundation — организация, объединяющая более 150 компаний, в числе которых ***Dell***, ***Intel***, ***Samsung***, ***Microsoft***, ***Cisco***, ***Intel***, ***Samsung***, ***IBM***, ***Dell***, ***Qualcomm*** и другие. Есть целый ряд отраслевых альянсов. Например, Thread Group (Qualcomm, ARM, Samsung, Osram и другие) создана для выработки протоколов совместной работы устройств «умного» дома. Объединение Industrial Internet Consortium (AT&T, GE, IBM, Intel, всего более 200 компаний) создано с целью скорейшего внедрения IoT в промышленности. Группа oneM2M занята выработкой универсальных алгоритмов межмашинного взаимодействия. Open Automotive Alliance (Honda, Hyundai Motor, Audi и др.) разрабатывает платформу для «умных» автомобилей на базе ОС Android.

На подобные альянсы возлагаются большие надежды, но смогут ли компании прийти к единому мнению и цивилизованно поделить рынок — покажет время. Добавьте сюда еще неизбежные патентные войны. Если борьба «всего лишь» за рынок смартфонов выливается в сложные судебные разбирательства и мультимиллиардные иски, представьте, какие ресурсы будут задействованы в борьбе за сегмент, исчисляемый триллионами долларов. Кстати, по данным исследования компании Lexinnova, в 2015 году наибольшим числом патентов в области IoT обладала LG (641 изобретение), на втором месте — Qualcomm (590), далее идут Ericsson (541),

IBM (438) и Nokia (367). Компании Microsoft, Cisco, Samsung, Intel владеют правами примерно на 200–255 патентов каждая. Так что, похоже, главная борьба за рынок еще впереди.

И это далеко не все вопросы. Мировые апологеты IoT в основном еще не определились даже на понятийном поле — каждая компания вкладывает в термин собственный смысл. Например, для ***Intel*** — это, в первую очередь, единая экосистема процессоров, интегральных схем, микроконтроллеров и других устройств, имеющих отношение к вычислительной системе. Для ***Google*** и ***Apple*** IoT значит управление пользовательскими устройствами и средствами развлечения. ***Microsoft*** предлагает использовать свои разработки для дома и бизнеса. ***Cisco*** и ***IBM*** рассматривают концепцию более широко — вплоть до «умного города» и даже «умной планеты». ***SAP*** и ***General Electric*** специализируются на промышленной автоматизации. И так в каждой отрасли. Поэтому глобальный «Интернет вещей» пока что остается умозрительной концепцией.

В то же время над выработкой общей точки зрения трудятся известные мировые некоммерческие объединения. Важную роль здесь играют Международный союз электросвязи (МСЭ, ITU), Международная электротехническая комиссия (МЭК, IEC), ISO, над общими стандартами для отрасли активно трудится и специальная комиссия IEEE, но работы ей, похоже, еще не на один год.

Третий важный момент, сдерживающий распространение «Интернета вещей», — электропитание. Экосистема IoT предполагает большое количество маломощных устройств, например, контроллеров и датчиков, которым все равно необходимо электричество. Как обеспечить его повсеместный доступ? Снабдить каждое изделие небольшим аккумулятором? А как перезарядить сотни, тысячи, миллионы таких батарей? Да к тому же аккумулятор накладывает ограничения на размеры устройства.

Проблема также имеет решение, но здесь все сложнее, чем в случае IPv6. Ответом является создание микроскопических генераторов, способных вырабатывать электричество из окружающей среды — тепла, ветра, электромагнитного поля. Решения такого типа уже есть, в 2011 году сотрудники Технологического института штата Джорджия представили генератор, вырабатывающий электроэнергию от малейших движений человеческого тела. Технологию назвали «прорывом», но, как показывает практика, от создания технологии в научном мире до ее повсеместного признания и коммерческого внедрения обычно проходят годы, если не десятилетия. Да и не все IoT-устройства можно прицепить к человеку — есть целый класс систем, которые должны работать автономно, условно говоря, «в чистом поле». Похоже, в этом направлении предстоит сделать еще немало открытий.

Есть и более локальные вопросы, которых тоже сегодня немало. Например, популярная нынче идея «умных» или даже беспилотных автомобилей часто, так сказать, разбивается о быт. Например, Volvo активно продвигает идею машин, подключенных к Интернету, но как отметил Ян Вассен, директор компании по бизнес-аналитике, только каждый десятый автомобиль производителя действительно подключен к беспроводной Сети. Как оказалось, пользователей беспокоят не только вопросы безопасности данных, передаваемых в радиоэфире, но и банальная устойчивость связи, а также карта покрытия операторов. Роуминг пока что стоит дорого, даже в ЕС, и простая поездка за границу на IoT-машине может вылиться в серьезную сумму только на оплату мобильного доступа в Интернет. Это, конечно же, не самая большая проблема. Но она позволяет лучше понять ограничения, связанные с развитием «Интернета вещей» на массовом рынке, где общая экосистема электронных устройств во многих случаях еще не готова к восприятию новой концепции.

Вас атакует... унитаз

А вот теперь мы подошли к самому главному моменту — вопросам безопасности. Потенциальное проникновение IoT во все аспекты человеческой жизни не на шутку всполошило специалистов по безопасности. Ведь если некий злоумышленник получит доступ к сети вещей, то теоретически он сможет добраться до огромного массива важной личной или секретной информации, а в худшем случае — получить доступ к экосистеме «умных» устройств. IoT — это в первую очередь Интернет, со всеми его недостатками в области безопасности и сохранности данных.

Уже сейчас «умные» устройства серьезно вредят бизнесу. Последнее веяние — на базе таких изделий хакеры формируют огромные бот-сети, которые участвуют в невиданных доселе DDoS-атаках. Причем нападение осуществляют зараженные принтеры, домашние маршрутизаторы, IP-камеры, различные датчики, даже т.н. smart-телевизоры и холодильники. Так, в сентябре 2016 года была зарегистрирована DDoS-атака интенсивностью 700 Гбит/с, в которой принимало участие свыше миллиона IoT-устройств. Такие атаки однозначно будут повторяться и набирать силу.

Но эта угроза касается в основном бизнеса, а ведь IoT может принести опасность буквально в каждый дом. Так, в феврале 2016 года группа специалистов компании Panasonic, тестирующая различные устройства на предмет информационной безопасности, смогла взломать... «умный» унитаз в одном из мест общественного пользования. Ничего опасного хакерам сделать, естественно, не удалось, но они развлекались тем, что внезапно спускали воду и пугали посетителей. С одной стороны, смешно, но с другой — атаке могут подвергнуться и более важные системы, например, злоумышленники могут заблокировать электронные замки по всему дому и требовать выкуп за их открытие, спровоцировать ложное срабатывание сигнализаций, могут даже устроить пожар, используя уязвимости в мощных электроприборах. В Интернете можно уже найти видеоролики, где хакеры получают несанкционированный доступ к системам управления «умного» автомобиля. Список угроз столь же обширен, как и возможности IoT.

При этом под угрозу попадают главным образом простые пользователи — риск получения доступа к устройствам и данным на предприятиях также велик, но там хотя бы есть собственная служба ИТ-безопасности, в отличие от домохозяйств. Эта проблема тоже решаема, но сегодня именно она

«Интернет вещей» — это и настоящее, и будущее

«Интернет вещей» (IoT) – это концепция, объединяющая различные устройства и оборудование с людьми в единую коммуникационную систему. Технологии «Интернета вещей» позволяют считывать и анализировать огромные объемы информации, собирать их воедино со множества подключенных устройств, будь это станки на производстве или бытовая техника в квартире. Если говорить о сегментах рынка, которые получают наиболее ощутимую выгоду от технологий IoT, – это розничная торговля, транспортный и сырьевой секторы, металлургия, энергетика, медицина, сельское хозяйство. Но список постоянно расширяется.

В Украине компании только присматриваются к данной концепции. На наш взгляд, это связано с общим уровнем цифрового развития украинских предприятий – многие компании еще не накопили достаточного количества взаимодействующих друг с другом устройств (датчиков), не прошли этап автоматизации ключевых бизнес-процессов. Соответственно, они еще не готовы к следующему шагу – применению IoT. Для многих наших компаний эта концепция представляется чем-то футуристическим.

Но в мире это уже реальность. Например, SAP обладает полным набором компетенций и продуктов для создания промышленных приложений «Интернета вещей» (опыт, платформа, готовые решения). Мы работаем в сфере «Больших данных» (Big Data), создаем новейшие алгоритмы для прогнозных моделей, занимаемся вопросами машинного обучения и искусственного интеллекта. Центральным решением для развития концепции «Интернета вещей» для нас является SAP HANA Cloud Platform. Несколько месяцев назад наша компания официально объявила о том, что намерена вложить 2 млрд евро в процесс ускорения развития IoT по всему миру, в том числе в СНГ.

Мы согласны с экспертами, которые прогнозируют, что большая часть рынка IoT в будущем придется именно на индустриальный «Интернет вещей». Также усилится тенденция по предоставлению услуг, а не просто оборудования.

Но для развития IoT в мире усилий одной компании мало, поэтому мы и продвигаем соответствующую экосистему в этом направлении, сотрудничая с партнерами, разработчиками, стартапами. На текущий момент IoT – один из наиболее важных глобальных трендов и очень перспективное направление развития нашего бизнеса.

Тем не менее, по мере того как технологии IoT завоевывают новые рынки, эксперты замечают и выделяют несколько ключевых недостатков, над которыми специалистам в данной области еще предстоит работать. Наиболее остро сейчас стоит вопрос безопасности и сохранности персональных данных. Промышленные предприятия очень волнуют сроки внедрения проектов IoT. Еще одна проблема, на которую обращают внимание специалисты, – отсутствие единых стандартов в сфере «Интернета вещей». Кроме того, руководители компаний отмечают высокую стоимость технологий как одно из препятствий к внедрению.

Но все эти проблемы постепенно разрешатся. Так, для того чтобы избежать проблем с безопасностью данных, можно использовать IoT-платформу, где вопросы сохранности данных учтены опционально в виде готовых сервисов. Если говорить о сроках внедрения, отмечу, что для IoT они не слишком отличаются от процесса проведения комплексной автоматизации предприятия. Использование существующих методологий и грамотное управление позволяет кардинальным образом снизить риски проекта, выполнить его в четко поставленные сроки и обеспечить полную безопасность и непрерывность бизнес-процессов организации. Над разработкой единых стандартов сейчас по всему миру работают множество организаций, в т.ч. на государственном уровне, а что касается стоимости технологий, то можно с уверенностью сказать, что по мере развития концепции она будет снижаться. Уже сейчас можно проследить, как изменилась цена на многофункциональные сенсоры. За последние пять лет она сократилась в сорок раз – с $20 до $0,5.

Максим МАТЯШ,
директор SAP по странам СНГ

вызывает наибольшие опасения как разработчиков, так и потенциальных пользователей. А вот компании, специализирующиеся на кибербезопасности, уже потирают руки — им откроется огромное поле для деятельности.

По предположению Gartner, к 2020 году с помощью IoT будут совершаться до четверти всех кибератак на бизнес, при этом на защиту от них компании будут выделять до 10% своего ИТ-бюджета. Для понимания масштаба в конкретных цифрах, упомянем, что тот же Gartner предполагает, что уже в 2018 году на защиту систем «Интернета вещей» во всем мире будет потрачено почти $550 млн.

Вопрос несанкционированного доступа к инфраструктуре IoT настолько серьезный, что 11 октября Еврокомиссия заявила о планах ввести в ближайшее время обязательную сертификацию для устройств, подключаемых к IoT; с подобными инициативами выступают многие страны. Но конкретный механизм реализации идеи неясен (похоже, даже самим инициаторам). Более того, в мире отмечается острый дефицит профильных специалистов по всем ключевым аспектам IoT, а это существенно замедляет как сам процесс распространения технологии, так и принятие решений относительно ее безопасности.

«Интернет вещей» постепенно входит в жизнь современного человека, хотим мы того или нет. Конечно, здесь еще много нерешенных проблем, но это, как говорится, «болезни роста», которые, очевидно, удастся преодолеть в ближайшие годы. Глобализация экономики и стремление крупных производителей скорее поделить рыночный пирог выступят здесь в качестве катализаторов процесса. Нам же, как потенциальным и действующим пользователям, остается надеяться, что IoT сделает нашу жизнь еще лучше, ну или, как минимум, не навредит.

Игорь КИРИЛЛОВ, СиБ