

# Интернет вещей: технологии и проекты

**Владимир Тен (Москва)**

На состоявшейся в конце ноября конференции «Интернет вещей: технологии и проекты» обсуждалось всё то новое, что появилось в этой сфере за прошедшие полгода.

В состоявшейся 30 ноября в Москве конференции «Интернет вещей: технологии и проекты» приняли участие видные российские разработчики и производители электроники, руководители предприятий, менеджеры проектов, руководители отделов и направлений – всего около 80 специалистов и экспертов. И им было, о чём поговорить, ведь изменения в Интернете вещей происходят с фантастической скоростью. А это значит, что в развитии этого сегмента сосредоточено значительное число ведущих разработчиков и производителей.

Программа конференции подразумевала различные тематические направления – от концепций до технологий и реальных проектов.

## Влияние на экономику, промышленность, рынки

В своём докладе «Интернет вещей: технологические сдвиги, проекты и направления развития, место и роль в экономике России» директор по стратегическим проектам, Json & Partners Consulting Михаил Шеховцов попытался систематизировать причины и следствия появления такого понятия, как Интернет вещей.

«На каждом витке технологических и социальных циклов происходит раз-

рыв между поколениями, технологиями и методами, – считает Шеховцов. – Нынешний виток цивилизации вызвал к жизни Интернет вещей, роботов, нейронные сети, искусственный интеллект, игровые технологии и виртуальную реальность, 3D-принтеры, альтернативную энергетику (солнце, ветер, термоядерный синтез, др.), композитные материалы, нанотехнологии, биотехнологии, распределённую финансовую систему, освоение космоса – вот факторы очередного разрыва».

По мнению Михаила Шеховцова, последствиями текущего технологического сдвига станут горизонтальная и вертикальная связность: сквозные процессы электронного управления (Product Lifecycle Management, PLM), электронное проектирование и сквозное электронное управление всем процессом (от заказа до эксплуатации и утилизации).

Собственно Интернет вещей превращается в систему объединённых компьютерных сетей и подключённых физических объектов (вещей) со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удалённого контроля и управления в автоматизированном режиме, без участия человека. По сути, с развитием

IoT мир превращается в единый компьютер (или единую систему распределённых компьютеров).

«Мы будем жить в едином информационном поле, связывающем все физические и биологические объекты в одно целое. Если предыдущая волна развития Интернета (конец 1990-х гг. – начало 2000-х гг.) затронула, в основном, «лёгкие» B2C-сегменты и наиболее близкие к Интернету рынки (медиа, телеком, розничная торговля), то сейчас Интернет завоёвывает «тяжёлые» (индустриальные и инфраструктурные) сектора и регулируемые и специализированные рынки (медицина, образование). В этом мире новыми лидерами станут программно-аппаратно-сервисные гиганты – платформы по дистрибуции различных видов продукции и услуг и замкнутые экосистемы полного цикла производственно-сбытового обслуживания».

Ядром платформы (или экосистемы) может стать любая базовая цифровая услуга или комплексный продукт, который в дальнейшем, за счёт интеграции в него других продуктов и сервисов, сотрудничества с другими игроками рынка и развития комплексных технологических и маркетинговых решений, становится платформой и экосистемой.

Внедрению промышленного Интернета в России посвятил своё выступление президент НАПИ Виталий Недельский. По его мнению, IoT не является традиционно организованным рынком. Он формируется на стыке «физи-



Михаил Шеховцов



Виталий Недельский



Павел Литвинов

ческих» технологий и интернет-бизнесов. Это ведёт, во-первых, к переходу от отдельно функционирующих устройств к комплексным интегрированным системам и формированию продуктово-технологических платформ. Во-вторых, добавленная стоимость переносится с аппаратного обеспечения на программное обеспечение для управления и интеграции устройств и обработки данных. И, в-третьих, как факт, – масштабирование локальных решений за счёт развития смежных технологий и рынков: Big Data, Cloud, Fog Computing...

Технологии IoT находятся в активной инвестиционной фазе – на пике ожиданий, что связано с относительно низким уровнем зрелости технологий и высокой бизнес-активностью. На рынок выводятся отдельные платформенные решения на базе ключевых опорных технологий. Платформы IoT работают по принципу экосистем многостороннего рынка. При этом архитектура IoT только формируется, однако к системообразующим относятся четыре уровня: устройства, связь, обработка и управление данными.

Сегодня наиболее активная работа на всех уровнях IoT-платформ идёт в области стандартизации. Ведётся активная работа в области стандартов, покрывающих все уровни архитектуры IoT. Координаторами выступают Международный союз электросвязи (ITU), Ассоциация по стандартизации Института инженеров по электротехнике и электронике (IEEE Standards Association), консорциумы Open Interconnect, W3C и др.

При этом, по мнению Виталия Недельского, контроль над платформой IoT – вопрос не только бизнеса, но и безопасности и технологического роста. Технологии и решения, лежащие в основе информационно-телекоммуникационных платформ, являются объектом национальных программ кибербезопасности. К сожалению, в России отсутствуют материнские платформы, к тому же за последние пять лет в России не появилось ни одной мощной компании в сфере нового Интернета. Отрасль слабо центрирована и не обновляется «изнутри». Только появление сильных отечественных компаний, выступающих в качестве лидеров, способно обновить отрасль и изменить сложившуюся общую практику подключения к универсальной системе при самостоятельной разработке приложений.



**Иван Покровский**

Начальник аналитического отдела «РТСофт» Павел Литвинов, выступая с докладом «Киберфизические системы в современном IT-ландшафте», отметил, что появился ряд технологий будущего, которые уже меняют или изменят нашу жизнь и деловой ландшафт в ближайшие годы. Среди них: искусственный интеллект и развитие робототехники, большие данные, облачные технологии и сервисы, дополненная реальность, интернет 3.0, аддитивные технологии.

Правительства развитых стран включили киберфизические системы в приоритетный список инноваций, считая их критически важными для защиты своих национальных интересов. Такие системы позволят ведущим державам устранить, в частности, их нынешнюю зависимость от стран-фабрик и вернуть себе реальную самостоятельность. Компьютеры повлияли на те стороны жизни человека, которые так или иначе связаны с информацией, а киберфизические системы изменят все остальные.

Такие научные направления, как искусственный интеллект и кибернетика, объединены общей судьбой: недолгий начальный период эйфории и оптимистических высказываний сменился полным фиаско и многолетним забвением. Оба столь многообещающих направления сгубило отсутствие должного здравомыслия, но есть и объективная причина – недостаточная готовность технологий того времени к решению задуманных грандиозных задач. Казалось, будущего у искусственного интеллекта и кибернетики нет, однако полвека спустя они возрождаются, но в совершенно иной ипостаси. Теперь нет ресурсных ограничений, а задачи ставятся предельно



**Виктор Поляков**

ясные – нет речи о какой-либо передаче машине творческих задач, о разумных рассуждениях и действиях с помощью вычислительных систем и иных искусственных устройств. В современных условиях искусственный интеллект ограничен экспертными системами, базами знаний, системами вопрос-ответ и ещё рядом столь же понятных задач. Кибернетика также отказалась от туманных целей вроде анализа и выявления общих принципов и подходов в процессе научного познания. Сегодня она представлена киберфизическими системами (Cyber-Physical System, CPS), продолжающими дело встроенных систем, но на новом уровне.

Генеральный директор Центра современной электроники Иван Покровский рассуждал на конференции о рынке IoT в стратегии развития электронной промышленности. По его мнению, конкуренция закрытых вертикально-интегрированных систем, пульта управления, микроконтроллеры, передатчики, концентраторы, шлюзы, сетевое оборудование, датчики – это всё вчерашний день.

«Нас ожидает конкуренция открытых технологий. IoT разрушает сложившиеся закрытые рынки проприетарных систем управления. Образуются широкие технологические рынки, не зажатые корпоративными, ведомственными или национальными стандартами. Более эффективные технологии увеличивают свою долю, вытесняя конкурентов на открытых горизонтальных рынках. Увеличение масштаба позволяет снижать стоимость и проникать в новые области применений, более чувствительные к стоимости решений, – отметил Покровский. – Главными задачами для российских раз-



работчиков и производителей являются: достижение независимости от жёстких вертикально-интегрированных структур и рынков, развитие экосистемы российских разработчиков и интеграция в международные экосистемы, концентрация на ключевых компетенциях (расширение охвата рынка), реализация эффекта масштаба, а также, возможно, создание собственных комплексных решений».

### РОССИЙСКИЕ ТЕХНОЛОГИИ ДЛЯ РЫНКА ИНТЕРНЕТА ВЕЩЕЙ

В своём выступлении генеральный директор Tibbo Systems Виктор Поляков акцентировал внимание на IoT-платформах как будущем систем управления. По его мнению, у современных SCADA и IoT-платформ много общего: одинаковые протоколы сбора данных, методы хранения архивов становятся практически идентичными, время бинарных хранилищ ушло в прошлое, мнемосхемы можно рисовать и там, и там, возможности обработки данных временных рядов также имеют много общего. В итоге, IoT-платформы обладают всеми признаками SCADA-систем четвёртого поколения (работа в облаке, веб-визуализация, и т.д.).

Но, по сравнению с SCADA, IoT-платформы имеют определённые преимущества, среди которых: решение комплексных кросс-доменных задач (управление ИТ-инфраструктурой, мониторинг транспорта, моделирование сервисов, и т.д.), сбор и обработка не только тэгов, но и структурированных данных (таблицы инцидентов, каталоги сервисов, произвольные иерархии объектов и связей между ними), хорошая поддержка множества других протоколов из мира ИТ (Telnet/SSH, FTP), IoT (MQTT, CoAP) и универсальных протоколов (SOAP, CORBA), сложная визуализация данных (кар-

ты, статистические диаграммы, формы ввода данных, OLAP-кубы), работа в режиме Publisher/Subscriber, общение вещей друг с другом напрямую.

IoT-платформы займут множество позиций, на которых сейчас работает разнообразное ПО нижнего уровня. Это будет похоже на глобализацию ERP-систем, которые обязаны уметь всё. Это касается не только производства, но и любых компаний, имеющих дело с физическими активами (ритейл, агрохолдинги, энергетика, нефтегаз, транспорт и даже телекомы). Даже в индустрии SCADA софт будет продаваться как сервис, а многие существующие нишевые системы мониторинга и управления должны будут трансформироваться в сторону более глобальных решений, либо уйти с рынка.

Исполнительный директор ООО «ИнЧип Технологии» Борис Кривошеин озабочен безопасностью сетевой инфраструктуры IoT. К непосредственным угрозам безопасности в эпоху IoT относятся: взрывной рост «поверхности проникновения угроз» и мощности сетевых атак, создание Botnet-сетей из сотен тысяч и миллионов IoT-устройств. Докладчик отметил слабость защиты IoT-устройств, которая обусловлена, например, ограничениями производительности и объёма памяти, что не позволяет использовать «полные» сценарии сетевой защиты. К недостаткам также можно отнести использование предустановленных паролей (более 60% частных и около 20% корпоративных пользователей не меняют их). Производители IoT-оборудования заботятся, в первую очередь, о функциональности и стоимости, а безопасность реализуется по остаточному принципу. К недостаткам в области безопасности также можно отнести неконтролируемые процессы разработки и производства IoT-устройств, возможность внедрения

различных «закладок» в цепочке поставки, а также ограниченные возможности обновления прошивок в случае обнаружения уязвимостей.

Среди методов противодействия – защита интерфейса управления, авторизация (аутентификация) пользователей и встречного оборудования, ограничение доступности сетевых портов и служб, реализация криптозащиты на транспортном и канальном уровне, защита (шифрование) персональных данных, хранящихся в устройстве, и некоторые другие. К сожалению, все они пока на стадии разработки.

Руководитель департамента перспективных технологий Лаборатории Касперского Андрей Духвалов, рассказывая о российской операционной системе для Интернета вещей, задался вопросом «Почему системы уязвимы?». И сам же на него ответил: «Код пишут люди, а люди делают ошибки. Кроме того, уязвимость обеспечивают такие факторы, как использование стороннего ПО, постоянное усложнение систем и экспоненциальный рост объёма кода».

Лаборатория Касперского выработала требования встраиваемых решений к операционной системе – это небольшой размер и малое потребление ресурсов, безопасность «из коробки», надёжность и устойчивое выполнение даже под атакой, готовность к оценке и сертификации.

Необходимо усиление архитектуры системы и сохранение возможности повторного использования существующего программного кода, разделение операционных сред по уровням критичности функций и данных, а также по соответствующим уровням доверия.

Председатель совета директоров компании «Альтоника Радио Системы» Александр Шептовецкий, рассуждая о классификации и ограничениях

LPWAN-решений IoT, среди ключевых преимуществ LPWAN отметил дальность, энергоэффективность и стоимость. LPWAN обеспечивает большое количество конечных устройств и их миниатюрность, обратный канал и безопасность.

Первое и основное требование к LPWAN-сети – обеспечение большой дальности связи. Предельно достижимая дальность связи пропорциональна квадратному корню из мощности, вложенной в один бит, и практически не зависит от ширины канала, если ширина канала равна или превышает скорость передачи информации.

Технический директор «СМК» Николай Неудобнов рассказал, что компания уже более 5 лет занимается разработками в области маломощных беспроводных сетей и имеет большой опыт их создания, внедрения и эксплуатации. Решения от «СМК» нашли применение на железнодорожном транспорте, в строительстве, сфере ЖКХ, пожароохранных системах и системах дистанционного управления и мониторинга. Для взаимодействия с заказчиком отработано несколько возможных сценариев: от разработки системы «под ключ» до поставки незапрограммированных радиомодулей. В линейке продукции компании имеется несколько модификаций радиомодулей для всех нелицензируемых на территории РФ диапазонов. Каждая модель прошла обязательное тестирование в сертифицированной лаборатории Texas Instruments.

Фирма производит необходимый инструментарий для поддержки раз-

работчиков и ускорения вывода продукции на рынок. Все применяемые протоколы открыты и относятся либо к проприетарным (SimpliciTI), либо к стандартным (ZigBee, RF4CE или 6LoWPAN). Нарботано несколько вариантов типовых решений, требующих лишь незначительных модификаций под конкретные требования заказчика, что сокращает время внедрения системы.

### ТЕХНОЛОГИИ ГЛОБАЛЬНЫХ КОМПАНИЙ

Руководитель отдела развития RS Components Сергей Кривандин поделился проблемами поставки компонентов для построения устройств и систем Интернета вещей. Компания RS предлагает более 550 000 наименований различной продукции, среди которой электронные компоненты, кабели и разъёмы, решения для автоматизации, механические изделия и инструменты, полупроводники, тестирующие и измерительные устройства, источники питания, а также различные компоненты для систем автоматизации, предназначенные для использования на промышленном производстве.

Технический специалист Keysight Technologies Алексей Телегин представил решения Keysight для проектирования, отладки и комплексного тестирования устройств Интернета вещей. Решения компании Keysight позволяют моделировать функционирование глобальных навигационных спутниковых систем, таких как GPS, ГЛОНАСС, Compass/Beidou 2 и Galileo, а в Центре сервиса и метрологии компанией проводится тестирование устройств IoT для здравоохранения и автоматизации промышленности.

### ПРОЕКТЫ РОССИЙСКИХ ОЕМ-КОМПАНИЙ И СИСТЕМНЫХ ИНТЕГРАТОРОВ

Генеральный директор компании Револьта Инжиниринг Максим Осорин представил проект AllGateKeeper – облачный сервис по управлению шлагбаумами и парковками. Это хороший пример реализации коммерческого IoT-сервиса в рамках партнёрской программы Thingworx Powered.

Начальник аналитического отдела РТСофт Павел Литвинов в своём втором докладе на конференции задался вопросом «Как убедить главного инженера использовать IoT?». В качестве доводов в споре с воображаемым

главным инженером он предложил следующие аргументы: верить в перспективы применения технологий Интернета вещей и найти свой путь (инвестиции в эту тему не могут пройти бесследно), собирать и хранить все данные (в том числе и «сырые» – они скоро станут товаром), увеличивать количество разных сенсоров (ценность информации растёт), инвестировать в разработку моделей своей деятельности (использование Big Data), применять беспроводные технологии, не бояться облачных сервисов (позаботившись об имперсонализации данных), заключать «информационные» альянсы со смежниками, начинать использование Интернета вещей с небольших проектов (опыт и мотивация).

### ЗАКЛЮЧЕНИЕ

Подводя итоги конференции, предоставим мнения двух специалистов, выступивших на мероприятии наиболее программно. По словам Михаила Шеховцова, «Программы развития Интернета вещей в различных странах мира (Индустрия 4.0 в Германии, Интернет+ и другие программы в Китае, Консорциум индустриального Интернета в США) отвечают специфическим потребностям развития отдельных отраслей экономики этих стран, соответствуют месту и роли этих отраслей в мировом разделении труда и значению в национальных экономках. Так и стратегия развития Интернета вещей в России должна решать конкретные задачи развития российской экономики и конкретные бизнес-задачи, стоящие перед различными игроками рынка».

Виталий Недельский конкретизировал заявление Шеховцова так: «Для России приоритетными могут стать социально значимые проекты в сфере IoT, позволяющие решать проблемы, вызванные предыдущим поколением инфраструктур. Внедрение технологий IoT позволит решать задачи по нескольким ключевым направлениям: социально значимые, где наблюдается дефицит кадров и рост затрат на обслуживание (образование, здравоохранение, сельское хозяйство), зоны массового выбытия изношенных основных фондов в сфере энергетики, ЖКХ, автоматизируемой промышленности, обеспечение безопасности и повышение качества жизни граждан (городские инфраструктуры, ритейл, транспорт, финансовый сектор, социальные сервисы)».

