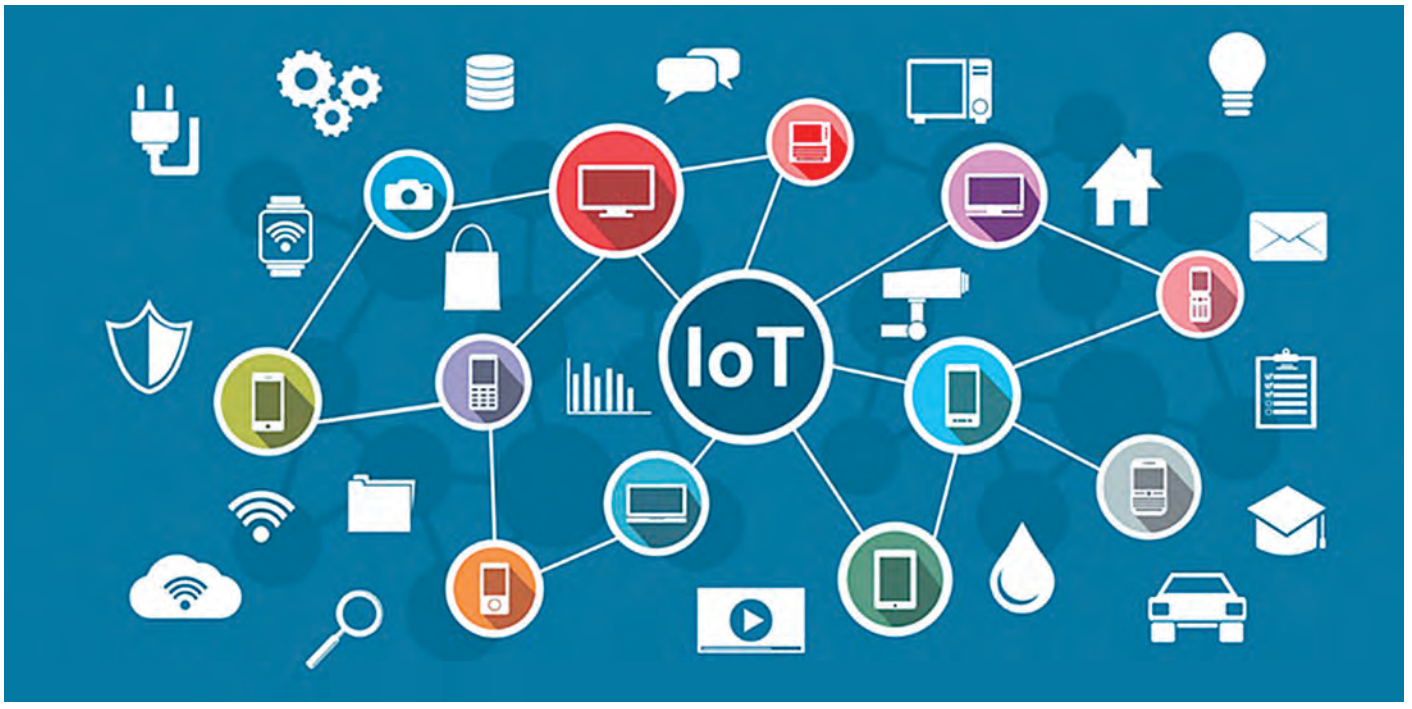
IoT — рынок, тренды, проблемы и перспективы

«Раньше думали: будет радио — будет и счастье. Вот радио есть, а счастья — нет».
Илья Ильф

Несмотря на то что сегмент «Интернета вещей» сейчас переживает период активного роста, похоже, мир до сих пор не готов воспринять все преимущества данной концепции. Потенциальным заказчикам не хватает знаний, специалистов, инвестиций.



Тема «Интернета вещей» не сходит со страниц тематической прессы вот уже несколько лет. Общее мнение практически единодушно выражает оптимизм относительно настоящего и будущего этой популярной концепции. Однако годы идут, проекты, вроде бы, тоже внедряются, но ощущаем ли мы то, что благодаря IoT окружающий мир начал меняться? В Украине — скорее всего, нет. А на Западе? Анализ открытых источников — в первую очередь статей в зарубежных отраслевых СМИ — убедительно демонстрирует то, что радикальных сдвигов в обществе или экономике развитых стран благодаря IoT пока не произошло. В результате ощущение чуда постепенно проходит, маркетинговый флер спадает под натиском реальности, а наступление удивительного будущего отодвигается в неопределенную перспективу.

Это если говорить про «IoT для всех». Но по отдельным отраслям ситуация может существенно отличаться. Например, больших успехов в вопросе внедрения «Интернета вещей» удалось достичь в промышленности, операторских системах связи, коммунальном хозяйстве, на транспорте и в ряде других специализированных областях. Другое дело, что информация, скажем, о новом этапе автоматизации производства не всегда интересует широкую общественность. В результате создается впечатление, что тема IoT постепенно сходит на нет, хотя, скорее, верно то, что она мигрирует в определенные ниши. Тем не менее «взрывной рост интереса» к IoT возможен в самом ближайшем будущем, если совпадет несколько важных факторов.

Рынок растет — остальное неясно

Для начала несколько слов о рыночной ситуации — она крайне туманна. Десятки аналитических агентств дают свои оценки и прогнозы, общий диапазон которых столь широк, что позволяет обосновать практически любой тезис о текущем положении и будущем состоянии сегмента. Это обусловлено главным образом тем, что границы понятия «Интернет вещей» до сих пор весьма условны, что позволяет аналитикам произвольно включать в область исследования самые различные типы устройств (а также ПО, услуги по интеграции и пр.). Например, в своем недавнем отчете IDC сообщила, что мировой рынок «экосистемы IoT» уже в 2023 году достигнет $1,1 трлн, компания Cision полагает, что к указанному времени сегмент достигнет примерно $0,84 трлн, мнение Statista — $0,8 трлн, оценка Fortune Business Inside — $0,57 трлн,

Orbis Research — $0,42 трлн. Список можно продолжать в таком же духе — единства здесь не будет.

Более-менее общее видение ситуации отмечается по предыдущим периодам. Так, оценки показателей мирового рынка IoT 2018 года в большинстве случаев попадают в диапазон $160–200 млрд, 2019-го — $200–250 млрд. В 2020-м рынок должен был бы стать еще больше, превысив рубеж в $300 млрд, но, судя по всему, прогнозы придется корректировать ввиду влияния эпидемии на все сферы глобальной экономики. Украинский рынок оценить еще сложнее — эксперты (сотрудники компаний-интеграторов и дистрибьюторов), с которыми нам удалось пообщаться в процессе подготовки материала, называли различные цифры — от нескольких миллионов до нескольких десятков миллионов долларов США. При этом все сходятся во мнении, что потенциал у местного сегмента IoT очень большой, но вряд ли его удастся реализовать в ближайшее время, поскольку все проекты, связанные с внедрением технологий «Интернета вещей», требуют немалых инвестиций, а в нынешней ситуации ожидать их не приходится. Когда же наша экономика вновь активизируется, основного спроса ожидают, в первую очередь, со стороны коммунальных и государственных предприятий, промышленности, транспорта и АПК.

IoT — не для пользователя

Когда тема «Интернета вещей» только начинала развиваться в широком информационном поле, довольно быстро наметилось два направления ее развития — «тяжелые» корпоративные решения и пользовательские системы. Примером первого из них является, например, промышленный «Интернет вещей» (Industrial Internet of Things, IIoT), вторая же группа объединяет различную потребительскую электронику и решения типа «умный дом» (точнее даже, «умное жилище»). Долгое время казалось, что это два относительно независимых направления, каждое из которых будет формировать отдельный рынок, где за выгоду от использования уникальных технологий будут платить, соответственно коммерческие компании и конечные потребители.

Сейчас же становится все более очевидным, что главным выгодополучателем остается бизнес, в первую очередь — крупный. Одна из главных особенностей систем IoT — сбор и анализ детальнейшей информации — пришлась очень кстати для многих компаний. В современном высококонкурентном мире бизнеса, особенно в экономически развитых странах, на рынке побеждает тот, кто лучше знает своего клиента и учитывает мельчайшие нюансы, влияющие на его выбор. Получить такое знание можно с помощью технологий IoT, собирая информацию с миллиардов пользовательских устройств — смартфонов, smart-часов, бытовых приборов, датчиков «умного дома» и т.д. При этом конечные потребители тоже получают определенное преимущество в виде дополнительных сервисов и удобства, которые обеспечивает им «умная» потребительская электроника, но компании приобретают именно финансовую выгоду — то, что потом можно превратить в деньги.

ИЗ ЧЕГО СОСТОИТ IoT

«Интернет вещей» – это не только концепция; в ее основе лежат вполне конкретные элементы и технологии. Чтобы внести больше ясности, перечислим основные из них.

Во-первых, это сенсоры и датчики – конечные устройства IoT, – собирающие те или иные данные.

Вторая группа, актуаторы – также конечные устройства, но уже оказывающие воздействие на окружающую среду, например, осветительные приборы, электронные замки, динамики и т.д.

Упомянутые элементы подключаются к шлюзам (gates), которые представляют собой специализированные микрокомпьютеры, способные осуществлять первичный анализ информации от датчиков или давать определенные команды актуаторам.

В масштабных системах шлюзы подключаются к полноценным серверам (которые отвечают за более сложную обработку и хранение данных), а те, в свою очередь, образуют сеть либо облако.

Связь между датчиками/актуаторами и шлюзами осуществляется с помощью специализированных энергоэффективных технологий передачи данных, например, LoRa или ZigBee. Шлюзы, в свою очередь, взаимодействуют с серверами по классическим сетям Ethernet или Wi-Fi.

Это один из аспектов современного мира с его экономикой, «основанной на знаниях» — благодаря новым технологиям компании уже не столько предполагают или прогнозируют, сколько знают то, как поведет себя клиент.

Скажем, «умный» холодильник с выходом в Интернет — это довольно занятная идея: он может, скажем, сам (на основе программы, заложенной пользователем) заказывать те или иные продукты, отслеживать скидки на интернет-сайтах популярных торговых сетей, уведомляя о них владельца, блокировать дверцу в определенные часы и т.д. Но за такой дополнительный функционал надо платить, зачастую, немало. Кроме того, что само «умное» устройство по определению дороже своего неинтеллектуального собрата, так еще и возрастают постоянные платежи — ведь надо платить не только за электричество, но за подключение к Интернету. Большинство пользователей к этому не готовы. Есть, конечно, любители инноваций, но не они преобладают на массовом рынке.

Зато производители давно смекнули, что продав «интеллектуальное» устройство с хорошей скидкой, можно затем с лихвой окупить такой дисконт за счет реализации знаний о предпочтениях потребителей. Информация, как правило, собирается в форме обезличенной статистики, а затем обрабатывается с помощью алгоритмов на основе ИИ. Зачастую можно отказаться от предоставления даже таких сведений, но в этом случае, вполне возможно, станет недоступен определенный функционал (либо его придется оплатить). Но даже если отказ не ведет к каким-либо последствиям, большинство пользователей все равно не будут копаться в настройках, чтобы отключить возможность сбора данных.

Условный «холодильник с интернетом», упомянутый выше, — возможно, не самый яркий пример. Более показательным в этом плане является практика использования smart-телевизоров. Эти устройства потенциально могут узнать о пользователе чрезвычайно много ценной информации, которую затем с удовольствием купят маркетинговые, рекламные, аналитические, PR агентства (в т.ч. работающие на политические партии), телеканалы и медиагруппы. Ведь данные о предпочтениях аудитории можно получить вплоть до конкретного домохозяйства. Теоретически можно пойти еще дальше и запретить, например, в интересах государства, демонстрацию того или иного контента определенным группам пользователей или целым регионам. Сейчас, когда у людей еще много обычных телевизоров — это утопия, но лет через десять, когда все будет в основном smart и онлайн — подобная ситуация станет вполне возможной. А основа всего этого — «Интернет вещей».

Отдельное большое и перспективное направление — персональные медицинские устройства, которые могут собирать достаточно детальную статистику о параметрах жизнедеятельности огромного числа людей с помощью IoT. Как полагают зарубежные аналитики, сбор и анализ подобных сведений способен дать существенный импульс развитию диагностической медицины — когда по едва уловимым признакам электронное устройство сможет выявить синдром приближающейся проблемы и уведомить об этом как самого пользователя, так и его врача. Здесь снова, как и во многих других случаях, пользователь получает удобство и нужную заботу в виде превентивной диагностики, а медицинская компания — деньги, например, за счет подписки на дистанционные врачебные услуги.

И, конечно же, IoT — основа таких перспективных и привлекательных концепций, как smart city, беспилотный транспорт, «умное» производство.

Ну и где ваше небо в алмазах?

Но если компании научились с помощью «Интернета вещей» собирать данные и обращать их себе на пользу, значит, у них-то, скорее всего, дела идут замечательно и за проектами IoT должны буквально выстраиваться очереди заказчиков? В теории вроде бы да, но, как обычно, хорошие идеи часто разбиваются о неумолимую практику. «Интернет вещей» — классический пример концепции обогнавшей свое время. Сегодня у нас есть масса подходов, идей, даже воплощенных разработок. Но не хватает главного — универсальной инфраструктуры передачи данных и единых стандартов. Доминирующая технология также отсутствует. Вместо нее — десятки отраслевых вариантов реализации IoT. Логично, что роль среды передачи для основной массы устройств «Интернета вещей» должны выполнять сети операторов мобильной связи, которые охватывают сегодня большую часть населения Земли. Но проблема в том, что нынешние форматы 3G и даже 4G плохо подходят для массового разворачивания инфраструктур

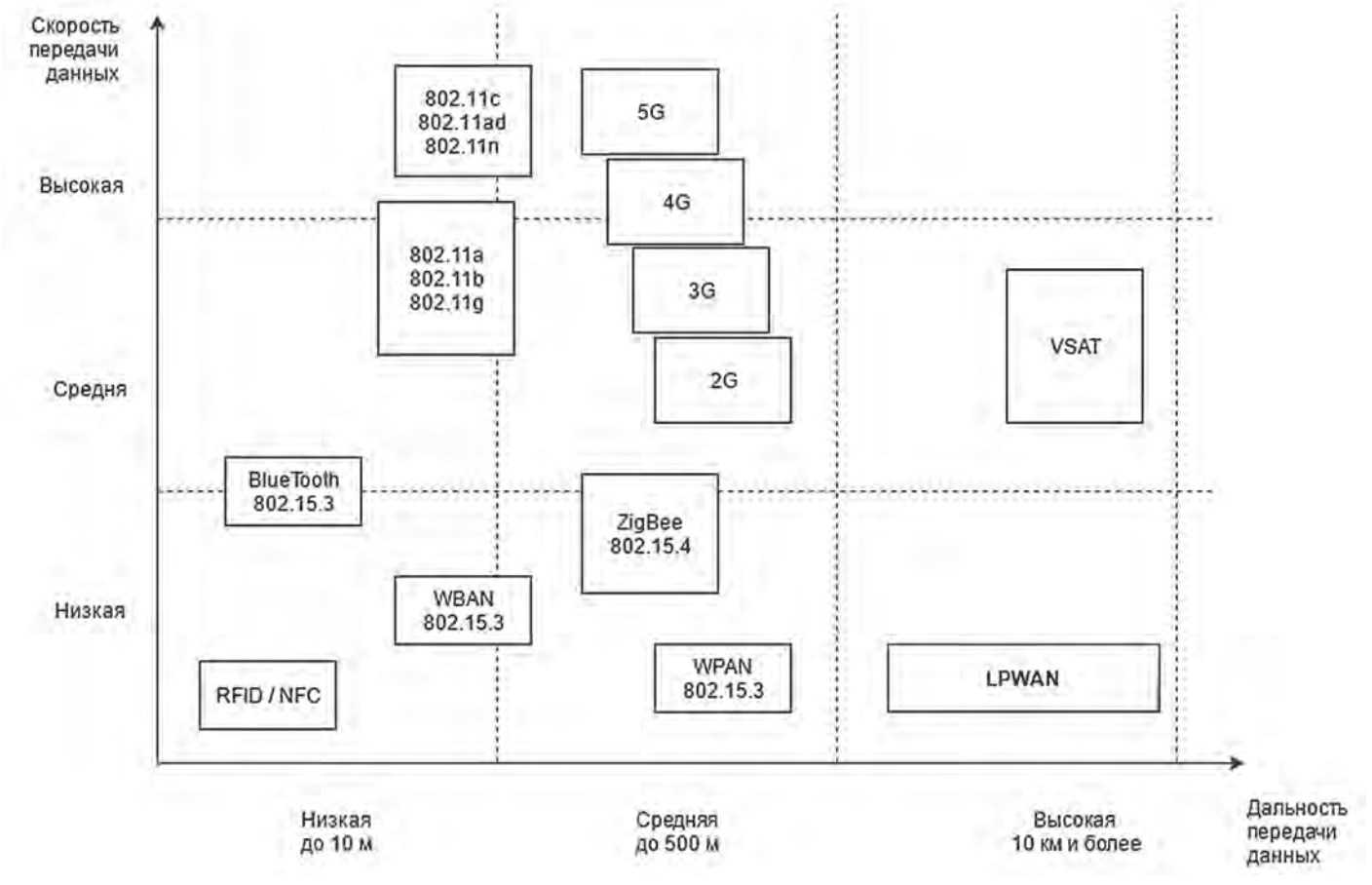


Рис. Сравнение различных радиотехнологий, используемых для построения сетей IoT. Источник: «Хабр» (habr.com)

IoT — скорости передачи данных должны быть больше (**рис.**), задержки меньше. Скажем, в США нормальной задержкой на сетях LTE считается 50 мс — более чем достаточно для человеческого восприятия, но в случае межмашинных интерфейсов, используемых устройствами IoT, желательно, чтобы задержка была существенно меньше — в пределах нескольких миллисекунд.

Это могут обеспечить только мобильные сети пятого поколения (5G). Собственно, с их повсеместным внедрением многие производители связывают будущее быстрое развитие IoT, а ведь операторы по всему миру так или иначе развернут 5G, как универсальную технологию передачи данных, в перспективе ближайших нескольких лет. Поэтому отраслевые технологии, например, LPWAN, скорее всего будут иметь довольно узкое применение, поскольку для них потребуется разворачивать собственные специализированные сети, вместо того чтобы использовать уже готовую инфраструктуру операторов связи. А пока 5G только начинает внедряться, многие компании предпочитают не спешить с реализацией проектов.

Еще одна проблема заключается в возможностях масштабирования. Классическая ситуация — инженеры разрабатывают отличный проект, создают прототипы и все работает, как задумано, пока сеть объединяет всего несколько устройств. Когда же проект быстро разрастается и количество подключений исчисляется тысячами, возникают неожиданные технологические проблемы, которые просто невозможно было выявить на стадии прототипа. Как свидетельствуют данные исследования, проведенного компанией Cisco в 2017 году среди почти 2 тыс. респондентов, около 60% проектов заходят в тупик еще на стадии утверждения концепта. Опрошенные эксперты отметили, что инициативы IoT часто выглядят хорошо на бумаге, но оказываются намного сложнее в реализации, чем кто-либо ожидал. В числе главных причин неудач особо были отмечены пять факторов:
– невозможность правильно рассчитать сроки реализации проекта;
– ограниченная внутренняя экспертиза;
– недостаточное качество данных;
– отсутствие интеграции между командами внедрения;
– превышение бюджета сверх изначально планируемого.

Кроме того, специалисты, столкнувшиеся на практике с крупными проектами IoT, говорят о том, что сложность подобных внедрений растет экспоненциально, по мере подключения новых устройств. В результате все больше времени начинает уходить на поиск ошибок и отладку процессов — в какой-то момент затраты на поддержку сети IoT (как временные, так и финансовые) начинают превосходить вложения в ее развитие. Подобной ситуации сегодня удается избежать, как правило, в тех проектах, где выдержан сбалансированный подход к требованиям функциональности и сбора данных, иными словами там, где обходятся разумным минимумом того и другого.

Судя по всему, главная ошибка неудачных проектов заключается в том, что разработчики перегружают систему функциями, требованиями и к тому же стремятся собрать все возможные данные в надежде, что из них потом можно будет извлечь полезную информацию. Как следствие, все решение выходит неожиданно сложным и ресурсоемким. В этом состоит основа мнения, что проекты «Интернета вещей» неоправданно дорогие — но при взвешенном подходе это не так.

И, кстати, при проектировании и построении сетей IoT зачастую игнорируют скрытые затраты, которые возникают неизбежно и могут составлять существенную часть стоимости внедрения. Речь о таких моментах, как подготовка проектной документации, техническое обслуживание (включая регулярное обновление АКБ), замена и ремонт вышедших из строя устройств и т.д. Многих проблем и дополнительных расходов можно было бы избежать при грамотном подборе и проектировании решения на самых ранних этапах, но по ряду причин (в первую очередь из-за отсутствия профессионального опыта и навыков) такое происходит крайне редко.

Вместе с тем «Интернет вещей» остро поставил вопрос кибербезопасности, причем на совершенно новом уровне. Ставки здесь постоянно растут, ведь в том случае, если концепция будет внедряться повсеместно, хакеры смогут получить доступ не только к самым детальным личным данным пользователей, но и к важным объектам критической инфраструктуры, транспорту, коммуникациям и т.д. При этом сложность обеспечения защиты IoT-сетей стремительно увеличивается по мере включения в них все большего числа устройств. Вопросов здесь пока гораздо больше, чем хотелось бы, и ответы на них необходимо получить в самое ближайшее время, иначе дыры в безопасности IoT сведут на нет все преимущества концепции и усилия по ее внедрению.

Тем не менее упомянутые сложности вовсе не означают, что IoT — плохая идея. Все как раз наоборот — идея прекрасна, но для ее практического и повсеместного воплощения многое еще предстоит сделать.

Несколько слов о будущем IoT

Судя по всему, «Интернет вещей» ждет перспективное будущее. Ведь эта концепция очень удачно впитывает в себя все самые передовые технологии. Появление 5G открывает новые перспективы по развитию инфраструктуры IoT, инструменты работы с большими данными дают возможность осуществлять глубокий и эффективный анализ информации, пограничные вычисления (Edge Computing) позволят разгрузить дата-центры и магистральные каналы связи за счет локальных вычислений. Большие надежды возлагаются на будущие достижения в сфере искусственного интеллекта, с помощью которого удастся обеспечить удобное управление сетями IoT и их бесшовное масштабирование. Облачные платформы станут основой для обработки и надежного хранения данных, а блокчейн обеспечит новые услуги с высоким уровнем безопасности. Да, потенциальных проблем на этом пути еще много, но с другой стороны — где их нет?

Игорь КИРИЛЛОВ, **СиБ**