IoT уже рядом

«Интернет вещей» плотно входит в повседневную жизнь. Просто мы этого еще не замечаем. Концепция проникает все глубже во все сферы человеческой деятельности — от энергетики и промышленности до бытовой техники. Украина — не исключение, однако новые возможности сопряжены и с определенными рисками.

Некоторые решения и технологии входят в нашу повседневную жизнь незаметно. Не то чтобы они были необходимы, просто общий прогресс ведет к тому, что определенные вещи, считавшиеся еще десятилетие назад чем-то из области фантастики, сегодня становятся фактически повсеместным стандартом. Одной из таких концепций может стать «Интернет вещей» (IoT). О возможностях IoT особенно много говорят в последние годы, но разговорами дело не ограничивается. Сейчас наступает период широкого применения технологии. В экономически развитых странах мира — это весьма ощутимый тренд. Украина еще в начале пути, но и у нас есть первые крупные внедрения, за которыми подтянутся остальные. По мнению многих специализированных компаний, уже в 2020 году мы, очевидно, будем наблюдать бум внедрения систем на базе IoT — к этому есть все предпосылки. Справедливости ради стоит отметить, что четкие рамки концепции еще не устоялись, и к «Интернету вещей» причисляют самые разнообразные системы и технологии. Но это нормальный процесс становления нового перспективного рынка. Тем не менее год от года конкретики становится все больше, появляются новые отраслевые стандарты, формируются устойчивые взгляды на то, как должен выглядеть тот или иной аспект IoT.

Давайте же рассмотрим, в каком состоянии сейчас находится отрасль в целом и каковы перспективы «Интернета вещей» в нашей стране. За последние несколько лет, прошедшие со времени написания предыдущего обзора по данной теме — ***«Internet of things: не только кофеварки», СиБ, №2, 2015 г.,*** — многое изменилось.

Здесь сразу стоит очертить круг рассматриваемых вопросов, ведь понятие «Интернет вещей» описывает чрезвычайно широкий круг явлений. В статье мы будем опираться на корпоративные и промышленные системы, использующие сети датчиков, шлюзов и контроллеров, которые фактически представляют собой дальнейшее развитие идеи M2M (machine-to-machine).

bticino

eliot™
ПРОГРАМА LEGRAND

Eliot – це назва програми Групи Legrand, присвяченої інтернету речей (ELectricity + Internet Of Things). Eliot – зареєстрований товарний знак, який є власністю Групи Legrand

Тепер виклик
з домофону передається
і на Ваш мобільний

Завантажте безкоштовні додатки

ANDROID APP ON Google play

Available on the App Store

CLASSE 300

Внутрішній кольоровий відеоблок з інтегрованим Wi-Fi*.

Монтаж на стіну або з підставкою на стіл.
Білий або чорний.

*доступна інтеграція з камерами NETATMO

ТОВ «Легранд Україна»
04080 м. Київ, вул. Турівська, буд. 31
Тел.: + 38 (044) 351–12–00,
Факс: + 38 (044) 351–12–15
@LegrandUkr

Бренд Групи legrand®

Таблица 1. Инициативы по развитию IoT, принятые в разных странах

Страна	Название программ	Меры по реализации программ
США	SmartAmerica Challenge; Industrial Internet Consortium; комплекс программ по развитию киберфизических систем	Целевые инвестиционные программы, направленные на развитие исследовательских центров и лабораторий как со стороны федеральных структур, так и на уровне отдельных штатов. Развитие государственно-частного партнерства. Внедрение тематических образовательных программ
ФРГ	Industrie 4.0	Государственное финансирование НИОКР и прикладных разработок в рамках индустриальных консорциумов
КНР	Дорожная карта развития IoT	Создание индустриальных зон в десяти областях и формирование сотни компаний-лидеров с помощью бизнес-инкубаторов. Инвестиции в НИОКР, использование лучших мировых практик, создание инновационных центров и лабораторий
Сингапур	Национальный план развития ИКТ	Создание инженерных лабораторий и реализация образовательных программ, инвестирование в проекты «умного города», поддержка и развитие тематических бизнес-инкубаторов, инженерных лабораторий, исследовательских центров
Индия	Проект развития IoT	Создание пяти демонстрационных центров, пятнадцати специализированных бизнес-инкубаторов (и такого же количества крупных образовательных учреждений) для развития IoT, реализация крупных проектов

«Интернет вещей» как элемент мирового прогресса

Технологии «Интернета вещей» стремительно развиваются во многих странах. Во всяком случае, об этом свидетельствуют свежие аналитические отчеты. Так, в конце августа нынешнего года Microsoft обнародовала результаты тематического исследования IoT Signals. По данным компании, 85% опрошенных организаций развивают один или более проектов, связанных с «Интернетом вещей» (к 2021 году таковых ожидается уже 94%). Но лишь 30% респондентов надеются окупить инвестиции в двухлетней перспективе. Все-таки IoT — это вложение на годы. Были заданы вопросы и относительно того, что мешает внедрению концепции. В числе основных сдерживающих факторов были названы сложности внедрения и нехватка квалифицированных кадров. К тому же почти все респонденты (97%) выразили обеспокоенность, связанную с вопросами обеспечения кибербезопасности для сетей IoT.

Есть оценки и по конкретным показателям. Так, согласно данным отчета IDC, в 2018 году объем глобального рынка IoT достиг $646 млрд, а по итогам 2019-го он должен вырасти еще на 15,4% — до $745 млрд. В то же время аналитическая компания GlobalData говорит о том, что в прошлом году общий объем данного рынка едва превысил $200 млрд, а планка в $300 млрд будет

Таблица 2. Основные телекоммуникационные технологии IoT

Название технологии	Альтернативное название	Зона действия	Радиодиапазон, МГц
NFC/EMV	ISO14443	Метры	13,56
RFID (метки HF)	–		13,56
Thread	802.15.4-2003/6LoWPAN	Десятки метров	2400
ISA100.11a	802.15.4e/6LoWPAN		2400
Z-Wave	ITU G9959		868, 915, 920
EnOcean	ISO14543-3-10		315, 915, 920
ANT+	–		2400
Bluetooth	802.15.1		2400
Positive Train Ctrl	802.15.4p	Десятки/сотни метров*	220
RFID (метки UHF)*	–		860, 960
ZigBee	802.15.4-2003, c d	Десятки метров/километры*	779, 868, 915, 920, 2400
Wi-Fi	802.11/a/b/g/n/ac	Сотни метров	2400, 5800
Sidewalk	–	Сотни метров	900
NB-IoT	Cat-M2	Километры	700, 800, 900
Wi-SUN	802.15.4g/e/6LoWPAN	Километры	920
WiMAX	IEEE 802.16	Километры	3500, 5000
LoRa	–	Десятки километров	433, 470, 868, 920
SIGFOX	–		868, 915
LTE Cat-M1	Cat-M		1400
Telensa	–		868, 915
OnRamp	802.15 4k		2400
Wireless M-Bus	EN13757		169, 433, 868
China WMRNET	WMRNET I, II, III, IV		433, 470
WirelessHART	802.15.4e		2400
Wi-Fi HaLow	802.11ah		779, 868, 915, 920
V2X	802.11p		5900

* В зависимости от реализации

взята лишь в 2023-м. Еще больший разброс наблюдается в вопросе количества подключенных устройств. Так, Berg Insight оценивает его в 1,2 млрд, а Strategy Analytics — в 22 млрд, и обе компании говорят об итогах 2018 года. Данные других отчетов приводить нет смысла, поскольку единства во взглядах зарубежных аналитиков не наблюдается, а любые оценки колеблются в широчайшем диапазоне. Но все сходятся во мнении, что мировой рынок IoT стремительно развивается и у него блестящее будущее.

В этом контексте интересен также отчет компании Eclipse Foundation, которая определила наиболее популярные в мире платформы для развертывания сервисов IoT (всего их насчитывается не менее полутысячи, и это число постоянно растет). Лидируют облачные операторы, а первая пятерка платформ выглядит следующим образом: Amazon Web Services (более половины рынка), Microsoft Azure, Google Cloud Platform, Kubernetes, IBM BlueMix. Самыми распространенными протоколами для обмена данными между устройствами IoT названы MQTT (Message Queuing Telemetry Transport, работающий поверх TCP/IP) и набирающий популярность открытый протокол AMQP (Advanced Message Queuing Protocol). Среди специализированных операционных систем чаще других встречаются FreeRTOS, ARM Mbed и Contiki.

При этом во многих ведущих странах мира тенденция к широкому внедрению IoT уже отражена в различных государственных программах, самой известной из которых, наверное, является знаменитая немецкая концепция развития инноваций в промышленности Industrie 4.0. Свои инициативы есть в США, КНР, Великобритании, Сингапуре, Индии (**табл. 1**).

На сегодняшний день IoT уже достаточно активно используется в таких сферах, как транспорт, коммунальное хозяйство, медицина, физическая безопасность, агропромышленный комплекс, розничная торговля (ритейл), «умный город», «умное здание» и т.д. Кроме того, проекты на базе IoT активно тестируются и внедряются в армиях стран НАТО (в прессе даже появился соответствующий термин — Internet of Battle Things). Главной целью IoBT является обеспечение эффективного взаимодействия между всеми «своими» устройствами на поле боя — это могут быть роботы, различные датчики, размещенные на борту военной техники, сенсоры, входящие в состав персонального снаряжения или «умного» оружия, и т.д.

Тем не менее, несмотря на все усилия отдельных разработчиков, профильных ассоциаций и правительственных структур, сфера IoT все еще очень далека от единства, что также является сдерживающим фактором в распространении концепции. Одних только телекоммуникационных технологий здесь несколько десятков (**табл. 2**). Они отличаются скоростью передачи, диапазоном радиочастот, радиусом действия, устойчивостью работы и пр. Каждая технология имеет своих сторонников и ориентирована на определенные сферы применения. Детальное рассмотрение каждой из них потянет на отдельную книгу (здесь у всех своя история, нюансы реализации, варианты исполнения), поэтому ограничимся простым перечислением наиболее распространенных из них. Главная задача таблицы — показать, сколь разнородным сегодня является «Интернет вещей». При этом список далеко не исчерпывающий, еще есть Dotdot, MiWi, SNAP и другие технологии.

МЕГАТРЕЙД
СПЕЦІАЛІЗОВАНИЙ IT-ДИСТРИБУТОР

cisco Partner
Distribution Partner

Запитай
про MSLA
у свого
IT партнера

Трансформуй
Capex в Opex
з рішеннями
Cisco MSLA

- Масштабуйтесь.
- Залишайтесь гнучкими.
- Знижуйте витрати за допомогою моделі pay-as-you-go.

megatrade.ua/msla

* Managed Service License Agreement
– гнучка ліцензійна модель для власників хмарної або гібридної інфраструктури

IoT ТРЕБУЕТ ОСОБОГО ПОДХОДА К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Повсеместное развитие технологий Интернета вещей (IoT) открывает множество новых возможностей, как для бизнеса, так и для частных пользователей. Особую роль в этом процессе играют средства измерения, такие как датчики и сенсоры, обеспечивающие преобразование сведений в машиночитаемые данные и тем самым наполняющие вычислительную среду значимой информацией. Но, к сожалению, эти виды устройств исторически наименее защищены с точки зрения информационной безопасности, что нередко играет на руку киберпреступникам.

Например, в декабре 2014 года было сообщено о значительном повреждении нефтепровода, соединяющего Каспийское и Средиземное моря. Предполагаемые причины сбоя связаны с кибератакой, которая отключила датчики, установленные по всей длине трубопровода для выдачи предупреждений о неисправностях. В то же время вредоносное ПО спровоцировало рост давления в трубе, что в итоге вызвало ее разрыв.

Кроме того, широкую известность также получил инцидент с вирусом Stuxnet, который атаковал операционную систему иранских урановых центрифуг Natanz, заставляя их функционировать в самом неблагоприятном режиме, что приводило к преждевременному выходу оборудования из строя. При этом, очевидно, система мониторинга также была взломана, что не позволило своевременно выявить нештатный режим работы. При этом сегодня множество вредоносных программ используют проект Stuxnet для атаки на организации и государственные структуры по всему миру. В числе известных примеров – Flame, Duqu, Stars, Shamoon, Nitro Zeus. Атаки совершались в т.ч. на энергетические сети Украины и Эстонии.

К счастью, параллельно с развитием технологий, цель которых вредить и разрушать, развиваются и средства защиты. В частности, есть уже готовые решения, позволяющие выявить аномалии в машинных данных, которые могут свидетельствовать о кибератаках. При этом подобные разработки носят междисциплинарный характер – в их основе достижения в области физики, машинного обучения, работы с большими данными.

Эффективная система противодействия киберугрозам для систем IoT обладает механизмами самообучения и, используя историческую информацию с датчиков и сенсоров, способна выявлять искаженные данные, аномалии, ложные сведения, информацию, не имеющую физической основы, и т.д. По сути, мы имеем некий «детектор лжи», способный выявлять ложные или скомпрометированные данные с датчиков и сенсоров на промышленных предприятиях.

Александр КУЧУК,
руководитель направления информационной безопасности ELKO Ukraine

Дело в том, что некоторые сценарии атак не требуют подделки данных, но тогда атаки, направленные на нанесение серьезного или катастрофического ущерба, всегда будут требовать манипулирования данными, чтобы скрыть вредоносные действия. Кроме того, если злоумышленник пытается систематически уничтожить множество устройств, он должен работать незаметно и, следовательно, подделывать некоторые данные на определенном этапе. При таких сценариях нужны специальные комплексные решения, позволяющие выявлять угрозы, которые не способен выявить человек либо стандартные системы кибербезопасности.

Решения, позволяющие вовремя выявлять аномалии в технологических данных и информировать ответственный персонал, не допуская возникновения инцидентов, которые могут повлечь за собой аварии и катастрофы, уже существуют и широко используются. И, конечно, они уже могут встать на защиту организаций в Украине.

Таким образом, о какой-либо унификации речь пока не идет. Более того, периодически появляются новые разработки. Например, в конце сентября 2019 года Amazon протестировала собственную радиотехнологию передачи данных для IoT под названием Sidewalk. Ее даже опробовали на реальном оборудовании в Лос-Анджелесе, в ближайшее время планируется коммерческий запуск. Но это, похоже, не предел. Сейчас начинают внедряться сети мобильной связи пятого поколения (5G), которые породят свой пул стандартов и подходов к построению IoT. Все это в целом характерно для начального периода становления любой сложной технологической отрасли. Так что какую форму приобретет «Интернет вещей» через 5–10 лет, сейчас даже сложно представить.

Безопасность под вопросом

По мере распространения «Интернета вещей» наряду с преимуществами всплывает немало актуальных и потенциальных проблем. Одна из наиболее существенных — обеспечение кибербезопасности. Ведь, получив доступ к сетям IoT, злоумышленники смогут создавать угрозы на новом уровне. Так «Интернет вещей» уже используется для проведения грандиозных DDoS-атак, в которых участвуют сотни миллионов устройств. Но это лишь начало. Новый виток развития — вымогательство денег у владельцев «умного дома». Уже зафиксированы случаи, когда, захватив управление системой, хакеры требовали выкуп, например, за разблокировку электронных дверных замков. Таким образом, любой человек теоретически может оказаться заложником в собственном доме. Кроме того, есть еще и скрытые угрозы. Например, злоумышленники могут негласно следить за людьми в доме, слушать их разговоры, а затем использовать полученную информацию в корыстных целях.

Но это, скорее, персональные проблемы, которые, не создают угроз национальной безопасности. Гораздо серьезнее то, что хакеры могут получить доступ к датчикам и системам управления на стратегических объектах — такие случаи отмечались для энергетической и транспортной инфраструктур в разных странах.

Что может дать контроль над обычными датчиками? С их помощью, например, можно исказить показатели измеряемых параметров, что в итоге нарушит работу всей системы или спровоцирует ошибочные действия персонала и, как следствие, приведет к аварии. В то же время отказаться от технологий IoT в современных системах вскоре будет попросту невозможно, а значит, вопросы безопасности необходимо решать уже сейчас. Но выработка единых подходов к решению данной задачи представляет собой большую проблему ввиду разнородности технологий, применяемых в сетях «Интернета вещей». Самое главное, что принятые сегодня методы киберзащиты в случае IoT вряд ли будут эффективны — нужны новые подходы. Они, естественно, разрабатываются — есть ряд коммерческих продуктов.

Но общий подход к решению задачи формируется в ходе работы над стандартом JTC 1 SC 41 Internet of Things and related technologies («Интернет вещей и смежные технологии»), который ведет специальный подкомитет Объединенного технического комитета №1 ИСО/МЭК. В рамках общей концепции разрабатывается и стандарт ISO/IEC 30149 Internet of Things (IoT) Trustworthiness frameworks, направленный на безопасность. Хронологически последнее заседание международной группы по этому вопросу состоялось в мае 2019 года, а утверждение стандарта запланировано на 2021 год.

Первые проекты в Украине

Как и во всем мире, сегмент IoT в нашей стране — это, прежде всего, рынок стартапов. Маститые интеграторы, как правило, не получают здесь преимущества перед небольшими, узкоспециализированными компаниями. Ведь «Интернет вещей» — это не столько конкретный набор технологий, сколько общая концепция, требующая гибкого и адаптивного подхода, а зачастую и определенных фирменных ноу-хау, созданных специально для решения задач конкретного заказчика. Конечно, со временем здесь появятся свои лидеры, но сейчас украинский рынок сильно фрагментирован, и кого-то выделить на нем достаточно проблематично. Тем более что по сути не существует сегмента IoT «в целом», здесь важна отраслевая специализация — одни компании сильны в автоматизации коммунального хозяйства, другие занимаются промышленными решениями, третьи берутся за АПК или коммерческое строительство. В каждом направлении уже сегодня представлены десятки игроков, и число их растет. Т.е. буквально сейчас мы наблюдаем за становлением совершенно нового рынка.

В то же время оценить его объем для нашей страны пока что не представляется возможным. Крупных проектов не слишком много, данные обо всех небольших внедрениях тоже собрать проблематично. Тем более что компании не особенно охотно делятся сведениями, да и большинство внедрений, как правило, носит «пилотный» характер. Экспертные оценки рынка дают слишком большой разброс — называются суммы от $2–3 до $50 млн и выше. Однако подавляющая часть оценок все же находится ближе к нижней границе этого условного диапазона. Это тем более

DELTA
Smarter. Greener. Together.

Повнофункціональне рішення для високоефективного електроживлення ЦОД

NEW

ДБЖ Delta Amplon RT 5-20 кВА (1:1 / 3:1)
с Li-ion батареями

- Висота 2U
- Вихідний коефіцієнт потужності дорівнює **1**
- Можливість паралельного включення до **4** ДБЖ

Server Network Banking POS Security

МЕГАТРЕЙД
СПЕЦІАЛІЗОВАНИЙ IT-ДИСТРИБУТОР

Офіційний дистрибутор DELTA в Україні
www.megatrade.ua

«УМНАЯ ПЫЛЬ» — КОМПЬЮТЕР В 1 КВ. ММ

Идея построения широкой распределенной сети на основе автономных информирующих сенсоров, которая могла бы работать в полевых условиях, впервые была реализована военными. В начале 90-х знаменитое оборонное агентство США DARPA в сотрудничестве с компанией Rand Corporation разработало модель миниатюрного компьютера – размером не более спичечного коробка, который содержал сенсор для учета параметров окружающей среды, вычислительного модуля, приемопередатчика и элемента питания (аккумулятор и солнечная батарея). Устройство назвали mote – «пылинка».

По мере совершенствования технологий микроэлектроники и более широкого их распространения стали появляться более компактные решения, в т.ч. коммерческие. Так, в 2015 году американская компания CubeWorks представила микроскопический модуль Cubisens, состоящий из процессора ARM Cortex M0 с 4 кБ памяти, радиопередатчика, сенсора, АКБ и солнечной батареи. Энергопотребление всей системы в режиме ожидания составляет 8 нВт, удельная мощность зарядного устройства – 10 нВт на 1 кв. мм.

Радиус действия каждого устройства невелик, но за счет последовательной схемы передачи данных (от датчика к датчику), можно построить довольно обширные сети. Появляются и другие разработки в этом направлении.

Микрокомпьютер — элемент «умной пыли» — на ребре монеты в пять американских центов

Так, в 2018 году IBM сообщила о разработке полноценного микрокомпьютера размером с крупную песчинку, площадь основания которого составляет всего 1 кв. мм. Помимо процессора и памяти в устройстве имеется приемопередающий модуль оптической связи. При этом, как сообщается, в случае массового производства такой компьютер будет стоить примерно $0,1 за единицу, что позволит строить обширные коммерческие сети на основе «умной пыли», состоящей из миллионов устройств.

правдоподобно, учитывая общее отношение украинских заказчиков к IoT. Многие из них слышали о концепции и даже теоретически хотели бы иметь у себя нечто подобное. Но страх потратить деньги впустую пока что слишком силен. Рынок еще в ожидании крупных и успешных внедрений.

По словам сотрудников компаний, работающих в сфере «Интернета вещей», потенциальные заказчики интересуются технологией, заказывают демонстрации и тестирование на конкретных задачах, но дальше дело заходит редко. При этом в нынешнем году на рынок IoT вышли операторы мобильной связи. Так, в середине апреля собственную сеть «Интернета вещей», покрывающую Киев, Львов и Кропивницкий, запустил Lifecell совместно с компанией IoT Ukraine. На момент старта ее услугами пользовались не менее десяти заказчиков (проект постепенно внедрялся с июля 2018 года). Для развертывания сети было установлено восемьдесят базовых станций. В качестве основной технологии выбрана LoRaWAN. Для построения системы использовалось оборудование и ПО таких компаний, как Libelium, Orion M2M, Abeeway, Cisco, Actility, Gross, Infomir, при этом две последние компании — это украинские разработчики. В числе первых заказчиков — ОАО «Кировоградгаз», КП «Львовводоканал», ЗАО «Львовоблэнерго», киевский ТРЦ «Арт Молл», гипермаркет «Ашан» и др. В числе наиболее востребованных возможностей — управление освещением, учет ресурсов (расход тепла, воды, газа), мониторинг состояния окружающей среды и микроклимата помещений, автоматизация парковок, контроль открытия канализационных люков и дверей в технологические помещения.

Немного позже, в июле, свою сеть IoT, развернутую в Киеве, представил и Vodafone Ukraine, правда, пока что в тестовом режиме. В отличие от решения Lifecell, здесь применяется технология передачи данных NB-IoT (Narrow Band Internet of Things), использующая радиоканалы LTE.

Возможности платформы были проверены на задачах «Киевводоканала». В ближайшее время планируется коммерческий запуск продукта по всей Украине. Напомним, что еще в феврале 2019 Vodafone Ukraine объявил о запуске партнерской программы для разработчиков, в рамках которой ожидается получение различных готовых продуктов для IoT и работы с большими данными.

Отметим, что ключевым отличием между NB-IoT и LoRaWAN является то, что для применения последней не требуется получение лицензии на использование радиочастотного спектра, к тому же оборудование, поддерживающее эту технологию, стоит относительно недорого. В то же время NB-IoT работает быстрее, но доступна по сути только операторам мобильной связи, поскольку используются базовые станции LTE (либо GSM). Эти две технологии, как правило, имеют разные сферы применения, поэтому нередко зарубежные компании комбинируют их в своих сетях.

Также известно как минимум об одном крупном внедрении, не связанном с телеком-операторами, на юге Украины, где компания «Одессагаз» установила в зоне своей ответственности несколько тысяч специальных модемов для централизованного сбора показаний газовых счетчиков в частных домах.

Интересный демонстрационный проект был реализован летом 2019 года в Киеве, где на участке тротуара протяженностью около ста метров был устроен прототип «умной улицы», оснащенной солнечными

панелями, зарядками для электротранспорта, системами видеонаблюдения и датчиками, анализирующими загрязнение воздуха. В своем комментарии относительно запуска проекта ***директор Департамента информационно-коммуникационных технологий КГГА Юрий Назаров*** отметил: «*Я рад, что горожане, проживающие на улице Салютной, имеют свободный доступ к возможностям, которые дает «Интернет вещей», а это, помимо прочего, современный уровень безопасности, энергосберегающие технологии и качественный Интернет*».

Но в целом сведения о более-менее заметных реализациях на территории Украины весьма скудны и отрывочны, хотя компаний, готовых внедрять IoT во всем его многообразии, сегодня хватает.

Рассуждая о факторах, тормозящих развитие «Интернета вещей» в нашей стране, опрошенные нами эксперты отмечают, что большинство из них лежит не в технологической плоскости. Главная проблема — устаревший подход к организации хозяйства. Скажем службы ЖКХ, как правило, не заинтересованы в уменьшении расхода ресурсов или сокращении персонала. К примеру, существующие нормативы допустимых значений утечки воды в коммунальных сетях приводят к тому, что ответственным службам проще списать перерасход, чем думать о том, как не допустить его в дальнейшем. Ведь в конечном итоге все эти непродуктивные потери переносятся на потребителя. При этом четкий контроль над расходом воды (газа, тепла), где оператор отвечает за каждый литр или калорию — в интересах потребителя, но он способен существенно осложнить жизнь коммунальным службам. Необходимость внедрения IoT осознается в первую очередь там, где существует рынок с нормальной конкуренцией.

С другой стороны, IoT мог бы помочь в учете расхода воды или газа на стороне абонента — с помощью датчиков можно в режиме онлайн собирать информацию со всех пользовательских приборов учета. Но для этого необходимы «умные» счетчики в каждом доме и квартире. Кто будет оплачивать их установку — вопрос открытый.

Что касается других сфер применения IoT, то подобные системы начинают внедряться, например, в АПК, но вопрос в том, что там не требуется большое количество датчиков и рынок относительно небольшой. Драйвером роста могла бы стать промышленность — там действительно можно развернуться, но украинский индустриальный сегмент пока что настороженно относится к «новомодной» концепции. Отдельные элементы IoT используются в новых многоквартирных жилых домах, ТРЦ, больших магазинах, но здесь сложно отделить «Интернет вещей» от привычной диспетчеризации зданий. Сфер применения IoT еще много — медицина, транспорт, логистика и т.д. Но здесь пока тоже простого интереса гораздо больше, чем реальных внедрений.

ТЕХНОЛОГИИ IoT МОГУТ ПРИНОСИТЬ ПОЛЬЗУ СТРАНЕ УЖЕ СЕЙЧАС

Евгений ЕВТУШЕНКО,
директор по развитию бизнеса DEPS

Рынок IoT в Украине развивается всего несколько лет, но в стране уже доступны решения, которые способны существенно повысить эффективность многих технологических и инфраструктурных систем. По опыту нашей компании могу отметить, что интерес к подобным решениям есть со стороны промышленности, коммунальных служб, организаций социальной сферы. И для всех этих организаций IoT открывает совершенно новые возможности. Возьмем для примера столичную службу газа. В Киеве около 100 тыс. точек мониторинга состояния трубопроводной магистрали, подлежащих периодической проверке. Все это делают люди, вручную – физически обходя каждый пункт. И здесь приходится искать баланс между актуальностью данных и стоимостью, ведь чем более оперативная информация нужна, тем больше сотрудников требуется для мониторинга. В то же время установка датчиков IoT позволяет получать данные со всех точек в режиме онлайн. Да, это потребует разовых вложений, но и постоянные расходы на огромный штат обходчиков можно сократить в разы. Так что если рассматривать стоимость решения в перспективе всего жизненного цикла, то IoT позволяет существенно экономить городской бюджет. Такая же ситуация с водоканалами, теплосетями и другими элементами коммунальной инфраструктуры – точная и оперативная информация, получаемая без участия человека, позволяет избежать непродуктивных расходов во всех смыслах данного понятия.

Но это если речь идет об экономической части, а ведь есть и другие аспекты. Например, социальный – с помощью IoT можно существенно поднять комфорт и безопасность в школах. Скажем, одна группа датчиков позволяет контролировать температуру, влажность и уровень углекислого газа во всех учебных помещениях. Другая отслеживает протечки и теплопотери в подвале. Отдельные сенсоры контролируют санитарные нормы пищеблока и т.д. Это лишь самые простые варианты применения, которых существует великое множество. Но главное, это не «космические технологии» – все это уже работает или может работать в Украине на самых обычных объектах – не только в городах-миллионниках, но и в небольших населенных пунктах. Для последних такие решения даже более актуальны, чем, скажем, для столицы, поскольку за счет автоматизации многих функций, а также возможности централизованного мониторинга и управления, IoT позволяет решить в т.ч. проблему нехватки квалифицированных кадров.

Будущее IoT: 5G, цифровые двойники и «умная пыль»

Как будет развиваться IoT в будущем? Однозначного ответа на этот вопрос не существует, ведь даже сейчас имеется слишком много факторов неопределенности, а в дальнейшем их число может еще увеличиться. Сфера «Интерента вещей» переживает не просто период становления, а скорее всего, проходит лишь его начальную фазу. В то же время вовсе без прогнозов обойтись невозможно. С экономической точки зрения все просто — мировой сегмент IoT будет расти. И дело не столько в конкретных показателях,

IoT В УКРАИНЕ — БОЛЬШИЕ ПЕРСПЕКТИВЫ И МАЛЕНЬКИЙ РЫНОК

Александр СЛЫКОВ,
инженер департамента R&D компании Verna

Рынок IoT в нашей стране находится на начальном этапе развития. В основном можно говорить о каких-то частных применениях коробочных решений на базе того же Xiaomi Mi Smart Home или подобных систем других производителей. В секторе бизнеса это скорее первые шаги, в основном пока нет понимания целесообразности массового внедрения IoT, того, как превратить все это в деньги. Но тем не менее, за последние пару лет отмечен определенный прогресс – если в 2017 году к нам не поступило ни одного запроса касательно IoT, то за последние пол года мы уже реализовали несколько небольших проектов. Плюс несколько на стадии «пилота».

Одно из наиболее успешных внедрений – оснащение системой телеметрии сети продуктовых складов. Производитель продуктов питания столкнулся с проблемой правильного хранения изделий у дистрибьюторов. Дело в том, что в летнее время внутри таких складов нередко нарушается температурный режим, и производитель вынужден удовлетворять большое количество рекламаций от покупателей, при этом часто не понимая, на каком этапе возникают проблемы.

В качестве решения было предложено на каждом складе установить по одной базовой станции LoRaWAN и несколько датчиков температуры/влажности воздуха в разных точках помещения. Благодаря встроенному в шлюз 3G/4G-модему система получила автономную сеть и потребовала лишь электропитания. Информация из разных точек консолидируется на сервере приложений и хранится там в течение нескольких месяцев. Это позволяет контролировать нужные показатели в режиме реального времени, а также выполнять анализ предыдущих периодов.

Кроме того, в системе настроены триггеры, срабатывающие при выходе какого-либо показателя за пределы установленных нормативов. Таким образом, заказчик при относительно небольшом бюджете проекта смог добиться хороших результатов по сохранности своей продукции и уменьшить количество жалоб. Полагаю, что в скором времени таких проектов станет больше, поскольку концепция и возможности IoT становятся все более популярными, а среди пользователей растет осведомленность о ее возможностях. Технология имеет большое будущее в сфере коммунального хозяйства (управление светофорами и наружным освещением, контроль городского транспорта и т.д).

К тому же оборудование становится все более доступным и функциональным, а его использование в условиях постоянно дорожающих энергоносителей может дать огромную выгоду для ЖКХ и энергоемких отраслей промышленности.

сколько в ожиданиях участников рынка — если сейчас кто-то из аналитиков заявит о том, что сегмент «Интернет вещей» сокращается, ему попросту не поверят. При этом сформировать нужную цифру в отчете вовсе несложно — поскольку границы понятия IoT очень размыты, в случае необходимости всегда можно добавить нужный объем того или иного сегмента к общей сумме.

Что же касается технологических аспектов, то здесь ситуация немного более определенная. Во всяком случае, если говорить о перспективе ближайшей пары лет. Например, большинство крупных участников мирового рынка заявляют о том, что они будут использовать (либо уже используют) в сетях IoT элементы «искусственного интеллекта» или машинного обучения. Это вполне логично, поскольку растущая сложность распределенных систем требует гибкого подхода к автоматизации процессов, который обеспечивает ИИ. Хотя в данном случае речь идет не столько об «интеллекте», сколько — если продолжать биологическую аналогию — об «искусственной нервной системе», которая обеспечивала бы эффективное функционирование огромного количества небольших периферийных устройств без непосредственного участия человека.

В индустрии экономически развитых стран уже вовсю применяется концепция «умных фабрик», в основе которой лежит идея т.н. «цифрового двойника» (digital twin) — виртуальная и предельно детализированная модель реального предприятия, благодаря наличию которой можно отслеживать все производственные процессы в режиме реального времени и оперативно вносить изменения в любые из них (**рис. 1**). Причем такая возможность должна присутствовать на каждом этапе жизненного цикла продукции — от разработки до поставки заказчику. Создать такую модель

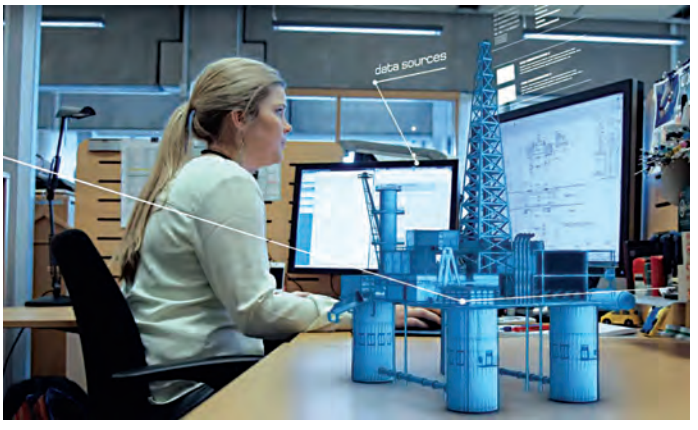

Рис. 1. Визуализация модели «цифрового двойника» (digital twin) для нефтедобывающей платформы

Рис. 2. Эволюция «Интернета вещей» с точки зрения компании IBM

невозможно без развитой сети различных сенсоров и промышленных технологий IoT.

Важным стимулом к повсеместному распространению IoT будет внедрение сетей мобильной связи пятого поколения, которые уже разворачиваются в тестовом режиме многими операторами связи. Принципиальным моментом здесь является то, что технология 5G может обеспечить построение децентрализованных межмашинных сетей мобильного ШПД — когда отдельные устройства обмениваются данными между собой напрямую, а не через централизованную систему, например, базовую станцию (**рис. 2**).

Такие технологии были доступны и ранее, но только 5G позволяет организовать передачу данных на достаточно высокой скорости (гигабиты в секунду) при сохранении ультракомпактного формата и низкого энергопотребления приемопередатчиков. Все это открывает совершенно новые перспективы перед системами «Интернета вещей», в первую очередь в вопросах обеспечения автономности работы и радиуса действия сетей. В свою очередь децентрализованная структура сети сама по себе располагает к внедрению технологии блокчейн — о потенциале ее применения в системах IoT нового поколения (использующих 5G) говорят все чаще.

Собственно отсутствие нормальной технологической базы для децентрализованных вычислений считалось одним их крупных препятствий на пути глобального внедрения «Интернета вещей». Миллиарды IoT-устройств, работающих в мире, формируют огромный поток данных, передавать которые по общим Интернет-каналам все сложнее, более того — это непродуктивно, поскольку во многих случаях требуется только локальное взаимодействие элементов системы, например, датчиков. Такая же ситуация и с обработкой данных — загружать их все в облака и затем получать оттуда, по сути, дорого и медленно. Сейчас данная проблема не ощущается слишком остро ввиду того, что рынок только начал развиваться, но по мере появления новых проектов децентрализация сетей будет попросту безальтернативным вариантом.

Для следующего этапа эволюции IoT уже готовы такие термины, как «туманные вычисления» (fog computing) и даже «умная пыль» (smart dust), и это реальное будущее «Интернета вещей».

Игорь КИРИЛЛОВ, **СиБ**

IoT ИЛИ WoT?

Термин Internet of Things (IoT), несмотря на свою популярность, все еще не обрел четкого и общепринятого определения. Например, IDC описывает его как «сеть сетей с уникально идентифицируемыми конечными точками, которые общаются между собой в двух направлениях по протоколам IP и обычно без человеческого вмешательства». Определение Gartner не менее абстрактное: «сеть физических объектов, которые имеют встроенные технологии, позволяющие осуществлять взаимодействие с внешней средой, передавать сведения о своем состоянии и принимать данные извне». Более конкретно рамки IoT определяет консалтинговая компания McKinsey, по мнению которой это: «датчики и приводы (исполнительные устройства), встроенные в физические объекты и связанные через проводные или беспроводные сети с использованием протокола IP, который «связывает» Интернет».

В то же время само название явления содержит определенное противоречие. Ведь Интернет – это вполне конкретная сеть передачи данных, в основе которой лежит стек протоколов TCP/IP. Что по ней будет передаваться – межмашинная информация, тексты или голосовые данные – уже вторично. В данном случае более корректным, очевидно, будет термин «паутина вещей», или Web of Things (WoT). Об этом косвенно свидетельствует тот факт, что в рамках Консорциума Всемирной паутины (World Wide Web Consortium или W3C) работает отдельная группа Web of Things Interest Group, которая трудится, пока не особенно успешно, над соответствующими стандартами. Тем не менее в широком смысле термин WoT вряд ли обретет популярность, ведь IoT – это уже узнаваемый «бренд», скорее выражающий идею, чем определяющий технологические особенности.