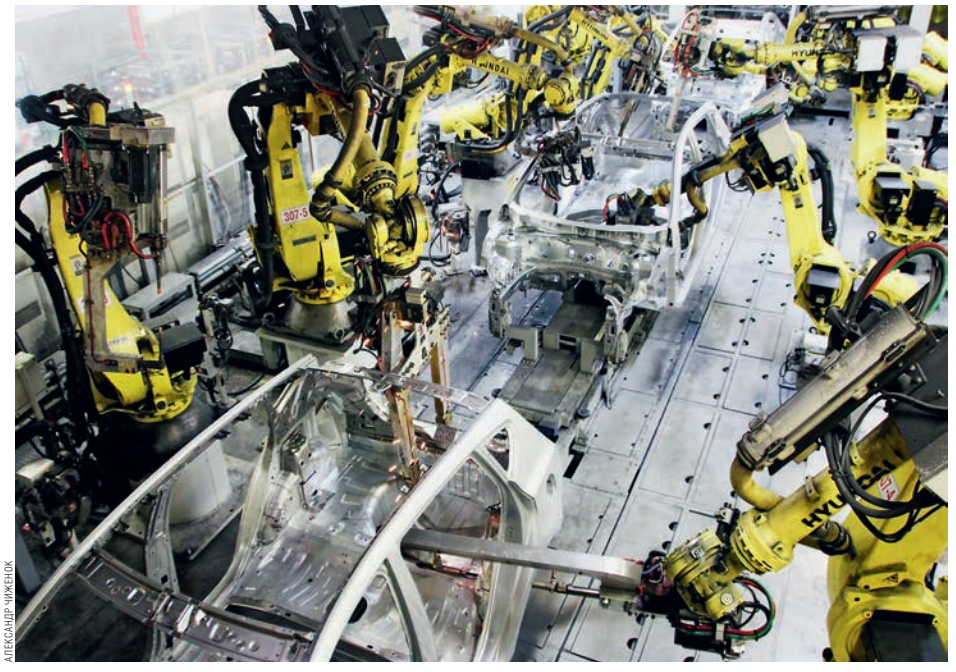
ТРЕНД В ПРОМЫШЛЕННОМ МАСШТАБЕ

ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ВЕЩЕЙ ИЛИ INDUSTRIAL INTERNET OF THINGS (IIOT) — ОТВЕТВЛЕНИЕ ОТ ОСНОВНОГО ИНТЕРНЕТА ВЕЩЕЙ, ЕГО ЧАСТЬ, ИСПОЛЬЗУЕМАЯ В ПРОИЗВОДСТВАХ РАЗЛИЧНОГО ТИПА, ДОБЫЧЕ ПОЛЕЗНЫХ ИСКОПАЕМЫХ, ГЕНЕРАЦИИ И РАСПРЕДЕЛЕНИИ ЭЛЕКТРОЭНЕРГИИ. В ОБЩЕМ, ВО ВСЕХ СФЕРАХ, ГДЕ НЕ ЗАДЕЙСТВОВАНЫ МАССОВЫЕ ПОТРЕБИТЕЛИ. СЧИТАЕТСЯ, ЧТО ИМЕННО IIOT — ДВИЖУЩАЯ СИЛА ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ. СВЕТЛАНА РАГИМОВА

По мнению исследователей Machina Research, глобальный рынок индустриального интернета вещей достигнет €484 млрд в 2025 году. Главными отраслями, которые будут генерировать выручку в этой сфере, будут транспорт, промышленность, ЖКХ, здравоохранение и новый сегмент под названием «умный дом». Сегодня интернет вещей наиболее распространен в транспорте и логистике, энергетике и ЖКХ, потребительском секторе и медицине, но в ближайшей перспективе деятельность всех индустрий будет связана с подключением к сети. Согласно статистике Ericsson, 75% компаний в мире уже проявляют активный интерес к внедрению технологических решений в области интернета вещей. Почти все (94%) опрошенных уверены, что эти технологии вызовут изменения в различных отраслях и рынках в ближайшие три года.

Александр Колычев, ведущий разработчик решений в области мобильного широкополосного доступа Ericsson в Северной Европе и Центральной Азии, говорит, что интернет вещей может не только повысить эффективность работы различных индустрий, но также представить абсолютно новые бизнес-модели, которые никогда раньше не использовались в традиционных отраслях. Таким образом, постепенно исчезает четкое разделение между индустриями, все сферы жизни современного человека будут объединены в рамках единой сети. Интернет вещей не обойдет стороной ни одну индустрию. Новые технологии приведут к полному пересмотру текущих продуктов и предложений.

Марат Матевосян, генеральный директор «Волгабурмаша», объясняет, что такое промышленный интернет вещей сегодня: «Поскольку термин IoT описывает большое количество разнообразных технологических решений от простейших RFID и до сложных роботизированных систем, работающих без человека, таких как буровые установки, шахты или целые заводы, сложно назвать отрасли, в которых не используется IoT. Гораздо сложнее выделить те отрасли, где уже удалось получить осязаемый экономический эффект от внедрения IoT-технологий. В настоящее время используется до 15% данных, получаемых с помощью IoT. В случае с вышеупомянутой буровой вышкой используется всего 1% данных. Нет пока эффективных алгоритмов применения столь больших объемов данных, поэтому подавляющее большинство IoT-технологий позволяют быстро получать информацию о каком-либо факте, но гораздо реже



АЛЕКСАНДР ЧИЖЕНОК

НА ФАБРИКАХ БУДУЩЕГО НЕ БУДЕТ ЛЮДЕЙ

они могут предвидеть, оптимизировать и тем более принимать самостоятельные решения».

Александр Колычев рассказывает, что у Ericsson есть опыт работы в области IIoT с совершенно разными рынками: «В нефтегазовой отрасли многие компании внедряют у себя технологии „умного“ месторождения, в ЖКХ нарастает применение „умных“ счетчиков, а городское автомобильное движение оптимизируется благодаря интеллектуальным технологиям управления транспортными системами. В любом из этих сценариев главным преимуществом у компаний-пионеров станет снижение капитальных расходов и повышение эффективности работы».

Основные на сегодняшний день сценарии использования технологий IIoT — smart metering («умные» электросети) и удаленное управление различным оборудованием, например роботами на фабриках, погрузчиками и прочим транспортом. В будущем промышленное применение интернета вещей позволит оптимизировать работу предприятия во всех аспектах. Система «умной» фабрики подразумевает оцифровку и объединение в сеть всех этапов производственного процесса. В таком сценарии сеть предприятия не должна быть «вещью в себе», у нее будет доступ к внешней макросети, что позволит использовать промышленные приложения из облака, удаленную обработку данных и централизацию информации, получаемой из территориально-распределенных производств.

К примеру, компания Ericsson построила лаборатории, демонстрирующие, как работает такой подход, на двух предприятиях в Италии. Роботы в лабораториях оснащены примитивными сенсорами и актуаторами. Системы обработки информации и навигации роботов размещены в облаке, соединение к которому устанавливается через мобильную сеть или при необходимости по Wi-Fi. Система «умного» управления фабрикой выдает приоритет и контролирует выполнение роботами задач, и они перемещаются по лаборатории, избегая столкновений с объектами и людьми при помощи обработки в облаке данных с установленного на них лидара. При этом всегда можно удаленно получить статус каждого конкретного робота, изменить его программу. «Такой сценарий использования можно экстраполировать и на реальное производство, когда благодаря интернету вещей фабрика будет управляться с максимальной эффективностью»,— рассказывает Александр Колычев.

Александр Герасимов, руководитель департамента ИТ и облачных сервисов J'son & Partners Consulting, говорит, что некоторые проекты в области IIoT уже ведутся в России и связано это с новой технологической политикой и сменой бизнес-модели глобальных производителей промышленного и технологического оборудования. «Они переходят на контракты жизненного цикла, в том числе и в России, что требует реализации совершено иного качества телеметрии, уже на принципах IIoT. Поэтому современное импортное промышленное оборудование уже частично подключено к облачным платформам IoT, таким как Predix для мониторинга фактического состояния турбин и других дорогостоящих элементов. Есть примеры, когда производственные линии, например, в пищевой промышленности также подключаются к платформам IoT для реализации предиктивного управления техническим состоянием оборудования»,— приводит примеры он.

По мнению Марата Матевосяна, в России в первую очередь будут внедряться недорогие и отработанные решения, эффективность которых уже апробирована в развитых странах: «Я бы выделил логистику как внешнюю, так и внутреннюю, а также системы, сигнализирующие о предстоящем ремонте сложных технических устройств (буровые установки, прокатные станы, энергетические объекты, станки)».

Юрий Пуха говорит, что пока сложно сказать, кто именно будет зарабатывать на IoT. По его словам, это будут прежде всего те компании, которые своевременно инвестируют в компетенции, развитие технологий и платформ, а также в экосистему. «Пока как на Западе, так и в РФ не вырисовались четкие лидеры данных направлений. В мире аналитики считают, что наибольший потенциал у производителей оборудования — в основном за счет R&D-возможностей и возможностей объединить стартапы и компании в экосистему. Но рынок не закрыт для других игроков — при правильных инвестициях возможны успешные выходы для операторов связи и индустриальных игроков»,— считает Юрий Пуха. ■

> СКВОЗЬ КРОТОВУЮ НОРУ

Один из острых вопросов, который важно решить в IIoT,— обеспечение информационной безопасности. Сбои в работе электростанций, индустриальных предприятий и критической инфраструктуры могут вызвать серьезные последствия и затронуть множество людей. МИША ДОЛЕР, глава Центра по изучению телекоммуникаций Университетского колледжа в Лондоне, рассуждает о кибербезопасности на страницах британской версии журнала WIRED.

ERICSSON

Безопасность в мире интернета вещей похожа на тему изменения климата: мы знаем, что необходимо действовать, чтобы избежать катастрофы в долгосрочной перспективе, но мы не знаем, как к этой задаче подступиться. «Вещь» в IoT — это что-то маленькое, часто вообще невидимое, с не слишком мощным процессором и небольшим объемом памяти. Таких «вещей» очень много, и люди не будут проверять их годами.

Физические характеристики IoT-устройств ведут к большому количеству вопросов, которые необходимо решить. Если их никто не проверяет, то как мы можем быть уверены, что к ним никто не подключается? Вандалоустойчивый дизайн должен стать более инновационным и превратиться в мейнстрим, тогда у нас будет уверенность, что мы контролируем свои устройства и данные. Вдобавок к этому такие устройства обычно не имеют физического пользовательского интерфейса. Как в таком случае мы можем ими управлять или, например, отключать в случае необходимости?

Но действительно сложный вопрос, однако, касается беспроводных коммуникаций. Множество IoT-устройств передают очень маленькие объемы информации. В действительности, размеры пакетов могут быть настолько малы, что некоторые наши фундаментальные алгоритмы криптозащиты не могут для них использоваться. Если вам кажется, что передача данных с измерительных датчиков может вызвать определенные сложности, то представьте, какие проблемы с безопасностью мы получим при даунстриме — обратном взаимодействии. Например, когда центр управления будет подключен к актуаторам, дронам, роботам.

По мере распространения IoT разработчики и вся экосистема кибербезопасности должны адаптироваться. Хакерам придется освоить новые навыки. Но из-за того что появится гораздо больше уязвимостей, они будут находить их быстрее и легче, что будет вести к хаосу. Антивирусным компаниям также придется переизобрести себя заново. На такие устройства с небольшим объемом памяти просто невозможно будет предустанавливать антивирусные программы. Мы пока видели не так много IoT-атак, но не из-за того, что система хорошо защищена, а потому, что просто еще в мире функционирует не слишком большое число устройств. И еще меньше хакеров, которые специализируются на IoT. Но когда IoT начнет обретать реальную ценность, нам лучше бы обеспечить безопасность, причем на глобальном уровне.

Ах да, упомянул ли я квантовые компьютеры? Когда они будут запущены в массовую эксплуатацию, а это случится в недалеком будущем, они легко смогут взломать любые наши традиционные шифры. Я уверен, что мы разработаем «заплатку». Но то, чего я не могу представить,— это то, что кто-то будет заниматься ремонтом триллионов IoT-устройств, которые выпущены, чтобы работать десятилетиями. Это те же самые устройства, которые управляют светофорами, кардиостимуляторами, тормозными системами автомобилей, поставкой топлива на атомные электростанции.