DOI: 10.22184/1992-4178.2018.174.3.156.168

Проблемы и перспективы развития промышленного Интернета вещей

М. Макушин[1], В. Мартынов, д. т. н.[2]

УДК 621.391:004.738.5 | ВАК 05.13.00

Интернет вещей (Internet of Things, IoT) находит широкое применение в промышленности и сельском хозяйстве. На самом деле Интернет вещей – это не «технология», точнее, не совсем технология, так как строится на основе большого количества других технологий. Это – бизнес-модель, предполагающая извлечение стоимости из полученных данных, упрощение и ускорение рабочих и управленческих процессов благодаря межмашинной передаче данных. В составе IoT выделяются многочисленные специализированные направления, в частности промышленный Интернет вещей (Industrial Internet of Things, IIoT). Последствия внедрения IIoT намного значительнее, чем приложений IoT, ориентированных на потребителя. IIoT-факторы производства охватывают критические сферы человеческой деятельности, где отказ систем недопустим.

СТРУКТУРА И РАЗВИТИЕ IoT

Исследовательская фирма IHS Markit (Лондон, Великобритания) выделяет четыре этапа освоения и внедрения IoT-решений. На первом этапе («Подключаемость и внедряемость») создается инфраструктура, определяются набор и типы подключаемых к сети устройств. На втором этапе («Сбор данных») обеспечивается развертывание и наращивание количества датчиков и запоминающих устройств, позволяющих собирать данные об окружающей среде, работе машин, оборудования и т. п. При этом значительное внимание должно уделяться безопасности передачи данных. Третий этап («Вычисления») предполагает начало обработки и анализа больших объемов данных, генерируемых IoT-приборами, четвертый этап («Созидание») – монетизацию IoT-системы и / или создание уникальных решений на основе трансформационных данных. Вариантов монетизации много, например, IIoT-решение на основе анализа данных о состоянии машин и оборудования позволяет формировать реальные планы технического обслуживания. В результате более быстрыми темпами растет производительность производства благодаря сокращению времени незапланированных простоев машин и оборудования (внеплановый ремонт и т. п.) и облегчается переналадка производства для выпуска продукции по требованию потребителей, что обеспечивает повышение уровня конкурентоспособности [1].

Каковы перспективы развития IoT? По данным IHS Markit, глобальная установленная база IoT-приборов увеличится с 27 млрд шт. в 2017 году до 73 млрд шт. в 2025-м (рис. 1). Эта тенденция будет характерна для всех вертикально-организованных отраслей, которые охватывает IoT.

Чем обусловлен подобный рост? В частности, действием в полупроводниковой промышленности так называемого закона Мура (удвоение числа транзисторов на кристалле ИС каждые 18 месяцев без увеличения удельной стоимости функции для конечного пользователя). Этим обусловлено долгосрочное снижение цен на ИС. Так, в 1992 году модуль Bluetooth стоил 50 долл., а сегодня носимые человеком приборы оснащены как минимум двумя модулями Bluetooth стоимостью менее 50 центов каждый. Основой IoT являются датчики, собирающие и передающие информацию для обработки, использования и хранения. При этом зачастую датчики, блоки и приборы IoT не требуют стационарного электропитания благодаря технологии сбора / преобразования энергии* [2].

По оценкам аналитической фирмы IDTechEx, с 2018 года промышленность будет уделять большое внимание стандартизации IoT и развертыванию / тестированию опытно-экспериментальных сетей с его использованием. Так, на зимних Олимпийских играх в Южной Корее демонстрировалась технология связи 4,8G, которая для простоты названа 5G.

Переосмысление подходов к развертыванию и использованию IoT

Согласно последним прогнозам экспертов, IoT приобретет огромный размах – миллиарды устройств, триллионы

[1] АО «ЦНИИ «Электроника», mmackushin@gmail.com.

[2] ФГБНУ «Аналитический Центр», Минобрнауки РФ, профессор.

* **Energy harvesting (= power harvesting / energy scavenging)** – сбор / преобразование энергии. Процесс, при котором энергия, получаемая из внешних источников (солнечная, тепловая энергия, энергия ветра, перепад солености воды, кинетическая энергия), поглощается и хранится для малых беспроводных автономных приборов, наподобие используемых в носимой (вмонтированной в одежду / аксессуары) электронике и беспроводных сенсорных сетях.

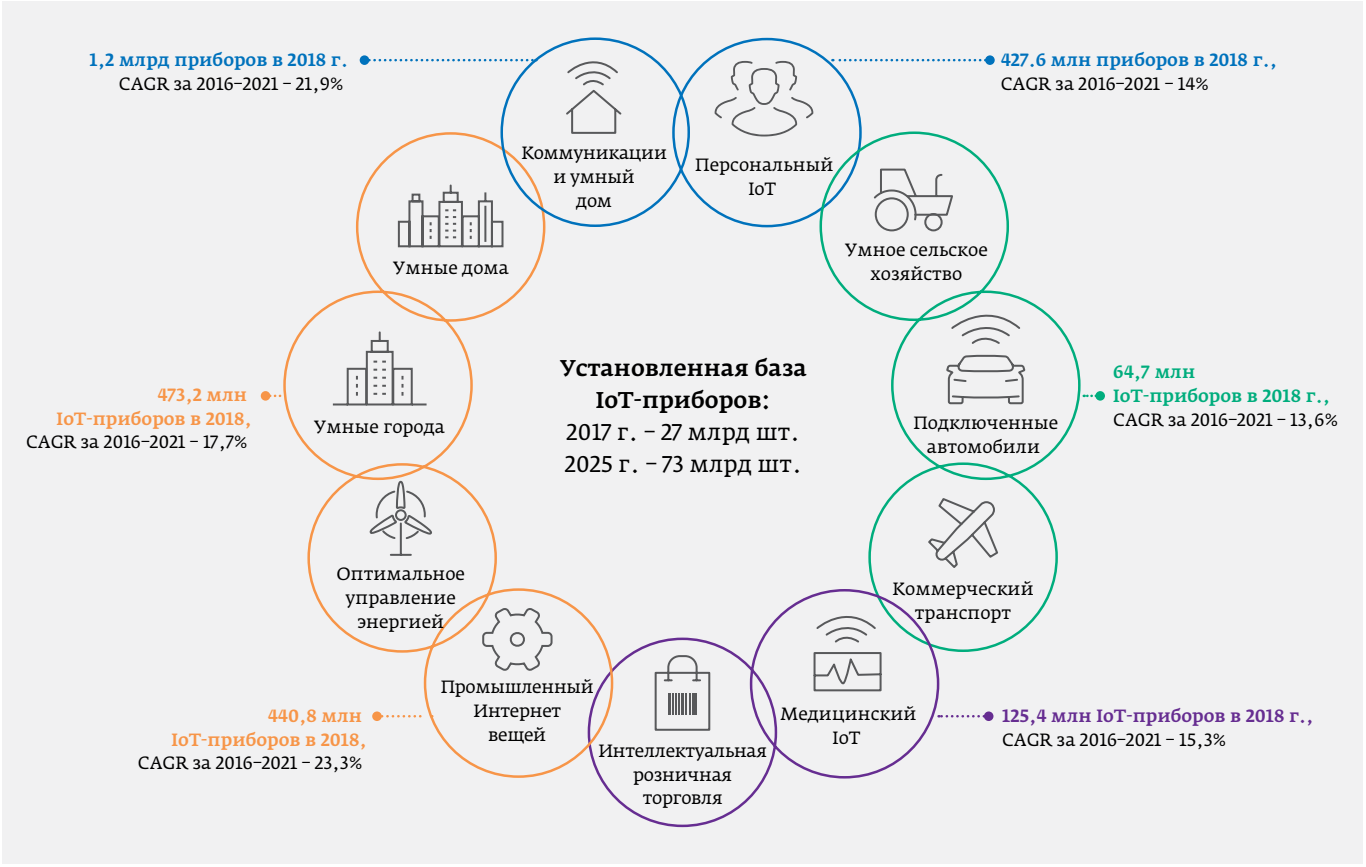

Рис. 1. Структура IoT, интеграция вертикально-организованных отраслей, объем отгрузок и CAGR на 2016–2021 годы.
Источник: https://cdn.ihs.com/www/pdf/Top-8-in-2018-Whitepaper.pdf

долларов прибыли. Однако для этого требуется не только технология, но и другой подход к ней, а также понимание того, как использовать все больший объем данных.

Данные полезны только тогда, когда они понятны всем и предоставляются клиентам, сотрудникам, потребителям в нужный момент времени. Желающие использовать IoT должны иметь четкое представление о том, как добиться устойчивого спроса. Для этого обычно требуется аналитика больших данных, и этот сегмент рынка стремительно развивается. Сочетание IoT и технологии больших данных* создает новые предпосылки для ускоренного развития и увеличения доходов.

Не менее важно понимать, что является Интернетом вещей, а что – нет. IoT представляет собой не единую технологию, а много крупных направлений, для дальнейшего развития которых нужна стандартизация, что требует совместных усилий большого числа заинтересованных организаций. При этом важно использовать открытые исходные коды.

С точки зрения потребителя IoT – это новый уровень удобства и комфорта в повседневной жизни. За

* **Big Data** – большие данные, в информационных технологиях серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объемов и значительного многообразия для получения человеко-читаемых результатов, эффективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети, сформировавшихся к началу 2010-х годов, альтернативных традиционным системам управления базами данных и решениям класса Business Intelligence.

всем этим стоит цепочка поставок и датчики как базовая основа. В конечном итоге IoT можно рассматривать как формирование сообщества и создание «зеленого мира».

IoT хорошо дополняет концепцию интеллектуального дома, управление которым осуществляется одним движением пальца. Человек отправляется утром на прогулку или пробежку, а к моменту его возвращения домой в определенное время включается душ с нужной температурой воды, готовится кофе (завтрак), сменная одежда. Автомобиль «знает», сколько времени нужно хозяину на сборы, и самостоятельно заводится для поездки по делам / на работу. Все сводится к удобству.

Таким образом, основное преимущество IoT в бесшовной связанности различных сфер жизнедеятельности человека. При этом речь идет не только об индивидуальных устройствах, а обо всех приборах, с которыми контактирует человек. Это уже не только удобство, но и экономия времени, других ресурсов [3].

IIoT: ОБЩИЕ ПОЛОЖЕНИЯ

Промышленный Интернет вещей отличается своими объемами и целями. В первую очередь это оптимизация производственных процессов предприятия, сокращение простоев оборудования, экономия различных ресурсов, управление качеством, поддержание безопасного режима работы и т. п. Кроме того, в этот перечень входят взаимодействие с поставщиками и клиентами по вопросам своевременности поставок, обеспечения качества продукции; анализ хозяйственной деятельности предприятия на базе собственного или облачного центра обработки и хранения данных (ЦОД) с использованием технологии больших данных; взаимосвязь с другими ЦОД и т. д.

Промышленный Интернет вещей – это не только заводы и автоматизированное производство, но и коммерческое использование, крупные коммерческие здания и торговые центры. Важными составляющими технологии промышленного Интернета вещей (как и других секторов Интернета вещей) являются передача данных в масштабе реального времени и масштабируемость беспроводных сетей датчиков.

Каковы основные факторы повышения спроса на IIoT?

Первый – подключаемость, технологичность и инновационность. Промышленные сегменты, такие как энергетика, генерируют огромные массивы данных. Технологии накопления и анализа открывают новые возможности их оптимизации и монетизации. **Второй** – стандартизация и безопасность. Промышленность нуждается в общих стандартах, позволяющих взаимодействовать интеллектуальным продуктам подключения, машинам и оборудованию различных поставщиков. В рамках промышленного использования облачных вычислений особенно важно обеспечить безопасность передаваемых и хранимых данных, не допустить несанкционированного доступа к данным, системам управления и т. п. **Третий** фактор – бизнес-модели. Промышленные предприятия испытывают трудности, обусловленные потерей инженерно-технического опыта из-за выбывания рабочей силы (переход к конкурентам, на другую работу, выход на пенсию и т. п.). Новые бизнес-модели возникают в результате деятельности машиностроителей, поддерживающих заказчиков, связанных с IIoT-услугами (т. е. дистанционный мониторинг и обслуживание машин и оборудования). **Четвертый** фактор – инновационность

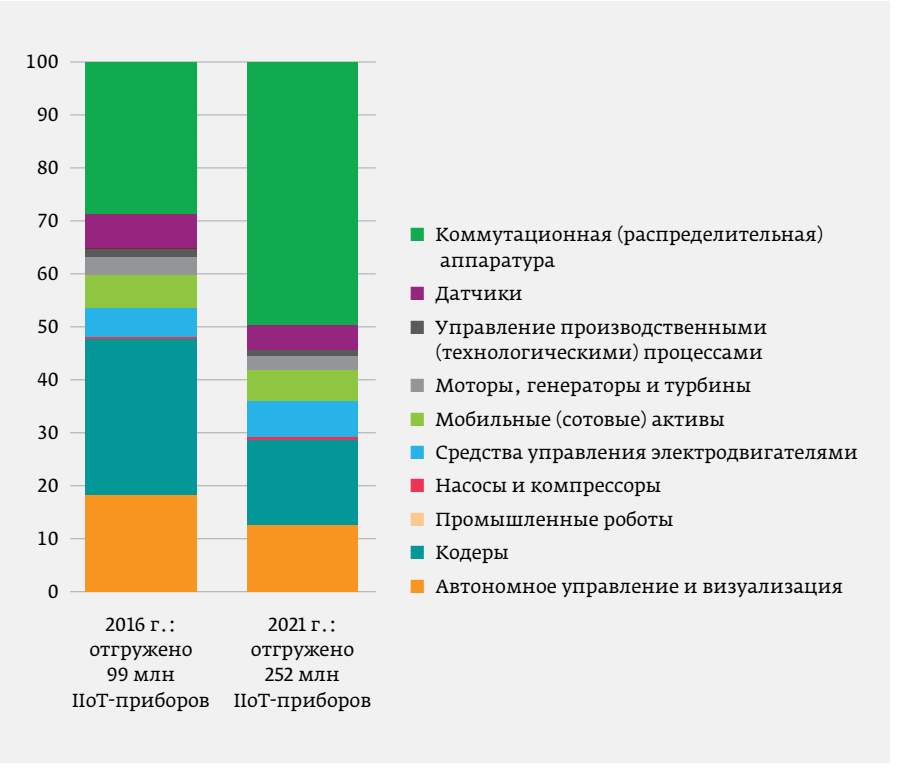

Рис. 2. Структура отгрузок IIoT-датчиков для приборов и систем различного типа в 2016 и 2021 годах. *Источник: https://cdn.ihs.com/www/pdf/IHS-Markit-IoT-and-Industrial-ebook.pdf*

и конкурентоспособность. По мере освоения и расширения использования IIoT возможно ускорение темпов роста производительности производства и повышение уровня конкурентоспособности.

Развитие IIoT обеспечивается на основе датчиков для самого разнообразного оборудования, приборов и систем, которые все шире используются в производственной среде. Фактором развития IIoT является способность сенсоров к подключению, передаче все больших объемов данных с возрастающей скоростью. По оценкам отраслевых специалистов, отгрузки датчиков в период 2016–2021 годов увеличатся более чем в 2,5 раза (рис. 2).

Рис. 3. Стадии освоения IIoT некоторыми вертикально-интегрированными отраслями. *Источник: https://cdn.ihs.com/www/pdf/IHS-Markit-IoT-and-Industrial-ebook.pdf*

Темпы освоения IIoT в вертикально-организованных отраслях различаются (рис. 3) в зависимости от открытости каждой отрасли к использованию технологий IIoT, а также от совокупности знаний, консерватизма, доступа к капиталу и проблем интеграции. Последствия внедрения IIoT намного значительнее, чем приложений IoT, ориентированных на потребителя [4].

ТЕНДЕНЦИИ РАЗВИТИЯ И ИННОВАЦИИ В ОБЛАСТИ IIoT

Основных тенденций развития IIoT несколько. Во-первых, специализированные проекты будут заменяться стандартными решениями. Во-вторых, IIoT во все большей мере становится катализатором цифровой трансформации (цифровизации) всех направлений повседневной жизни. В-третьих, машины и оборудование

будут поставляться в состоянии готовности к применению в среде IoT. В-четвертых, по мере развития IIoT модели ценообразования и потребления будут упрощаться. Рассмотрим эти тенденции подробнее.

Стандартные решения взамен специализированных

Большинство ранних IoT-реализаций относились к разряду специализированных проектов, поэтому системный интегратор или провайдер услуг должен был определять область применения, проектировать и управлять реализацией проекта. По мере распространения IIoT промышленность будет рассчитывать, что используемые системы «просто работают». Другими словами, если работу корпоративных систем нужно поддерживать с точки зрения Интернета и обеспечения данными, то в будущем функционал корпоративных систем должен обеспечиваться средствами IIoT. По всей видимости, доступ к IoT станет возможен в рамках корпоративных систем или использования технологии IoT для построения систем, обеспечивающих наращивание ценности бизнеса. Рынок IoT-платформ и компонентов сохранится, но станет менее заметным для пользователя.

По оценкам журнала The Manufacturer, платформы IIoT или компоненты для приложений предлагают уже более 350 провайдеров. При этом при создании полного решения они зачастую полагаются на свою экосистему партнеров. В большинстве случаев партнеры предоставляют IoT-приборы, облачные вычисления и хранилища, краевые вычисления, корпоративные приложения, общее управление проектами или системную интеграцию. Если облачные вычисления (cloud computing) уже широко известны, то краевые (пограничные или туманные) вычисления (edge, fog / fogging computing) – явление новое. Это метод оптимизации облачных вычислительных систем путем дополнения обработки данных в облаке обработкой на границе сети (облака) вблизи источника данных. Данный подход позволяет снизить объем трафика между датчиками и ЦОД, генерировать данные в источнике или вблизи него. Иными словами, вычислительная нагрузка на ЦОД снижается, поскольку краевые приборы передают не весь объем данных, а только первично обработанные. Метод требует использования ресурсов, не подключенных к сети постоянно (ноутбуки, смартфоны, планшетные ПК, датчики и т. п.). Следует отметить, что облачные и краевые вычисления не антагонисты, а взаимодополняющие и расширяющие возможности друг друга концепции.

В краткосрочной перспективе прогнозируется появление предложений с расширенными аналитическими возможностями и связанных с ними интегрированных услуг. Больше внимания будет уделяться обеспечению безопасности передачи данных типа «прибор – облако», а процессу слияний / поглощений на рынке IIoT.

В долгосрочной перспективе ожидается:

- появление интегрированных услуг дополненной реальности (augmented reality – технология, накладывающая изображения, сгенерированные компьютером / вычислительным устройством, на реальный мир, который видит пользователь, то есть augmented reality предоставляет смешанную картину);
- снижение стоимости основных функций управления приборами в целях увеличения продаж в области аналитики и автоматизации бизнес-процессов;
- превращение IIoT-услуги как платформы (PaaS, platform as a service) в часть стандартного корпоративного ИТ-портфеля, наравне с CRM (Customer Relationship Management – система управления взаимоотношениями с клиентами – прикладное ПО для автоматизации стратегии взаимодействия организации с заказчиками) и ERP (Enterprise Resource Planning – интегрированная система планирования и управления ресурсами предприятия).

PaaS относительно новая услуга, потребитель получает доступ к информационно-технологическим платформам, таким как ОС, СУБД, связующее ПО, средства тестирования и разработки облачного провайдера. Вся информационно-технологическая инфраструктура, включая серверы, вычислительные сети, системы хранения, управляется провайдером, определяющим набор доступных заказчику платформ и параметров. Потребителю предоставляется право использовать платформы, создавать их виртуальные экземпляры, разрабатывать, инсталлировать, тестировать, эксплуатировать на них прикладное ПО, динамически меняя количество нужных вычислительных ресурсов. Плата взимается в зависимости от уровня потребления. Тарификация возможна по объему обрабатываемых данных, времени работы приложений, количеству транзакций, сетевому трафику. Экономический эффект провайдера достигается за счет экономии на масштабах, когда из множества потребителей в одно и то же время только часть их активно использует вычислительные ресурсы. К этому же виду услуг можно отнести использование виртуализации [5].

IIoT КАК КАТАЛИЗАТОР ЦИФРОВОЙ ТРАНСФОРМАЦИИ

С помощью IIoT можно трансформировать промышленные предприятия в полностью компьютеризированные,

высокоавтоматизированные, а в некоторых областях и автономные структуры.

Например, фирма CNH Industrial изготавливает интеллектуальные подключаемые продукты как часть портфеля потребительских предложений. Продукты, предназначенные для мониторинга производительности клиентского оборудования, интегрируются с основными корпоративными бизнес-системами, такими как ERP и CRM.

На ганноверской выставке в апреле 2017 года IoT операционная система Mindsphere (Siemens) стала центральным элементом презентаций нескольких фирм-партнеров с использованием «цифровых двойников»* в целях оптимизации разработки и развития продуктов, управления производством и повышения производительности оборудования / эксплуатационных характеристик продукции в процессе производства. Концепция новых способов работы и понимания производительности подключенных устройств поддерживается средствами аналитики данных (для поддержки рабочих процессов). Siemens также признает возможность локальных преобразований – например облачной поддержки системы SCADA (Supervisory Control And Data Acquisition – гибкая автоматическая система управления производством) в автоматизированных системах, или интеграции локальных серверов пограничных вычислений в целях соблюдения все более жестких требований ко времени ожидания.

Предложения корпорации IBM отличаются от предложений конкурентов тем, что возможности в сфере облачной поддержки IoT сочетаются с когнитивно-вычислительными возможностями. В IoT-платформе Watson объединены функции обработки естественного языка, машинного обучения, а также анализа изображений и текста. Соответственно, это оптимальное решение для IoT-проекта, предусматривающего голосовое управление продуктами на этапе эксплуатации.

Фирма PTC наряду с решением Thingworx для ПО IoT предлагает технологию дополненной реальности, предназначенную для расширения взаимодействия с подключенными устройствами. Смартфон или планшет оператора может добавлять информацию в видеопоток продукта или демонстрировать показания датчиков, результаты анализа и наложения инженерных деталей.

Машины и оборудование будут поставляться в состоянии IoT-готовности

Корпоративные системы во все большей степени будут способны находить IoT-приборы, устанавливать соединение и управлять ими. Например, немецкая фирма Kaeser уже поставляет воздушный компрессор Sigma Air Manager 4.0 в виде законченного IoT-решения для составления графика технического обслуживания согласно текущему состоянию (на основе прогнозирования запаса надежности).

Безопасность станет основным требованием

В настоящее время только 31% производителей (менее трети!) рассматривают кибербезопасность как один из высших приоритетов. В прессе уже неоднократно сообщалось о том, что системы IoT взломаны или поставлены под угрозу. Например, в результате атаки червя Mirai были взломаны по причине уязвимости различные подключенные к сети предметы повседневного пользования (цифровые видеомагнитофоны и камеры) для их повседневного выхода в автономном режиме на сайты таких корпораций, как Amazon, Netflix, Twitter, Spotify, Airbnb и PayPal, чтобы добиться отказа в обслуживании клиентов этих фирм.

Вскоре компании, выпускающие IIoT-продукты и услуги, начнут предлагать надежные средства безопасности: например, такие как AWS, используемые в IoT-платформах Rachio и Azure, предоставленных фирме Rolls-Royce корпорацией Microsoft.

Безопасность должна быть заложена в конструкцию на каждом уровне, что уже осуществляют производители микропроцессоров – ARM и Intel. В сетях поставок для обеспечения безопасности, а также для контроля за перемещением каждой партии товара (от отгрузки со склада до конечного потребителя) будут использоваться решения на основе блокчейн, примером может служить ряд супермаркетов, включая Walmart.

* **digital twin** – цифровой двойник, то есть система моделирования, которую заказчик может использовать в своих целях. Модель цифрового двойника на современном уровне (конец 2017 года – начало 2018-го) обеспечивает наличие элементов искусственного интеллекта, возможности машинного обучения и анализа сопутствующего ПО.

Упрощение моделей ценообразования и потребления

Фирмы, получающие IoT-решения через своих поставщиков корпоративных систем, перейдут к моделям ценообразования и потребления на основе уже знакомых им принципов. Фирмы, использующие IoT-решения для формирования корпоративных систем, обеспечивающих ценности бизнеса, также найдут пути выгодного ценообразования.

Итак, IIoT обеспечивает реальную ценность для широкого круга предприятий в большинстве отраслей. Начать работу с IoT-решениями будет все проще, способ выбирается в зависимости от внутренних ИТ-возможностей фирмы – потребителя IIoT-решений. Прогнозировать, кто останется в числе основных провайдеров через пять-десять лет, пока невозможно – хотя у большинства крупных современных провайдеров шансы есть [5].

ИНФРАСТРУКТУРА IIoT

К достаточно разнообразной инфраструктуре IIoT можно отнести системных интеграторов, поставщиков основных средств и мобильных активов, комплектующих, платформ, всевозможных услуг, облачных технологий (включая облачный хостинг), а также стандарты, например, промышленный Ethernet, промышленные шины, стандарты связи (от Bluetooth до Z-Wave). Кроме того, в состав инфраструктуры IIoT входят специализированные промышленные альянсы, занимающиеся вопросами данной технологии. Наконец IIoT-инфраструктура охватывает некоторые фирмы в смежных вертикально-организованных отраслях, которые пользуются IIoT-услугами или планируют освоить эту технологию.

Инфраструктура IIoT уже несколько раз с различной степенью подробности описывалась рядом исследовательских фирм. Один из последних примеров представлен в феврале 2018 года исследовательской фирмой IHS Markit (табл. 1) [4].

ВОПРОСЫ ЗАЩИТЫ ДАННЫХ В IIoT

По мере развития информационно-коммуникационных технологий не только повышается эффективность экономики, но и обостряются проблемы в области безопасности и защиты данных. Использование хакерских атак и вредоносных программ против возможных конкурентов становится повседневной практикой. Соответственно, повышается роль и значимость специалистов / служб информационной безопасности. В этом плане представляет интерес опыт немецких и японских фирм.

Несмотря на длительное сотрудничество, эти компании по-разному подходят к освоению IIoT, в частности в целях повышения производительности труда. Германия, стремясь удержать положение лидера, делает упор на обеспечение защиты данных в рамках концепции Industry 4.0*. Японские специалисты в большей мере склоняются к решению задач автоматизации и роботизации производства.

Во многих случаях корпоративные клиенты готовы использовать IIoT для повышения эффективности производственных / деловых процессов. IIoT обеспечивает значительную экономию времени при принятии управленческих решений, планировании текущей и перспективной деятельности. Однако сегодня наиболее существенной проблемой использования IIoT остается уязвимость от хакерских атак. Подобные атаки не всегда определяются по источнику происхождения, так как одна из главных задач их авторов – скрытность.

Многочисленные примеры кибератак приводят к выводу: все уровни инфраструктуры IIoT должны быть защищены (рис. 4).

Отмечая достоинства систем защиты баз данных и систем управления / распределения ресурсов, западные эксперты указывают на серьезную уязвимость популярной библиотеки криптографического обеспечения OpenSSL. Используемые в них SSL** / TLS*** системы поддерживают конфиденциальность связи по Интернету и некоторым виртуальным частным сетям (VPN), но не гарантируют защиту от возможных проникновений. В момент их появления в 2012–2014 годы в них было обнаружено около 40 системных ошибок и еще столько же было выявлено в 2017-м.

* **Industry 4.0 (The Fourth Industrial Revolution)** – 4-я промышленная революция, ожидаемое массовое внедрение киберфизических систем в производство и обслуживание человеческих потребностей, включая быт, труд и досуг. Также это производственная сторона, эквивалентная ориентированному на потребителей Интернету вещей. Один из существенных аспектов Industry 4.0 – идея сервис-ориентированного проектирования (от пользователей, применяющих заводские настройки для производства собственных продуктов, до компаний, которые поставляют индивидуальные продукты по заказу потребителей).

** **SSL (Secure Sockets Layer)** – протокол защищенных сокетов, гарантирующий безопасную передачу данных по сети (сочетает криптографическую систему с открытым ключом и блочное шифрование данных).

*** **TLS (Transport Layer Security)** – протокол защиты транспортного уровня, развитие криптографического протокола SSL, обеспечивающий защищенную передачу данных между узлами сети Интернет. TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для обеспечения конфиденциальности и коды аутентичности для сохранения целостности сообщений.

Таблица 1. Инфраструктура IIoT

Области применения	Фирмы
Прикладные средства:	
– основные средства	
Моторы, генераторы, турбины	ABB, Alstom, Danfoss, DEC, Emerson, General Electric, Mitsubishi Electric, Rockwell Automation, Schneider Electric, Siemens, Yaskawa
Измерительная аппаратура	Azbil, Cameron, Emerson, Endress+Hauser, Honeywell, Krohne, Magnetrol, Siemens, Vega, Yokogawa
Контроллеры технологического процесса	ABB, Emerson, Honeywell, Mesto, Rockwell Automation, Schneider Electric, Siemens, Yokogawa
Автономные контроллеры	Advantech, B&A Electric, Beckhoff, Mitsubishi Electric, Omron, Pro-face, Rockwell Automation, Schneider Electric, Siemens
Блоки или устройства управления электроприводом	ABB, Danfoss, Emerson, General Electric, Mitsubishi Electric, Rockwell Automation, Schneider Electric, Siemens, WEG, Yaskawa
Промышленные роботы	Fanuc Robotics, Kawasaki Robotics, Kuka, Mitsubishi Electric, Nachi, Staubli, Toshiba Machine, Yamaha Robotics, Yaskawa
Оконечное оборудование	Atlas Copsco, Flowserve, Gargner Denver, Grundfos, Ingersoll Rand, KSB, Sullair, Sulzer, Xylem
– мобильные активы	
Обслуживающие роботы	AktiveLink, Adept, Aethon, Amazon Robotics, Carbon Robotics, Fetch Robotics, Locus, Open Bionics, Savioke, Siasun, Softbank, Titan Medical, Yaskawa
Автомобили большой грузоподъемности	Caterpillar, Daimler, Ford, John Deere, MAN Truck&Bus, Navistar, Tata, Toyota, Volvo
Виртуальная/дополненная реальность	APX, Autodesk, Daqri, PEУ Vive, Microsoft HoloLens, Virtalis, Vuforia, VuzixWorldviz
БПЛА (дроны)	3D Robotics, AEE, AeroVironment, Ascending Technologies, CybAero, DJI, Ehang, Insuti, Parrot, Precision Hawk, Skycatch, Yuneec
Радиомаяки	Bluvision, Estimote, Kontakt.io, Radius Networks, Sensorberg, Sensoro
Автоматические самоходные тележки	Daifuku, Muratec, Dematic, Tarex
Составные элементы	
Аппаратное обеспечение (ИС и модули)	ARM, Analog Devices, Infineon, Intel, Nexcom, NXP, Sierra Wireless, Texas Instruments
ПО (встраиваемые ОС)	DDC–I, ENEA, Green Hills Software, Linux, Mentor Graphics, QNX, Texas Instruments, Wind River
Подключаемость (сети полевого уровня)	Bluetooth, LoWPAN, Neon, SigFox, Wi-Fi, ZigBee, Z-Wave
Партнеры (системные интеграторы)	Automated Technology Group, CG Controls, Intech, Leidos Energy, Maverick Technologies, Prime Controls, Wood Group Mustang
Датчики и актюаторы	Advantech, Bosch, Honeywell, Infineon, Libelium, Mermsic, Sensirion, TE, Texas Instruments

Таблица 1. Продолжение.

Области применения	Фирмы
Облачный хостинг	Amazon Web Services, IBM, Microsoft, Oracle, Saleforce, SAP, ThingWorx
Промышленный Ethernet	CC-Link IE, EtherCAT, Ethernet/IP, Powerlink, PROFINET, Sercos
Услуги управления изменениями	Accenture, Deloitte, PWC
Маршрутизаторы и шлюзы	Adlink, Advantech, Cisco, Eurotech, Intel, Kontron, Multi-Tech, Sierra
Наборы средств для разработки/наборы средств разработки ПО	Anaren, Atmel, Avnet, Eurotech, Marwell, Texas Instruments, VMware
Промышленные полевые шины	ASI-Interface, ControlNet, DeviceNet, FireWire, Hart, INTERBUS, IO Link, Link, Profi Bus, USB
Специализированные промышленные альянсы	Asia IoT Alliance, Industrial Internet Consortium, Industrie 4.0, Made in China 2025, Manufacturing USA
Платформы и реализации	
Промышленные платформы	ABB, Bosch, Cisco Jasper, Emerson, Fujitsu, General Electric, Hewlett-Packard Enterprise, Hitachi, Honeywell, Hewlett-Packard, Huawei, IBM, Microsoft, Predix, Rockwell Automatiom, RTI, Schneider Electric, Siemens, ThingWorx
Средства аналитики	Azima, DLI, N3N Visualize, KCF Technologies, Pruftechnik, Senseye
Интерфейсы (виртуальная/дополненная реальность)	APX, Autodesk, Daqri, HTC Vive, Microsoft HoloLens, Virtalis, Vuforia, Vuzix, Worldvis
Кибербезопасность: – аппаратное обеспечение; – ПО; – услуги	Belden, Lockheed Martin, Phoenix Contact, Siemens, Symantec, Trend Micro BAE Systems, Belden, Moxa, Phoenix Contact, Radiflow, SEL, Siemens Accenture, BAE Systems, Deloitte, Lockheed Martin, Siemens, Yokogawa

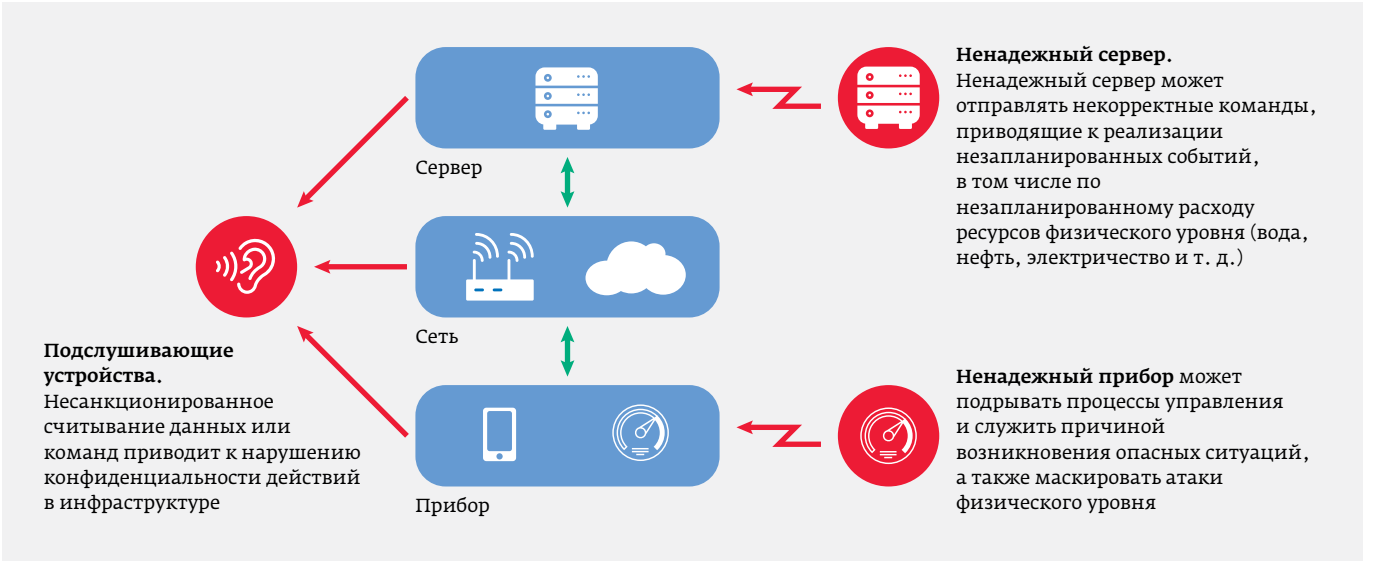

Рис. 4. Угрозы в области безопасности IoT. *Источник: Infineon*

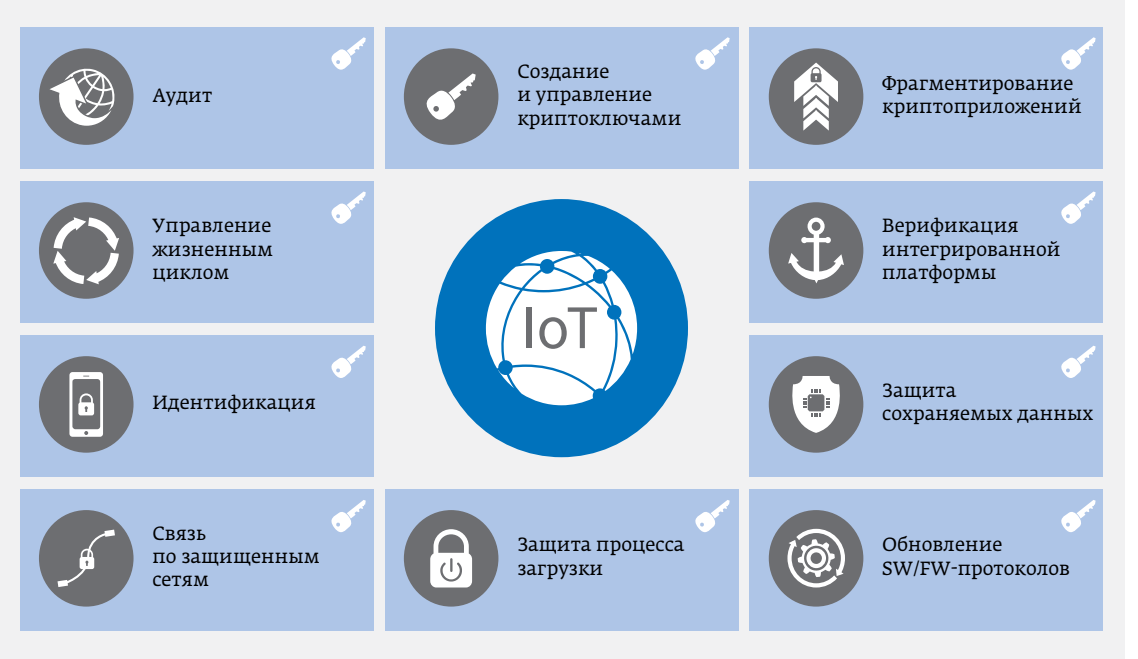

Рис. 5. Общие подходы к обеспечению защиты данных с точки зрения специалистов корпорации Infineon Technology. *Источник: Infineon*

Общие подходы к безопасности данных (с точки зрения специалистов немецкой корпорации Infineon Technology) приведены на рис. 5. Таким образом, программные методы обеспечения безопасности не относятся к исчерпывающим – опыт последних лет показывает необходимость их поддержки и дополнения на уровне аппаратного обеспечения.

Область разработки микросхем обеспечения безопасности данных остается достаточно конкурентной. На европейском рынке основными соперниками Infineon Technology являются корпорации NXP Semiconductors (Нидерланды) и STMicroelectronics (Франция / Италия) [6].

* * *

IIoT, являясь одной из реализаций IoT в целом, отличается от своих «собратьев» наибольшим комплексным воздействием на повседневную жизнь человека – товары, услуги, крупные торговые центры и т. п. IIoT в принципе является основным катализатором цифровой трансформации человеческого общества. Такие факторы его развития, как инновационность и потенциал повышения конкурентоспособности, обуславливают ускорение темпов роста производительности производства и достижение высокого уровня рентабельности при освоении новой продукции. Оптимизация производственных процессов, сокращение простоев оборудования, экономия различных ресурсов и поддержание безопасного режима работы делают IIoT необходимым, критическим фактором дальнейшего развития промышленного сектора. Но на этом влияние IIoT на окружающую среду не ограничивается – его развертывание стимулирует спрос на вычислительную технику и услуги ЦОД, средства и системы связи, ИС и датчики. Это рост продаж и занятости в смежных отраслях, расширение существующих и формирование новых рынков.

Таким образом, как трансформационная технология IIoT уже оказывает и будет оказывать все большее воздействие на окружающую человека действительность и на него самого.

ЛИТЕРАТУРА

1. IoT trend watch 2018. IHS Markit, January 2018. https://ihsmarkit.com/Info/0118/iot-trend-watch-2018.html
2. Top 8 in 2018: The top transformative technologies to watch this year. https://ihsmarkit.com/research-analysis/tmt-blog-top-transformative-technology-trends-of-2018.html
3. Dorsch J. IoT's Many Different Forms. Semiconductor Engineering, December 7th, 2017 https://semiengineering.com/iots-many-different-forms/
4. How IoT is transforming the industrial ecosystem. IHS Markit, February 2018. https://cdn.ihs.com/www/pdf/IHS-Markit-IoT-and-Industrial-ebook.pdf
5. Trends and innovations in Industrial IoT. The Manufacturer, 17 Nov 2017 https://www.themanufacturer.com/articles/trends-and-innovations-in-industrial-iot/
6. **Yoshida J.** Does Japan Get Industrial IoT? EE Times, 9/28/2017 https://www.eetimes.com/document.asp?doc_id=1332368