УДК 629.7.01 DOI 10.21778/2413-9599-2017-1-124-140

М. В. Макушин, А. Н. Стяжкин, А. В. Фомина

Центральный научно-исследовательский институт «Электроника», Москва, Россия

ПРОИЗВОДСТВЕННО-ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ РАЗВИТИЯ ИНТЕРНЕТА ВЕЩЕЙ

В статье представлены современное состояние и перспективы Интернета вещей, его воздействие на рынки полупроводниковых приборов и конечных электронных систем. Также рассматриваются вопросы обеспечения безопасности данных и доступа к системам Интернета вещей, основные проблемы развития и роль правительственных органов. Оцениваются перспективы развертывания Интернета вещей в российских условиях.

Ключевые слова: *безопасность, Интернет вещей, подключаемость, сети.*

Для цитирования: Макушин М. В., Стяжкин А. Н., Фомина А. В. Производственно-технологические аспекты развития Интернета вещей // Радиопромышленность. 2017. № 1. С. 124–140.

M. V. Makushin, A. N. Styazhkin, A. V. Fomina

Central Research Institute «Electronics», Moscow, Russia

INDUSTRIAL AND TECHNOLOGICAL ASPECTS OF DEVELOPMENT OF INTERNET OF THINGS

The article presents the current status and prospects of Internet of things, the impact thereof on the markets of semiconductor devices and electronic systems. The article also deals with the issues of data security and access to systems of Internet of things, the key problems of development and the role of governmental authorities. Prospects for deployment of Internet of Things in the Russian conditions are also reviewed.

Keywords: *security, Internet of Things, connectivity, networks.*

For citation: Makushin M. V., Styazhkin A. N., Fomina A. V. Industrial and technological aspects of development of internet of things. Radiopromyshlennost, 2017, no. 1, pp. 124–140 (In Russian).

DOI 10.21778/2413-9599-2017-1-124-140

Введение

Термин «Интернет вещей»[1] подразумевает опознаваемые объекты и их виртуальные представления в интернет-подобных структурах, охватывает все подключаемые к Интернету приборы и устройства различного назначения. По мере развития Интернет вещей довольно скоро трансформируется во Всеохватывающий Интернет[2]. На данный момент развития Интернета вещей существуют специализированные направления: медицинский, промышленный, энергетический Интернет вещей и т.д. Для развития этих технологий требуются производительные процессоры и микроконтроллеры, а также средства обеспечения безопасности передаваемых данных и систем, получающих подобные данные.

[1] IoT (Internet of Things), Интернет вещей – понятие, относящееся к однозначно опознаваемым объектам (вещам) и их виртуальным представлениям в интернет-подобных структурах; охватывает все подключаемые к Интернету приборы и устройства различного назначения.

[2] IoE (Internet of Everything), Всеохватывающий Интернет – дальнейшее развитие Интернета вещей (IoT, Internet of Things), в рамках которого осуществляются контакты между людьми, людьми и вещами (в т.ч. машинами и сетями датчиков), между вещами (в т.ч. межмашинный обмен данными, обмен данными между сетями данных, сетями данных и машинами), а также поддерживающие это процессы. Понятие, относящееся к ситуации, когда в любое время любой человек и любая вещь могут быть соединены в интернет-подобной среде.

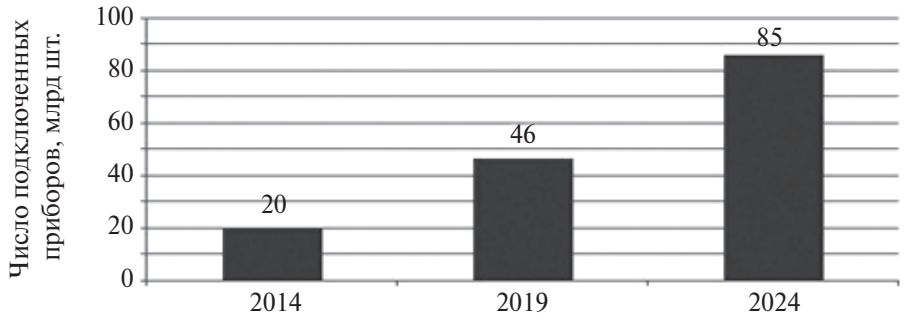

Рисунок 1. Прогноз роста числа приборов, подключенных к Интернету

Мир находится на ранней стадии развития Интернета вещей – технологической эволюции, основанной на использовании подключенных к Интернету приборов для расширения возможностей средств/систем связи, автоматизации сложных промышленных процессов и обработки больших объемов информации. Для оценки порядка эволюции в данной области можно отметить, что, если в 2014 г. в мире действовало 20 млрд подключенных к Интернету приборов, то в 2024 г. их число превысит 80 млрд шт. (рис. 1) [1].

Хотя концепция Интернета вещей по-прежнему сравнительно нова, она уже трансформируется в более широкую модель – Всеохватывающий Интернет. Эта метаморфоза не только охватывает подключенные к Интернету приборы, но и предусматривает полный отход от того образа использования подобных приборов в Интернете, что существовал до сих пор. В настоящее время большинство подключенных к Интернету приборов требует непосредственного человеческого взаимодействия и используется в основном для потребления информационного наполнения (контента) и развлечений (компьютерные игры). В будущем же большинство подключенных приборов будет использоваться для мониторинга и управления различными системами, машинами и объектами – в частности, в таких областях, как освещение, обогрев/кондиционирование, блокировка окон, автомобильная электроника «под капотом» и т.п.

В целом предполагается, что продажи полупроводниковых приборов для Интернета вещей будут расти, и в период 2019–2020 гг. их общий объем может составить 50–75 млрд долл. Структура продаж полупроводниковых приборов приведена на рис. 2 [2].

Перспективы развития рынка подключенных приборов, включая жилой сектор

По данным аналитиков корпорации Gartner, в 2016 г. число подключенных к Интернету вещей в мире увеличится на 30% по сравнению с 2015 г., при этом ежедневно будет подключаться по 5,5 млн новых приборов. В 2020 г. число подключенных приборов достигнет 20,8 млрд шт. С технической точки зрения число оказывающих услуги приборов Интернета вещей достигнет 25 млрд, что на 22% больше показателей 2015 г.

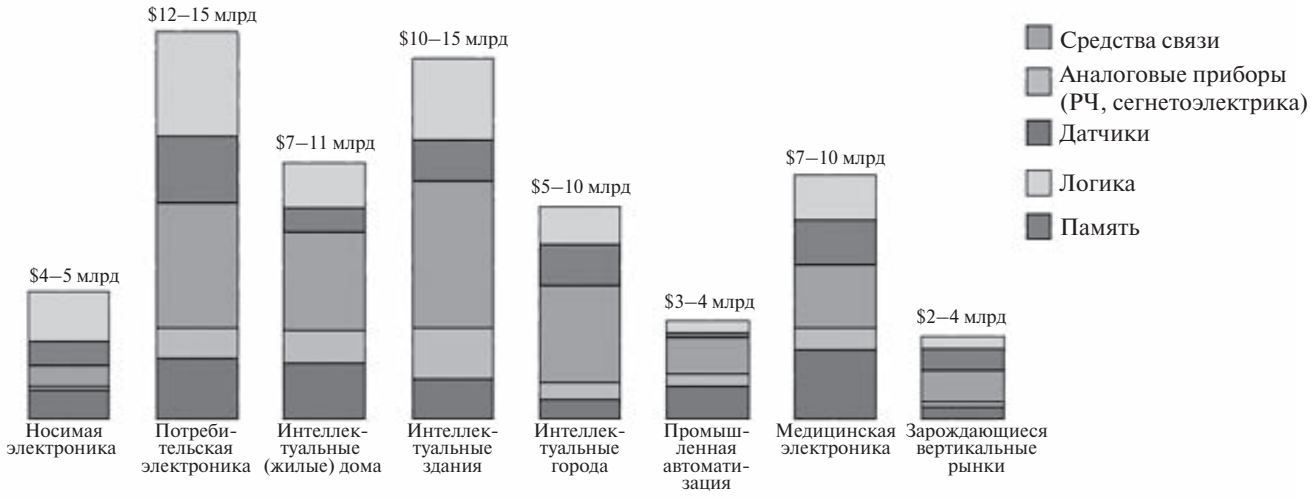

Рисунок 2. Оценка состояния рынка полупроводниковых приборов для Интернета вещей в 2019–2020 гг.

В сфере услуг доминирует профессиональная категория (когда бизнес заключает контракты с внешними поставщиками на проектирование, установку и эксплуатацию IoT-систем). Однако услуги подключения (через поставщиков услуг связи) и потребительские услуги демонстрируют бóльшие темпы роста.

Таким образом, услуги становятся реальным движителем роста ценности Интернета вещей, все большее внимание уделяется новым услугам, оказываемым конечным пользователям. Помимо подключаемых к сети автомобилей пользователи продолжают подключать к Интернету вещей различные приборы (табл. 1).

Именно на потребительский сектор приходится набольшее число подключений: 3 млрд приборов в 2015 г., 4 млрд – в 2016 г. и 13,5 млрд – в 2020 г. [3]. Однако корпоративный сектор лидирует, в том числе и по затратам на Интернет вещей. В корпоративном секторе специалисты Gartner рассматривают два класса подключаемых приборов. Первый состоит из универсальных или кросспромышленных приборов, используемых в различных отраслях промышленности (их также можно отнести к инфраструктуре предприятий). Речь идет о подключаемых к Сети системах освещения, отопления, вентиляции и кондиционирования воздуха, системах управления зданиями/сооружениями. Отмечается, что подобные системы разворачиваются главным образом с целью экономии затрат. Действительно, с точки зрения затрат на аппаратное обеспечение на потребительский сектор в 2016 г. приходится 546 млрд долл., а на корпоративный (в целом) – 868 млрд долл. (табл. 2).

Ко второму сектору относятся вертикально специализированные приборы, используемые в отдельных отраслях. К этому классу относятся различные виды специализированного оборудования: системы, используемые в операционных больниц, следящие устройства для контейнерных перевозок и т.п.

В настоящее время крупнейшей категорией по числу подключений в корпоративном секторе являются специализированные приборы и системы. Однако ситуация меняется, и в 2020 г. по числу подключений будут лидировать универсальные приборы и системы. Правда, расходы на специализированный сектор и в 2020 г. будут превосходить расходы на универсальный сектор.

Большие возможности развития Интернету вещей представляет жилищный сектор. По данным последнего исследования фирмы Navigant Research, мировые доходы от продаж приборов Интернета вещей для жилищного сектора в период с 2015 по 2025 г. увеличатся с 7,3 млрд до 67,7 млрд долл., а общий объем продаж за эти годы составит 330 млрд долл. К жилищным приборам Интернета вещей относится широкий диапазон изделий, таких как интеллектуальные термостаты, позволяющие пользователям дистанционно (с помощью

Таблица 1. Анализ и прогноз развития структуры установленной базы приборов Интернета вещей в 2014–2020 г. (млн шт.)

Тип приборов	2014	2015	2016	2020
Потребительская электроника	2277	3023	4024	13509
Инфраструктура предприятий*	632	815	1092	4408
Вертикально специализированные приборы**	898	1065	1276	2880
Всего	3807	4902	6392	20797

Таблица 2. Анализ и прогноз развития структуры конечных расходов на IoT в 2014–2020 гг. (млрд долл.)

Тип приборов	2014	2015	2016	2020
Потребительская электроника	257	416	546	1534
Инфраструктура предприятий*	115	155	201	566
Вертикально специализированные приборы**	567	612	667	911
Всего	939	1183	1414	3010

* Включая подключенное к Интернету освещение, системы отопления, вентиляции и кондиционирования воздуха, системы управления зданиями/сооружениями, в основном разворачиваемыми в целях экономии расходов.

** Специализированное оборудование, использующееся в операционных больниц, следящие устройства при контейнерных перевозках и т.п.

смартфона) контролировать температуру и/или СИД-освещение в доме. Крупнейшие изготовители начинают осознавать возможности, которые предлагают подобные обменивающиеся данными приборы с точки зрения повышения эффективности, автоматизации, безопасности и комфортности жилищ.

Однако на пути развития рынка жилищных приборов Интернета вещей существуют серьезные трудности, например наличие многочисленных протоколов и стандартов, создающих барьер интероперабельности (функциональной совместимости). Протоколы Wi-Fi[3], ZigBee[4], Bluetooth[5] и прочие соперничают за выживание на рынке, что создает путаницу и неудобства для потребителя и замедляет освоение жилищного Интернета вещей [4].

Воздействие Интернета вещей на рынок полупроводниковых приборов

Развертывание Интернета вещей будет оказывать существенное влияние на рынок полупроводниковых приборов, потребует широкого международного сотрудничества и разработки новых технологий. Подобные альянсы и консорциумы уже формируются. Так, например, весной 2016 г. SITRI[6], CEA-Leti[7] и MINATEC[8] заключили соглашение о разработке новых технологий для рынка Интернета вещей, предусматривающее ускорение разработки инновационных решений на основе подхода «Больше, чем Мур»[9] и развитие соответствующей экосистемы. Соглашение покрывает такие области, как микроконтроллеры, датчики, микроэлектромеханические системы (MEMS), входные радиокаскады систем связи 5G, вычислительные средства и средства связи с ультранизкой потребляемой мощностью, радиочастотные ИС на основе технологий «кремний-на-изоляторе» (КНИ) для радиоприборов (RF-SOI) и полностью обедненного кремния (FD-SOI). Разработки будут ориентированы как на международный, так и на быстро растущий рынок Интернета вещей КНР [5].

Надо отметить, что наибольший спрос операторы Интернета вещей будут уделять микроконтроллерам и датчикам, в том числе MEMS-датчикам, – именно они станут основой инфраструктуры Интернета вещей. Действительно, микроконтроллеры включают в свой состав не только ядра процессоров, но и память, управляющую схемотехнику, периферийные интерфейсы, шины и многие другие блоки. Поэтому воздействие Интернета вещей на полупроводниковые приборы лучше всего рассмотреть на их примере.

Основная борьба на поле микропроцессорных архитектур и микроконтроллеров для Интернета вещей разгорается между компаниями ARM и Intel. При этом отмечается, что взрывной рост числа конечных узлов делает роль микроконтроллеров стратегической. Фирма ARM является лидером в расширяющихся сферах применения конечных узлов, выпуская микроконтроллеры Cortex-M. В то же время Intel – крупнейшая полупроводниковая

---

[3] Wi-Fi (Wireless Fidelity) – стандарт Wi-Fi на беспроводную связь, логотип, выдаваемый после сертификации оборудования ассоциацией WECA и гарантирующий интероперабельность между беспроводными PC – картами LAN (локальных сетей), устройств и точек доступа различных производителей. Данная технология предназначена для беспроводных подключений в рамках офиса, дома, на расстоянии 50–70 м от базовой станции.

[4] ZigBee – патентованный набор коммуникационных протоколов высокого уровня, разработанный для использования маленьких цифровых радиоустройств с низкой потребляемой мощностью на базе стандарта IEEE802.15.4 для беспроводных личных (персональных) сетей. Также называется 802.15. Технология работает по так называемой «сетчатой схеме», позволяя автоматически устанавливать связь с авторизованными устройствами, расширяя или сужая сеть по мере входа и выхода из зоны покрытия новых устройств. Если некоторые устройства или базы отключаются или их сигнал блокируется, другие автоматически ищут новые схемы коммуникации. Свое необычное имя технология получила от другой схемы оптимизированной схемы адаптации: зигзагообразной траектории полета шмеля (Zig – сокращение от zigzag, Bee от Bumblebee – шмель).

[5] Bluetooth, технология «Голубой Зуб» – перспективная универсальная технология беспроводной связи разнотипных микропроцессорных устройств локальной сети в диапазоне 2,4 ГГц, названная так в честь датского короля X в. Гарольда II по прозвищу Голубой Зуб, прославившегося собиранием датских земель.

[6] SITRI (Shanghai Industrial Technology Research Institute) – Шанхайский НИИ промышленных технологий.

[7] CEA-Leti – европейский центр исследований в области микроэлектроники, курируемый французским атомным ведомством (Electronics and Information Technology Laboratory of the French Atomic Energy Commission).

[8] Minatec, первоначальное наименование – «Центр инноваций в области микро- и нанотехнологий» (Micro and Nanotechnology Innovation Centre) – европейский научно-исследовательский центр, расположенный в Гренобле, Франция. Создан в 2006 г. LETI и INPG (Grenoble Institute of Technology – Гренобльский технологический институт).

[9] «More than Moore» («Больше, чем Мур») – концепция, направленная на достижение больших результатов и в более широком диапазоне, чем изложено в т.н. «Законе Мура» (удвоение числа транзисторов на кристалле каждые 18–24 месяца без увеличения удельной стоимости функции для конечного потребителя). Заключается в использовании 2,5- и 3-мерных архитектур, позволяющих существенно наращивать функциональность, сокращать занимаемое пространство и потребляемую мощность, а также в использовании перспективных материалов и приборных структур.

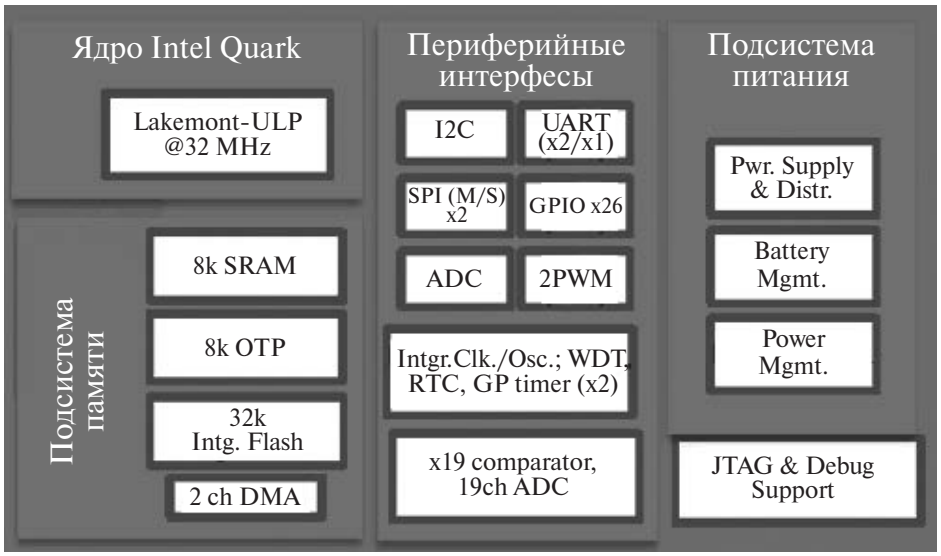

Рисунок 3. Первая итерация микроконтроллера Quark x86 корпорации Intel

фирма, занимающая в рейтинге поставщиков микроконтроллеров 17-е место благодаря относительно новым кристаллам ИС Quark x86, что ставит ее примерно на один уровень с Panasonic и Sharp. При этом Renesas, NXP и Microchip почти на порядок опережают Intel по поставкам микропроцессоров.

Рынок ИС, продающихся иногда дешевле 1 долл., для Intel нов, а для Интернета вещей является стратегическим. Интернет вещей становится новой эрой благодаря достижениям в области технологий конечных узлов, так как позволяет искусственному интеллекту быть примененным там, где ранее он не имел доступа к Интернету.

Для того чтобы конкурировать с ведущими изготовителями микроконтроллеров, корпорации Intel необходимо сделать так, чтобы кристаллы ИС Quark отвечали следующим требованиям (рис. 3):

- выйти на уровень активной мощности в 1 мВт, чтобы конкурировать с ядрами Cortex-M0;
- включать богатый портфель опций памяти, устройств ввода-вывода и подключаемости партнеров ARM;
- быть нацеленными на специализированные вертикальные рынки, такие как автомобильные микроконтроллеры с различными шинами протокола CAN;
- провести свои x86 инструментальные средства программирования и партнеров в мир микроконтроллеров;
- облегчить поддержку аппаратного обеспечения безопасности на уровне не худшем, чем у фирмы ARM с ее новой технологией TrustZone CryptoCell [6].

Фирма ARM уже предлагает портфель продуктов и услуг, которые должны облегчить создание безопасных систем для Интернета вещей. Ядро портфеля – операционная система и набор облачных предложений[10] типа «ПО как услуга» (SaaS), предназначенные для ускорения разработки ИС для облачных вычислений – как для производственных лицензий ARM, так и для ее потребителей-проектировщиков.

В портфеле также представлены два процессорных ядра архитектуры ARMv8-M. Ядро Cortex-M33 является 32-разрядным процессором общего назначения с технологией безопасности TrustZone, ЦОС-расширениями и возможностью осуществления операций с плавающей запятой. Для тесного взаимодействия с заказным аппаратным ускорителем предлагается интерфейс сопроцессора.

Cortex-M23 является в большей степени основным ядром, ориентированным на применения с ультранизкой потребляемой мощностью и технологией TrustZone. Отмечается, что Cortex-M23 на 75% меньше и на 50% эффективнее Cortex-M33, и что оба процессорных ядра пригодны для применений с функциональной безопасностью.

Наряду с процессорными ядрами ARM разработала системный СФ-блок, расширяющий

[10] Cloud computing – облачные вычисления, технология распределенной обработки данных (компьютерная архитектура), в которой компьютерные ресурсы и мощности предоставляются пользователю как интернет-сервис по требованию. При этом нагрузка на входящие в облако компьютеры распределяется автоматически.

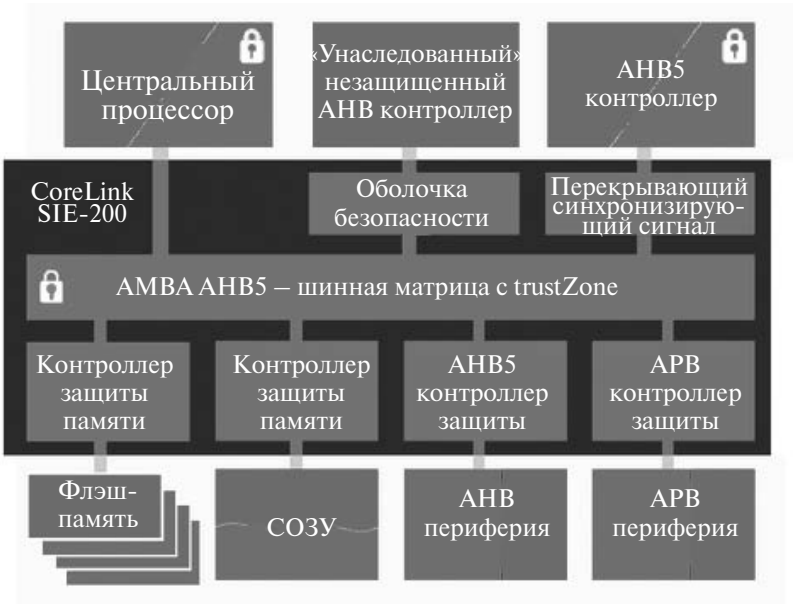

Рисунок 4. Блок-схема шины CoreLink SIE-200 фирмы ARM

параметры безопасности TrustZone за пределы собственно ядра. Шина CoreLink SIE-200 (рис. 4) предварительно верифицирована с процессорами ARMv8-M и построена на шинной матрице AHB5 с целью обеспечения аппаратно-принудительной изоляции между защищенными и незащищенными приложениями. С целью соответствия различным архитектурным нуждам шина создана как реконфигурируемая. В целях обеспечения защищенной передачи сигналы по каждой транзакции в рамках системы шины CoreLink SIE-200 использует протокол AMBA.

Шина CoreLink SSE-200 в виде СФ-блока доступна для проектирования полностью верифицированных подсистем. Предполагается, что она позволит разработчикам отказаться от многих работ по интеграции основной подсистемы и верификации. Это поможет сократить цикл разработки новой продукции на срок от 6 до 12 месяцев.

Ядра Cortex-M23 и Cortex-M33 уже доступны для широкого лицензирования, они используют встроенную операционную систему OS5. Услуга встраиваемого облака, обеспечиваемая представленным портфелем, будет предоставляться с I квартала 2017 г. [7].

По данным исследовательской корпорации IHS, рынок микроконтроллеров, используемых в подключенных к Интернету машинах, носимой электронике[11], средствах автоматизации зданий и других применениях Интернета вещей в период 2014–2019 гг. увеличится с 1,7 млрд до 2,8 млрд долл., т.е. CAGR[12] составит 11%. За этот же период CAGR рынка микроконтроллеров достигнет 4% (рис. 5). Согласно данным последнего исследования IHS[13], IoT состоит как из существующих приборов, адресуемых по интернет-протоколу, так и из подключаемых к сети Интернет электронных приборов. Данное определение отличается от определения Всеохватывающего Интернета, в котором даже неподключенная электроника и неподключенные объекты, как ожидается, будут представлены во Всемирной паутине.

IHS подразделяет IoT-рынок на три отдельные категории: контроллеры, такие как ПК и смартфоны; инфраструктура, включая маршрутизаторы и серверы; узлы (точки присоединения/устройства, подключенные к сети), например замкнутые телевизионные системы (системы наблюдения / ведомственное ТВ), светофоры и т.п. Каждая из указанных категорий предоставляет свои возможности поставщикам аппаратного и программного обеспечения, а также услуг.

Интернет вещей имеет тенденцию к установлению устойчивых взаимоотношений с рынком микроконтроллеров, так как малые узлы, используемые для подключения к Сети, а также концентраторы

[11] Wearable electronics, wearables – носимые устройства, например микродисплей, встроенный в очки, или датчики и другие устройства, вмонтированные в одежду или обувь.

[12] CAGR (Compound Annual Growth Rate) – среднегодовой темп прироста в сложных процентах.

[13] Microcontroller Market Tracker.

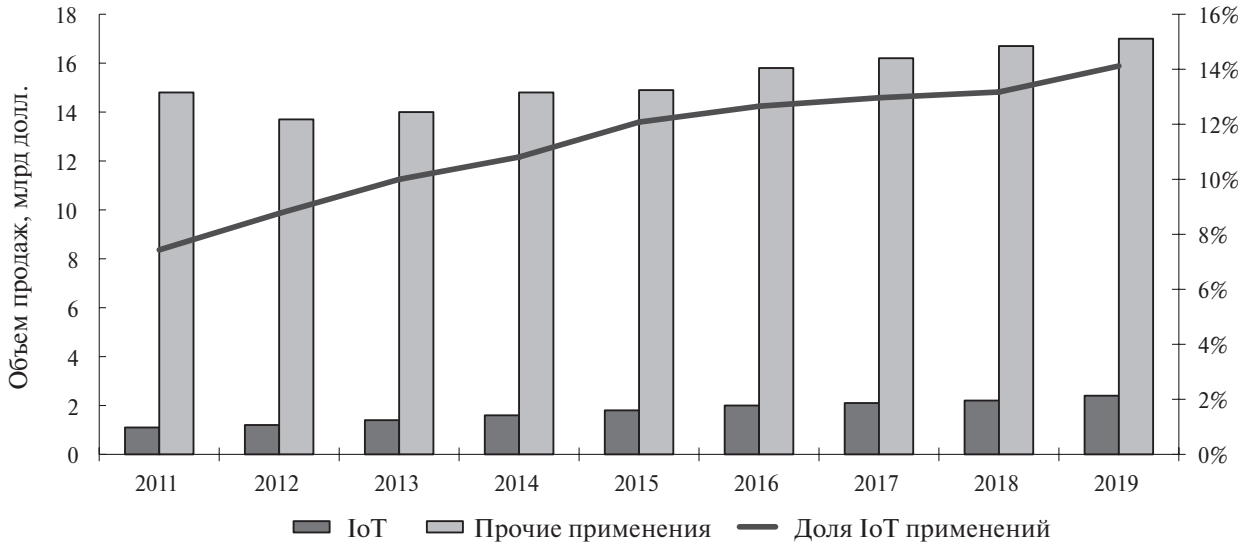

Рисунок 5. Динамика и прогноз развития рынков микроконтроллеров для Интернета вещей и других применений в 2011–2019 гг.

датчиков, собирающие данные, в первую очередь базируются на платформах микроконтроллеров. Многие значительные поставщики микроконтроллеров уже следуют за шумихой, развернутой вокруг миллиардов подключаемых приборов. Однако проблема промышленности сейчас состоит в том, чтобы не ошибиться с количественной оценкой новой возможности, так как Интернет вещей является концептуальной тенденцией, а не прибором, приложением или даже новой функцией.

Ввиду того, что подключаемость к Интернету вещей требует нового рассмотрения свойств полупроводниковых приборов, многие фирмы-изготовители начали разработку решений в области платформ Интернета вещей. В то же время другие фирмы провели реорганизацию и создали подразделения Интернета вещей, призванные решить реально возникающие проблемы. Это особенно верно в отношении рынка микроконтроллеров. Среди поставщиков полупроводниковых приборов, принявших стратегии, ориентированные на Интернет вещей, можно назвать такие корпорации, как Atmel, Broadcom, Cisco Systems, Freescale Semiconductor, Infineon Technologies, Intel, Microchip Technologies, NXP, Qualcomm, Renesas Electronics и Texas Instruments [8].

Взаимосвязь производственной базы и Интернета вещей

Наблюдаемая в последнее время тенденция сдвига от новейших полупроводниковых технологий к более зрелым дает регионам с большим парком оборудования для обработки 200-мм пластин значительные возможности. Во многом это касается Европы, являющейся мировым лидером на нескольких важных сегментах рынка, например, в таких направлениях развития «Интернета вещей», как интеллектуальные автомобили и электроника для здравоохранения.

Европейцы обладают технологическими и производственными знаниями, позволяющими удовлетворить требования этих сегментов. Однако здесь первостепенное значение имеет не освоение новейших (минимальных) топологий, а достижение рентабельности. Это и создает благоприятные условия для применения бывшего в использовании полупроводникового оборудования и соответствующих услуг. Помимо вопросов трехмерной интеграции, в связи с увеличением трафика данных возрастает роль различного рода датчиков и сопутствующих приборов. Наиболее рентабельным является производство данных изделий на пластинах диаметром 200 мм – эта технология хорошо отработана. Оборудование по обработке 200-мм пластин во многих случаях требует «переработки» и «перенацеливания». Однако данные процессы позволяют поставщикам полупроводниковых приборов продлить использование имеющегося оборудования, избежать закупки дополнительного оборудования и, соответственно, снизить издержки. Надо отметить, что применение «зрелого»/«устаревшего» (либо бывшего в использовании оборудования) требует поддержки современных методик контроля производственного процесса, новых средств тестирования и корпусирования.

Развитие рынка изделий полупроводниковых приборов и оборудования для их производства показывает, что инвестиции в «зрелое оборудование» оказываются востребованными, в частности для Интернета вещей, база которого остается основой для производства крупносерийных изделий электронной техники.

Рисунок 6. Потенциал Интернета вещей: мощности по обработке 200-мм пластин

По существующей производственной базе можно сделать следующие выводы:

- заводы по обработке пластин диаметром от 150 до 200 мм составляют около 40% установленных производственных мощностей;
- мощности кремниевых заводов[14] по обработке 200-мм пластин в период 2012–2016 гг. увеличатся на 7%;
- новые применения, относящиеся к мобильности, датчикам и Интернету вещей, как ожидается, предоставят значительные возможности для производства на пластинах диаметром 200 мм.

Из 27 млрд долл., затраченных на оборудование заводов по обработке пластин в 2013 г., и 31 млрд долл. в 2014 г. на бывшее в использовании оборудование приходилось около 5%, или 1,5 млрд долл., ежегодно. Также в 2014 г. инвестиции в заводы по обработке 200-мм пластин наращивались кремниевыми заводами и IDM[15], их объем б/у оборудования по обработке пластин этого диаметра вырос на 45%.

Что касается собственно предприятий, то в период 2013–2015 гг. было закрыто или остановлено 15 заводов по обработке 200-мм пластин, но одновременно было открыто 11 новых заводов / производственных линий (рис. 6). На рис. 7 приведена структура производства различных приборов на пластинах диаметром 200 и 300 мм.

Бывшее в использовании оборудование будет как минимум формировать часть стратегии почти любого производства или разработки полупроводниковых приборов в Европе. Так как значимость бывшего в использовании оборудования для полупроводниковой промышленности и исследований в Европе растет, критически важным становится поддержка цепи поставок, обеспечивающая качество оборудования, поддержку и услуги, соответствующие нуждам потребителей. К общим проблемам по цепочке поставок относятся:

- создание по всей Европе кооперационных связей между пользователями и поставщиками бывшего в использовании оборудования, а также выработка необходимых видов сотрудничества;
- гарантирование возможности доступа к успешным инженерным ресурсам, поддерживающим установленную базу бывшего в использовании оборудования;

[14] Foundry – кремниевый завод по производству ИС по спецификациям заказчика с предоставлением заказчику широкого спектра услуг использования инструментальных средств фирм-союзников из числа поставщиков САПР для проектирования собственных ИС с использованием базы библиотек стандартных элементов различных fabless- и IDM-фирм (по контрактам foundry с последними), платформ и сложнофункциональных блоков (на тех же условиях). Кремниевые заводы могут заниматься разработкой новейших технологических процессов, но разработкой собственных конструкций ИС, как правило, не занимаются.

[15] IDM (Integrated Device Manufacturers) – интегрированные изготовители приборов; традиционные полупроводниковые фирмы полного цикла – разработка, проектирование, производство и маркетинг ИС.

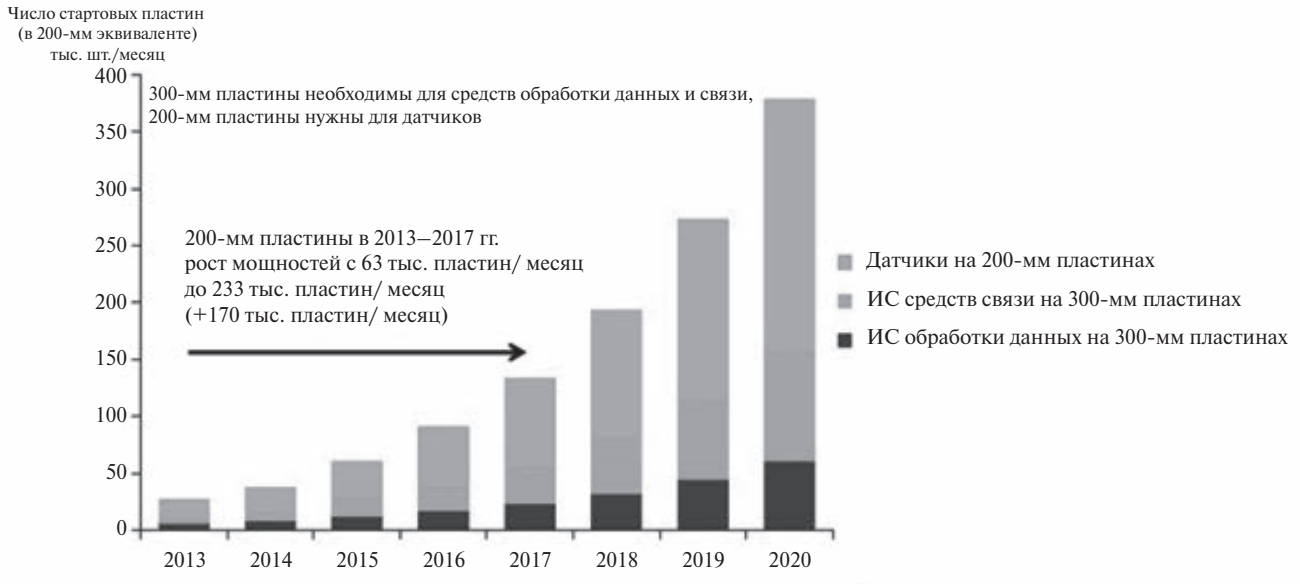

Рисунок 7. Создание в Европе жизнеспособной и профессиональной индустрии бывшего в использовании оборудования

- существующий дефицит донорских систем или критических компонентов, что ограничивает использование б/у оборудования [9].

Технологии Интернета вещей для здравоохранения

По мере развития технологий подключаемости и наращивания возможностей средств связи, их интеграции в повседневную среду здравоохранения и медицинской техники, все острее встают вопросы надежности работы медицинской аппаратуры и защиты персональных данных пациента. Надежность обычно измеряется средним временем наработки на отказ (MTBF), но, когда речь идет о рынках, где требования к безопасности являются критически важными, эта формула приобретает совершенно новый уровень важности. Действительно, сбой в смартфоне – простое неудобство. Сбой же в медицинском приборе может стоить жизни. Это указывает на то, сколько усилий надо приложить для проверки как на уровне, предшествующем реализации ИС в кремнии (последний этап проектирования), так и на уровне после реализации ИС в кремнии (проверка ИС, проверки интеграции ИС в прибор). Это одна из причин, по которым рынок медицинского Интернета вещей развивается медленнее, чем потребительские рынки. Различные применения выдвигают неодинаковые требования к своему использованию. Зачастую как база используется достаточно «зрелая» техника. Соответственно, формулирование требований к новым поколениям медицинской электроники усложняется.

Более того, по мере развития индустрии электронного здравоохранения, включая «медицинский» Интернет вещей и «дистанционную» медицину, увеличивается объем регулирующих требований и документации по выводу новых изделий на рынок. Повышаются риски и издержки освоения новой продукции.

Перед медицинскими приборами Интернета вещей встает также проблема получения признания. Речь идет о разумной стоимости и потенциальных возможностях приборов дистанционного мониторинга здоровья. Число проверок жизненно важных функций за последние несколько лет существенно увеличилось, а требования к медицинской электронике усложнились.

Еще несколько лет назад в медицинских учреждениях плохо понимали, как работать с дистанционными потребительскими приборами и что такая работа в будущем потребует от медицинского сообщества. Сейчас ситуация полностью изменилась. Благодаря использованию таких приборов можно, например, архивировать на больничном сервере показания кровяного давления и т.п. за любой период, а потом при необходимости их извлечь. При этом используемые приборы не обязательно должны быть медицински одобрены – для постановки диагноза можно использовать данные смартфонов, а также специальных браслетов и других носимых устройств, оснащенных медицинскими датчиками. Произошло изменение в подходах: с «это медицинский прибор» на «используем любой прибор, способный дать необходимую информацию». Разумеется, в операционной наиболее жесткий уровень требований к сертификации медицинского оборудования, и использование потребительских приборов недопустимо. Но за ее пределами ситуация другая, и для обеспечения наилучшего мониторинга состояния пациента и его лечения используется все, что

доступно. Налицо своего рода прорыв потребительских приборов в мир профессионального оборудования. Это открывает массу возможностей, помимо возможностей медицинских сертифицированных приборов.

Также открываются недоступные ранее возможности с точки зрения проектирования систем. Рассмотрим, например, слуховые аппараты. Ранее упор делался на минимизацию прибора и продление срока источника питания. Сегодня же слуховые аппараты переживают своего рода технологическую революцию. Дело не только в более гибких корпусах – приборы стали отличаться более адаптивным поведением. Появились привлекательные стандартные функции, такие как возможность управления мобильным телефоном при помощи слухового аппарата, оснащенного Bluetooth. Для того чтобы сделать возможности слуховых аппаратов более изощренными, используются относительно простые ЦОС-процессоры. Благодаря им слуховые аппараты могут определить, в каких условиях находится пользователь (в переполненной комнате или смотрит телевизор), и автоматически подстроить режим работы. Кроме того, слуховой аппарат через мобильный телефон может передавать в медицинский центр данные о частоте пульса, температуре, давлении. Но все эти новые функции одновременно порождают и новые проблемы [10].

Десять основных направлений развития и проблем Интернета вещей на 2017–2018 гг.

Международными специалистами определены 10 основных проблем развития технологий Интернета вещей на ближайшие два года, корреспондирующих с основными направлениями его развития. Отмечается, что Интернет вещей требует широкого спектра новых технологий и навыков, которыми многие организации еще не владеют. Одной из повсеместно проявляющихся проблем в пространстве Интернета вещей является незрелость технологий и услуг, а также их поставщиков. Разработка архитектурных решений проблемы незрелости и управление рисками, которые она создает, будет одним из основных вызовов для организаций, использующих Интернет вещей. Во многих технологических отраслях также возникнут значительные проблемы, связанные с недостатком знаний и опыта. Технологии и принципы Интернета вещей будут оказывать очень серьезное воздействие на организации, их бизнес-стратегии, методики управления рисками и широкий диапазон технических сфер, таких как архитектура и проектирование сетей. Ниже более подробно рассматриваются 10 основных аспектов технологического развития Интернета вещей и связанных с ними проблем, с которыми пользователи будут сталкиваться в 2017–2018 гг.

Безопасность

Интернет вещей открывает широкий диапазон новых рисков и вызовов в области безопасности, угрожающих собственно приборам Интернета вещей, их платформам, операционным системам и системам (средствам) связи, а также системам, с которыми они связаны. Для защиты приборов и платформ Интернета вещей от информационных атак и злонамеренного вмешательства в работу аппаратных или программных средств на физическом уровне потребуются технологии обеспечения безопасности, способные шифровать их системы связи, а также направленные на решение новых проблем, таких как «вещи», выдающие себя за другие (с целью незаконного проникновения в систему), или атаки типа «отказ при выходе из режима ожидания» (denial-of-sleep attack), истощающие батареи.

Обеспечение безопасности Интернета вещей будет затрудняться тем фактом, что многие «вещи» используют простые процессоры и операционные системы (ОС), которые могут не поддерживать сложные подходы к обеспечению безопасности. На данный момент ощущается недостаток опытных специалистов в области безопасности Интернета вещей, решения в области обеспечения безопасности фрагментированы и вовлекают в себя различных поставщиков. В период до 2021 г. появятся новые угрозы, так как хакеры ищут новые способы осуществления атак на приборы Интернета вещей и протоколы, так что «вещи» с длительным сроком службы могут потребовать модернизированного аппаратного и программного обеспечения с целью адаптации на протяжении этого срока к изменениям в системах Интернета вещей, в которых они используются.

Аналитика

Бизнес-модели Интернета вещей будут использовать информацию, собираемую «вещами» относительно самых различных вопросов: например, для понимания потребительских предпочтений, улучшения оказания услуг и продуктов, выявления и перехвата моментов бизнеса. Однако Интернет вещей требует новых аналитических подходов. Уже сейчас требуются новые аналитические инструментальные средства и алгоритмы, однако ожидаемое увеличение объемов данных в период до 2021 г. может привести к тому, что аналитические средства Интернета вещей будут все дальше расходиться с традиционной аналитикой.

Управление приборами

Нетривиальные «вещи» с длительным сроком службы будут требовать управления и мониторинга. Это включает в себя мониторинг приборов, модернизацию микропрограммного и программного обеспечения, диагностику, анализ сбоев и формирование отчетов об этом, управление на физическом

уровне и управление безопасностью[16]. Интернет вещей также приносит в задачи управления новые проблемы масштаба: инструментальные средства должны быть способными осуществлять мониторинг и управление тысячами, а может быть, и миллионами приборов.

Маломощные сети ближнего радиуса действия

Выбор для приборов Интернета вещей беспроводной сети влечет за собой требования балансировки многих конфликтов, таких как диапазон, срок службы батарей, пропускная способность, плотность, стоимость оконечных точек (устройства передачи и/или обработки данных) и эксплуатационных расходов. Среди маломощных сетей Интернета вещей ближнего радиуса действия в период до 2025 г. будет доминировать беспроводная соединяемость. При этом намного большее число соединений будет использоваться в широкомасштабных сетях Интернета вещей. Однако компромиссы технических и коммерческих подходов будут означать, что решения многих проблем будут сосуществовать. Таким образом, появления единого доминирующего победителя или кластера среди определенных технологий, приложений и экосистем поставщиков не ожидается.

Маломощные широкомасштабные сети

Традиционные сотовые сети не обеспечивают хорошего сочетания технических характеристик и эксплуатационных расходов для IoT-применений, которым требуется комбинация широкомасштабного охвата со сравнительно низкой пропускной способностью, длительным сроком службы батарей, низкой стоимости аппаратного оборудования и эксплуатации, а также высокой плотности соединений. Долгосрочной целью широкомасштабных сетей Интернета вещей является достижение скорости передачи данных от сотен бит/с до десятков Кбит/с при общенациональном охвате, срока службы батарей до 10 лет, стоимости аппаратной конечной точки около 5 долл., поддержки сотен тысяч приборов, подключенных к базовой станции или ее эквиваленту. Первые маломощные широкомасштабные сети (LPWAN) были созданы на фирменных технологиях, но в долгосрочном плане возникают стандарты, такие как узкополосный Интернет вещей (Narrowband IoT, NB-IoT), которые и будут доминировать в данной области.

Процессоры

Процессоры и архитектуры, используемые приборами Интернета вещей, определяют многие из их возможностей, то есть будут ли приборы Интернета вещей способны обеспечивать высокий уровень безопасности и шифрования, нужную потребляемую мощность, или же они будут достаточно сложными для поддержки операционной системы, модернизируемого микропрограммного обеспечения и средств управления встроенными приборами. Как и при проектировании аппаратного обеспечения в целом, существуют сложные компромиссы между характеристиками, стоимостью аппаратного обеспечения, стоимостью программного обеспечения, возможностью модернизации программного обеспечения и т.д. В результате для понимания последствий выбора процессора потребуются глубокие технические знания и навыки.

Операционные системы

Традиционные ОС, такие как Windows и iOS, были разработаны не для применений Интернета вещей. Они обладают слишком большой потребляемой мощностью, требуют быстродействующих процессоров и в некоторых случаях – отсутствия таких свойств, как гарантированный отклик в реальном масштабе времени. Они также требуют слишком большого объема памяти (занимаемого программой) для малых приборов и могут не поддерживать ИС, используемые разработчиками Интернета вещей. Соответственно, широкий диапазон специфических ОС Интернета вещей был разработан во многом под другие требования к объему, занимаемому аппаратным обеспечением, а также его характеристикам.

Потоковая обработка событий

Некоторые применения Интернета вещей будут генерировать очень большие скорости передачи данных, которые (данные) необходимо анализировать в реальном масштабе времени. Системы, создающие десятки тысяч событий в секунду, распространены достаточно широко. В некоторых системах, например телекоммуникационных системах и системах телеметрии, передаются миллионы событий в секунду. Для удовлетворения подобных потребностей были созданы вычислительные платформы с распределенными потоками (DSCP). Для обработки потоков с очень высокой скоростью передачи данных они обычно используют параллельные архитектуры, что позволяет решать такие задачи, как аналитика в реальном масштабе времени и распознавание образов.

Платформы

Платформы Интернета вещей связывают в единый продукт большое число инфраструктурных

[16] Security management – управление безопасностью, одна из пяти категорий средств сетевого управления согласно модели ISO, предполагающая процесс управления доступом к сети и ее ресурсам (предоставление, ограничение, допущение, запрещение). Может предусматривать составление и ведение списков доступа в маршрутизаторах (создание брандмауэров), организацию парольной защиты для критических сетевых ресурсов, выявление и блокировку точек возможного проникновения злоумышленников.

компонентов систем Интернета вещей. Услуги, предоставляемые подобными платформами, можно разделить на три основные категории:

1. Низкоуровневые приборы контроля и осуществления таких операций, как связь, мониторинг состояния и управление прибором, обеспечение безопасности данных и обновление микропрограммного обеспечения.
2. Сбор, преобразование и управление данными Интернета вещей.
3. Разработка приложений Интернета вещей, включая событийную логику, прикладное программирование, визуализацию, аналитику и устройства сопряжения для подключения к корпоративным системам.

Стандарты и экосистемы

Хотя стандарты и экосистемы не являются, строго говоря, технологиями, большинство в конечном итоге материализуются в виде интерфейсов прикладного программирования (API). Стандарты и связанные с ними API будут существенными, поскольку приборам Интернета вещей потребуется возможность интероперабельности и поддержания связи. Это обусловлено тем, что многие бизнес-модели Интернета вещей будут опираться на распределенное (совместное) использование данных между многочисленными приборами и организациями.

Как ожидается, возникнет большое число экосистем Интернета вещей, коммерческие и технические сражения между которыми будут определять ситуацию в таких областях, как интеллектуальные дома, интеллектуальные города и здравоохранение. Организациям, создающим продукцию, возможно, придется разрабатывать ее в различных вариантах для поддержки разнообразных стандартов и экосистем. Кроме того, им придется быть готовыми к обновлению продуктов в течение их жизненного цикла по мере развития стандартов, возникновения новых стандартов и связанных с ними API [11].

Роль государственных органов в развитии Интернета вещей

США

Министерство торговли США в рамках стимулирования развития цифровой экономики стремится обеспечить развитие Интернета вещей в качестве открытой платформы. Действуя через собственное Национальное управление по телекоммуникациям и информации (National Telecommunications and Information Administration, NTIA), министерство пытается выяснить, какое место оно должно занимать в развитии Интернета вещей. Для этого через издание «Федеральный регистр» до 23 мая 2016 г. проводился опрос заинтересованных сторон относительно «преимуществ, проблем и потенциальной роли правительства в развитии Интернета вещей». Целью министерства являлся анализ современных технологических и политических решений развития Интернета вещей и подготовка соответствующей «Зеленой книги»[17].

«Зеленая книга» призвана определить основные проблемы, влияющие на развертывание Интернета вещей, потенциальные выгоды и вызовы, возможную роль федерального правительства в ускорении развития Интернета вещей во взаимодействии с частным сектором.

Специалисты Министерства торговли США уже определили значительный потенциал Интернета вещей в таких сферах, как здравоохранение, безопасность, охрана окружающей среды, а также возможность появления новых отраслей промышленности. Особое внимание уделяется вызовам в области безопасности и защиты национальных интересов как в США, так и за рубежом. В рамках обработки предварительных данных опроса отмечается необходимость разработки конкретных стратегий по преодолению возможных вызовов, связанных с развитием Интернета вещей, которые могут привести к увеличению издержек, сроков вывода на рынок новых продуктов и услуг, сокращению инвестиций. Результаты опроса Министерство торговли США намерено использовать для выработки целостного с экономической точки зрения подхода к развитию Интернета вещей, который будет наилучшим образом стимулировать инновационный процесс и рост национальной экономики. В рамках своего исследования Министерство сформулировало 28 вопросов, включая следующие:

- Существуют ли проблемы и возможности, связанные с развитием Интернета вещей, сходные и/или отличные от тех, с которыми общество и правительство сталкивались ранее?
- Какие определения следует использовать при рассмотрении «ландшафта» Интернета вещей и почему?
- В отношении существующих или разрабатываемых законов, подзаконных актов, норм и т.п., применяемых к Интернету вещей, есть ли примеры, которые способствуют или тормозят его развитие?

[17] Green Paper, «Зеленая книга» – официальный правительственный документ, содержащий предложения относительно будущей политики правительства, представляется для обсуждения парламенту. Название – по цвету обложки.

- Существуют ли технологические проблемы (совместимость, наличие спектра и т.п.), которые могут препятствовать развитию IoT, и что может сделать государство для решения этих проблем?
- Какое влияние (положительное или отрицательное) будет иметь развертывание Интернета вещей на рынок рабочей силы США, и какие действия (если таковые имеются) следует предпринять правительству страны во избежание негативных эффектов?
- Какие вопросы (если таковые имеются) относительно Интернета вещей должны привлечь внимание Министерства торговли США в плане международного сотрудничества?

В дополнение к ответам на любой из вопросов министерство просило респондентов поднимать те проблемы, которые покажутся им имеющими отношение к затронутой проблематике [12].

Шпионаж

Безопасностью Интернета вещей озабочены государственные органы различных стран. Так, руководство Национальной разведки США[18] утверждает, что Интернет вещей может использоваться враждебными разведками для наблюдения, сетевого доступа и т.п. Кроме того, Интернет вещей может стать новой сферой деятельности киберпреступников, изыскивающих способы воровства персональной информации. Таким образом, использование Интернета вещей и дает новые возможности разведсообществу США, и создает новые угрозы национальной безопасности.

Эксперты полагают, что американские и зарубежные разведслужбы будут собирать информацию путем перехвата сигналов, передаваемых приборами Интернета вещей, подобно тому как это сейчас осуществляется с сотовыми телефонами.

Интернет вещей определенно привлекает внимание как вполне достижимая для хакеров цель. В начале 2016 г. президент Обама подписал новый «Национальный план действий по обеспечению кибербезопасности» (Cybersecurity National Action Plan), призванный, в частности, обеспечить безопасность приборов Интернета вещей. В рамках данного закона предполагается создание центра тестирования и сертификации приборов Интернета вещей.

Согласно данным отчета Dark Reading (негосударственное сообщество по вопросам информационной безопасности), угроза зомбированных[19] приборов Интернета вещей в 2016–2017 гг. является одной из крупнейших угроз информационной безопасности. Предполагалось, что в 2016 г. хакеры попытаются преобразовать подобные приборы Интернета вещей в Зомби-сеть вещей (BoT) [13].

Проблема обеспечения безопасности данных в связи с увеличением числа подключенных к Интернету вещей приборов

По данным специалистов корпорации Gartner, число подключенных к Интернету вещей приборов за период с 2009 по 2020 г. возрастет в 30 раз – до 26 млрд шт. Объем продаж этих приборов по всему миру достигнет 1,9 трлн долл. Одним из основных преимуществ распространения Интернета вещей является увеличение доступности данных, но по мере их развертывания увеличиваются опасения относительно надежности защиты данных.

Управление безопасностью данных в аппаратном обеспечении

Важными этапами обеспечения безопасности данных являются аутентификация[20] и шифрование. Аутентификация источников формирования и сбора данных является одной из мер обеспечения конфиденциальности/секретности наличной информации. Интернет вещей состоит из большого набора компонентов, включая аппаратное обеспечение, встраиваемое ПО, а также устройств, идентифицируемых с «вещами/объектами». Соответственно, требования защиты данных предъявляются на каждом уровне. Аппаратная защита обычно осуществляется в ИС, поддерживающих «вещи». Математическая безопасность аутентификации и алгоритмы шифрования вызывают меньше опасений, так как они не являются чем-то новым и достаточно хорошо отработаны. Однако хакеры могут использовать недостатки обеспечения безопасности данных в ИС. Одной из главных угроз для безопасности данных

[18] National Intelligence – национальная разведка, правительственный аппарат (при администрации президента) по координации работы всех разведслужб США (разведсообщество из 16 организаций, включая ЦРУ, РУМО и т.п.), собственно разведывательной деятельностью не занимается. Создана согласно «Закону о реформе разведки и борьбы с терроризмом» 2004 г.

[19] Zombie/zombified computer (зомбированный компьютер) – подключенный к Интернету ПК, атакованный (захваченный) хакером, зараженный вирусом или трояном. Обычно – один из ПК целой зомбированной сети (botnet), использующейся для выполнения вредоносных задач под дистанционным управлением злоумышленников, которые рассылают спам (по оценкам, они посылают 80% всего спама в мире), атакуют web-сайты и т.д. Большинство владельцев таких ПК даже не знают об этом.

[20] Authentication (аутентификация, установление подлинности) – служебная функция системы контроля доступа, обеспечивающая сопоставление введенных пользователем пароля и логина с хранимой учетной записью.

в ИС являются атаки по «сторонним» каналам (SCA[21]), направленные на уязвимые данные, к которым относятся пароли пользователей, идентифицирующие данные и секретные ключи, необходимые для аутентификации и алгоритмов шифрования. Специфические SCA включают в себя дифференциальный анализ энергопотребления (DPA) и дифференциальный электромагнитный анализ (DEMA).

Существует много опубликованных и неопубликованных данных относительно атак на безопасность ИС, доступных на рынке. При этом SCA-угрозы быстро развиваются, их потенциал и разнообразие нарастают. Рост угроз обусловливает совершенствование методик защиты, применяемых производителями ИС. При этом защитные методики, применявшиеся в 2012 г., уже в условиях 2014 г. перестали быть эффективными. Более того, по мере появления новых приборов возникают и новые угрозы.

Помимо прочего, существенной трудностью, возникающей у изготовителей ИС, становится растущая сложность методик защиты. Сплошь и рядом защитные методики, являющиеся алгоритмом или специфическим протоколом, являются многослойными решениями, ориентированными на широкий круг угроз. Подход по принципу «лейкопластыря» становится затянутым и громоздким в управлении. Уязвимость к SCA-угрозам может значительно ослабить защиту данных. Эта уязвимость может привести к потере прибыли (включая контрафакт предметов потребления), утрате конфиденциальности (ухудшение идентификационных данных), повреждению аутентификации (появление несанкционированных устройств в закрытых сетях) и т.п.

Повышение устойчивости защиты

Как упрощенный способ рассмотреть проблему SCA можно привести вопрос отношения сигнал/шум. В таком случае сигнал означает уязвимые данные, утекающие сквозь сигнатуру мощности. Шум является акустическим фоном окружающей среды либо произведенным шумом, добавленным в систему для оттенения сигнала, извлекаемого из сигнатуры мощности. Многие современные защитные меры концентрируются на увеличении шума в системе для затенения сигнала. Проблема подобного подхода заключается в появлении статистических методов, нацеленных на выделение сигнала из шума, что приводит к уменьшению потенциала разворачиваемых защитных мер. Эффективным способом преодоления этой проблемы является «вплетение безопасности в ткань проектирования». SCA-угрозы могут адресоваться скорее к источнику проблемы, чем к ее симптомам. Перспективным может быть также создание сигнатуры мощности безотносительно к обрабатываемым данным. Соответственно, защита данных может оказаться более стабильной, если удастся встроить элементы безопасности в «строительные блоки» конструкций. Этим можно будет не только увеличить стабильность защиты, но и упростить ее. Упрощенный подход встраивания аппарата обеспечения безопасности данных в «ткань проектирования» приводит к использованию защищенных библиотек стандартных элементов, устойчивых к SCA-угрозам. Такие библиотеки могут использовать методологии аналогового проектирования в целях решения проблемы SCA-угроз на уровне их источника, уменьшая SCA-сигнал для затруднения его извлечения из сигнатуры мощности. Использование стандартных элементов может быть достаточно простым, так как они являются базовыми строительными блоками логического проектирования. Эти критические этапы обеспечения безопасности данных обойти невозможно [14].

Ожидаемый рост отчислений на обеспечение безопасности Интернета вещей

По данным исследовательской корпорации Gartner, корпоративные и потребительские расходы на обеспечение безопасности Интернета вещей в 2016 г. составят почти 350 млн долл. В ближайшие годы эти расходы будут увеличиваться, так как сети подключенных объектов непрерывно расширяются. В период 2014–2018 гг. отчисления почти удвоятся (табл. 3).

Предполагается, что после 2020 г. отчисления на безопасность Интернета вещей будут расти значительно быстрее, так как будет накоплен наилучший опыт применения, произойдут организационные изменения, появятся более масштабируемые сервисные опции, которые позволят улучшить исполнение задач.

При этом темпы развития Интернета вещей в различных отраслях значительно отличаются, вследствие чего различны уровни как приоритетов, так и осведомленности (персонала/пользователей) о правилах (информационной) безопасности. Соответственно, отличаются и расходы на обеспечение безопасности Интернета вещей. В конечном счете, по оценкам Gartner, по объему расходов на безопасность Интернета вещей будут лидировать следующие

[21] SCA (Side-Channel Attacks) – одно из направлений криптоанализа, описывающее и изучающее атаки на базы данных по «сторонним» каналам. Основная идея данного подхода – шифрующее устройство рассматривается не только как математический аппарат, но и как его конкретная реализация на практике (в т.ч. материальная реализация криптоалгоритма, включая его физические свойства – время выполнения, потребляемая при шифровании мощность, ЭМИ от шифрующего устройства и т.п.).

Таблица 3. Анализ и прогноз мировых отчислений на обеспечение безопасности Интернета вещей

Годы	2014	2015	2016 (оценка)	2017 (прогноз)	2018 (прогноз)
Отчисления, млн долл.	231,86	281,54	348,32	433,95	547,20

секторы: подключенные к сети автомобили, тяжелые грузовики и другие сложные машины; гражданские воздушные суда; оборудование, используемое в сельском хозяйстве и строительстве.

До настоящего времени основное внимание уделялось уязвимости систем безопасности Интернета вещей автомобилей и другого крупного оборудования. Недостаточная степень защищенности потенциально может привести к значительному материальному ущербу, людским потерям (раненые, убитые). В 2015 г. в одной из статей журнала Wired была показана возможность взятия хакером кода управления автомобилем Jeep Cherokee во время езды по скоростному шоссе.

По прогнозу Gartner, в 2020 г. более 25% выявленных атак на системы безопасности предприятий будет осуществляться с использованием Интернета вещей. Однако в корпоративных бюджетах безопасности на собственно Интернет вещей будет по-прежнему приходиться менее 10%. Проблемой поставщиков средств безопасности станут малые бюджеты и начальный уровень разработок. Поставщики, похоже, уделяют слишком много внимания выявлению точек уязвимости и вредоносным кодам, а не сегментированию и другим долгосрочным средствам, которые способны лучше защитить Интернет вещей.

Специалисты считают, что усилия в области безопасности Интернета вещей все больше будут сосредоточиваться на управлении, аналитике и подготовке данных и работе приборов. Сценарии безопасности Интернета вещей потребуют механизмов доставки, которые будут развиваться со скоростью, соответствующей требованиям мониторинга, обнаружения, управления доступом и другим потребностям в области безопасности.

Предполагается, что существенное усилие Интернета вещей по масштабу и присутствию не будет полностью реализовано без «облачных» услуг. В 2020 г. более половины всех реализаций Интернета вещей будут полагаться на ту или иную форму «облачной безопасности» [15].

Интернет вещей как возможная точка роста для российской микроэлектроники

Анализ положения с развертыванием Интернета вещей показывает, что для него вполне пригодна существующая в Российской Федерации производственная база. Освоение Интернета вещей позволит повысить эффективность производства, сферы здравоохранения и других отраслей народного хозяйства. При этом надо учитывать, на основе зарубежного опыта, что развертывание Интернета вещей должно осуществляться на основе открытого протокола при соблюдении мер обеспечения безопасности данных и гарантированно безопасного доступа / пользования сетями Интернета вещей.

Исследования российских ученых-экономистов показывают, что по мере освоения новых материалов и технологических процессов существенно растут издержки производства, затраты на НИОКР и оборудование. Увеличивается необходимость консолидации НИОКР и производственной базы, в том числе за счет процессов расширения частно-государственного партнерства и международного сотрудничества [16–20].

Развертывание Интернета вещей предоставляет возможность загрузки существующих мощностей и использования собственной продукции вместо импортной. При этом представляется целесообразным формирование консорциума и федеральной программы по развитию Интернета вещей. Важнейшими задачами, которые встанут перед ними, будет стандартизация, оптимизация НИОКР различных радиоэлектронных производств и научно-исследовательских организаций, оптимизация федеральных расходов и т.п.

Заключение

Развитие Интернета вещей уже серьезно воздействует на все стороны жизни человека. С точки зрения медицины, управления производством, дорожным движением и т.п. новая технология обладает большим потенциалом. Однако по мере ее развертывания все острее будут вставать вопросы сохранности и обеспечения безопасности данных, обеспечения авторизованного доступа к системам контроля и управления.

Развертывание Интернета вещей также позволяет использовать достаточно зрелые мощности и бывшее в использовании оборудование. То, что для развертывания Интернета вещей не требуются новейшие производственные мощности с дорогостоящим оборудованием и технологиями, характеризующимися передовыми проектными нормами (22/20 нм и менее), делает эту сферу деятельности привлекательной для стран, находящихся в таком же положении, как Россия. Соответственно, сферу Интернета вещей можно использовать как средство накопления финансов, необходимых для развития других направлений отечественной микро- и радиоэлектроники.

СПИСОК ЛИТЕРАТУРЫ

1. Happich J. Transforming the world: IoT, big data and 3D printing. EE Times Europe, Jan. 13, 2015.
2. Макушин М. В. ConFab 2016 – попытка оценки перспектив // Экспресс-информация по зарубежной электронной технике. Вып. 26 (6614) от 7 июля 2016 г. М.: ЦНИИ «Электроника».
3. Gartner: 6.4B connected «Things» in use in 2016. Solid State Technologies. The Pulse, Nov. 13, 2015.
4. Shipments of residential Internet of Things devices expected to total over $330 billion through 2025. Solid State Technologies. The Pulse, Nov. 13, 2015.
5. SITRI, CEA-Leti and MINATEC to cooperate in «More than Moore» technology development. Solid State Technology. The Pulse, March 17, 2016.
6. Merritt R. Intel, ARM Battle over Io T. EE Times, 10/25/2016.
7. Quinnell R. ARM Does IoT Security Chip to Cloud. EE Times, 10/25/2016.
8. Happich J. IoT Boosting MCU Market, Says IHS. EУ Times Europe, 9/21/2015.
9. Connock P. Europe's secondary industry in the spotlight. Solid State Technology. Advanced Packaging, Sept. 22, 2015.
10. Morrison G. Healthcare IoT: Promise And Peril. Semiconductor Engineering, Nov. 3, 2016/
11. Макушин М., Мартынов В., Сухоруслова Ю. Парадигма парадигм, или Интернет вещей // Электроника: Наука, Технология, Бизнес. № 10 (00160). 2016. С. 74–82.
12. Quinnell R. US Government Seeks Guidance On Its Role in IOT. EE Times, 4/12/2016.
13. IoT Next Surveillance Frontier, Says US Spy Chief. InformationWeek GOVERNMENT, News, 2/10/2016.
14. Макушин М. В. О проблемах обеспечения безопасности данных в связи с увеличением числа подключенных к Интернету приборов // Экспресс-информация по зарубежной электронной технике. Вып. 7 (6544) от 26 февр. 2015 г. М.: ЦНИИ «Электроника».
15. McGrath D. IoT Security Spending to Skyrocket. EE Times, 4/25/2016.
16. Оптимизация программных мероприятий развития оборонно-промышленного комплекса. / А. М. Батьковский, А. В. Фомина, Е. Ю. Байбакова, М. А. Батьковский, С. И. Боков, В. В. Клочков, Г. А. Лавринов, А. Н. Стяжкин, Ю. Ф. Тельнов, В. Я. Трофимец, Е. Ю. Хрусталев // под ред. А. М. Батьковского и А. В. Фоминой. М.: Тезаурус, 2014. 504 с.
17. Батьковский А. М., Стяжкин А. Н., Фомина А. В. Инструментарий экономической оценки эффективности инвестиций при анализе инновационного развития предприятий оборонно-промышленного комплекса // Вопросы радиоэлектроники. 2016. № 6. Вып. 5. С. 96–107.
18. Управление рисками инновационного развития базовых высокотехнологичных отраслей / А. М. Батьковский, А. В. Фомина, М. А. Батьковский, В. П. Божко, В. В. Клочков, П. А. Калачихин, А. В. Коновалова, А. Н. Стяжкин, Ю. Ф. Тельнов, Н. Н. Чернышева // под ред. А. М. Батьковского, А. В. Фоминой. М.: Тезаурус, 2015. 332 с.
19. Батьковский М. А., Стяжкин А. Н., Фомина А. В. Инновационное развитие радиоэлектронной промышленности России // Вопросы радиоэлектроники. 2015. № 3. С. 243–258.
20. Развитие fabless-индустрии в КНР и значение ее опыта для отечественных дизайн-центров / П. В. Кравчук, М. В. Макушин, А. Н. Стяжкин, А. В. Фомина // Вопросы радиоэлектроники. 2017. № 1. С. 90–103.

REFERENCES

1. Happich J. Transforming the world: IoT, big data and 3D printing. *EE Times Europe,* Jan. 13, 2015.
2. Makushin M. V. ConFab 2016 – an attempt to assess the prospects. *Express information on foreign electronic engineering.* Issue 26 (6614) of July 7, 2016. Moscow, TsNII «Elektronika» (In Russian).
3. Gartner: 6.4B connected «Things» in use in 2016. Solid State Technologies. *The Pulse,* Nov. 13, 2015.
4. Shipments of residential Internet of Things devices expected to total over $330 billion through 2025. Solid State Technologies. *The Pulse,* Nov. 13, 2015.
5. SITRI, CEA-Leti and MINATEC to cooperate in «More than Moore» technology development. Solid State Technology. *The Pulse,* March 17, 2016.
6. Merritt R. Intel, ARM Battle over IoT. *EE Times,* 10/25/2016.
7. Quinnell R. ARM Does IoT Security Chip to Cloud. *EE Times,* 10/25/2016.
8. Happich J. IoT Boosting MCU Market, Says IHS. *EY Times Europe,* 9/21/2015.
9. Connock P. Europe's secondary industry in the spotlight. Solid State Technology. *Advanced Packaging,* Sept. 22, 2015.
10. Morrison G. Healthcare IoT: Promise And Peril. *Semiconductor Engineering,* Nov. 3, 2016.
11. Makushin M., Martynov V., Sukhoruslova Yu. Paradigm of paradigms, or Internet of Things. *Electronics: Science, Technology, Business,* no. 10 (00160), 2016, pp. 74–82 (In Russian).
12. Quinnell R. US Government Seeks Guidance On Its Role in IoT. *EE Times,* 4/12/2016.
13. IoT Next Surveillance Frontier, Says US Spy Chief. *InformationWeek GOVERNMENT, News,* 2/10/2016.
14. Makushin M. V. On problems of maintained data security in connection with the increasing number of Internet-connected devices. *Express information on foreign electronic engineering.* Issue 7 (6544), February 26. 2015. Moscow, TsNII «Elektronika» (In Russian).
15. McGrath D. IoT Security Spending to Skyrocket. EE Times, 4/25/2016.
16. Batkovskiy A. M., Fomina A. V., Baibakova E. Yu., Batkovskiy M. A., Bokov S. I., Klochkov V. V., Lavrinov G. A., Styazhkin A. N., Telnov Yu. F., Trofimets V. Y., Khrustalev E. Yu. *Optimizatsiya programmnykh meropriyatii razvitiya oboronno-promyshlennogo kompleksa* [Optimization of the program activities of the military-industrial complex]. Under the editorship of A. M. Batkovsky and A. V. Fomina. M.: Thesaurus, 2014. 504 p. (In Russian).
17. Batkovskiy A. M., Styazhkin A. N., Fomina A. V. Tools of economic evaluation of investments efficiency in analysis of innovative development of enterprises of the military-industrial complex. *Voprosy radioelektroniki,* 2016, no. 6, pp. 96–107 (In Russian).

18. Batkovskiy A. M., Fomina A. V., Batkovskiy M. A., Bozhko V. P., Klochkov V. V., Kalachikhin P. A., Konovalova A. V., Styazhkin A. N., Telnov Yu. F., Chernysheva N. N. *Upravlenie riskami innovatsionnogo razvitiya bazovykh vysokotekhnologichnykh otraslei* [Risk Management of innovative development of high-tech industries]. Under the editorship of A. M. Batkovsky, A. V. Fomina, Moscow, Thesaurus, 2015, 332 p. (In Russian).
19. Batkovsky M. A., Styazhkin A. N., Fomina A. V. Innovative development of electronic industry in Russia. *Voprosy radioelektroniki,* 2015, № 3, pp. 243–258 (In Russian).
20. Kravchuk P. V., Makushin M. V., Styazhkin A. N., Fomina A. V. Development of fabless-industry in China and the value of its experience for domestic design centers. *Voprosy radioelektroniki,* 2017, № 1, pp. 90–103 (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Макушин Михаил Викторович, главный специалист, АО «ЦНИИ “Электроника”», 127299, Москва, ул. Космонавта Волкова, д. 12, тел.: 8 (495) 940-65-77, e-mail: makushin_m@instel.ru.
Стяжкин Александр Николаевич, к.э.н., старший научный сотрудник, начальник отдела, АО «ЦНИИ “Электроника”», 127299, Москва, ул. Космонавта Волкова, д. 12, тел.: 8 (495) 940-65-85, e-mail: stiazhkin_a@instel.ru.
Фомина Алена Владимировна, д.э.н., генеральный директор, АО «ЦНИИ “Электроника”», 127299, Москва, ул. Космонавта Волкова, д. 12, тел.: 8 (495) 940-65-00, e-mail: instel@instel.ru.

AUTHORS

Makushin Mikhail, chief specialist, Central Research Institute «Electronics», 12, Kosmonavta Volkova st., Moscow, 127299, Russian Federation, tel.: +7 (495) 940-65-77, e-mail: makushin_m@instel.ru.
Styazhkin Aleksandr, PhD, head of department, Central Research Institute «Electronics», 12, Kosmonavta Volkova st., Moscow, 127299, Russian Federation, tel.: +7 (495) 940-65-86, e-mail: stiazhkin_a@instel.ru.
Fomina Alena, Doctor of Economic Sciences, general director, Central Research Institute «Electronics», 12, Kosmonavta Volkova st., Moscow, 127299, Russian Federation, tel.: +7 (495) 940-65-00, e-mail: instel@instel.ru.