

IoT-радиопроцессор с криптокодированием структуры радиосигнала

Алексей Галицын (Москва)

Описанная в статье технология обеспечивает реализацию новой парадигмы в архитектуре и обеспечении безопасности беспроводного Интернета вещей (IoT), ориентированных на конвергенцию Интернета вещей и концепции «туманных вычислений». Предлагаемый подход обеспечивает простоту и прозрачность построения безопасного локального мира умных вещей и его подключения к Интернету, эргономичность архитектуры систем, простоту обеспечения и высокий уровень безопасности, уникальную помехозащищённость при многократном снижении себестоимости радиосистем Интернета вещей (IoT), Индустриального Интернета вещей (IIoT) и Всеобъемлющего Интернета (IoE) в будущем.

ВВЕДЕНИЕ

Мировая полупроводниковая индустрия вышла на уровень «систем на кристалле» (System on Chip – SoC). На этом уровне развития полупроводниковая фабрика, производя кристалл, фактически будет производить функционально законченное изделие (электронную часть Вещи). Существует очень большая вероятность того, что в ближайшие несколько лет ведущие производители классических универсальных микросхем большой степени интеграции переориентируются на производство готовых изделий – систем на кристалле для «своих» умных вещей массового гражданского и военного рынков. Поэтому сегодня не приходится надеяться на Западный мир, который в области полупроводников уже вышел на уровень «систем на кристалле» и осознал, что производить (в ущерб себе) и поставлять в Россию даже микросхемы прошлого века – значит терять огромные рынки вооружений.

Всё это может привести к большим проблемам (не исключая санкционные) для подавляющего большинства приборостроительных предприятий России, использующих импортную элементную базу [1]. Об этом неустанно, в течение 20 лет, заботится наше правительство: закупает полупроводниковые фабрики, выделяет денежные средства госкорпорациям на приобретение оборудования для дизайн-центров по проектированию кристаллов (SoC) для военной и космической техники. При этом умалчивается тот факт, что не только развивать полупроводниковую индустрию, но даже просто покупать и

содержать полупроводниковые фабрики на средства госбюджета не может себе позволить ни одна страна мира, кроме России (даже США). Как результат – отечественные фабрики практически не загружены (нет конкурентоспособной продукции), а затраты на их текущее содержание огромны и дотируются из бюджета. И это в то время, когда без собственной элементной базы, без дизайн-центров по проектированию систем на кристалле, не только «Цифровая экономика» или оборонная промышленность, но и сам технический прогресс в стране может стать невозможным уже завтра.

Более того, к проектированию собственных систем на кристалле большинство российских приборостроительных предприятий попросту не готово. Количество дизайн-центров, способных создавать конкурентоспособные системы на кристалле, крайне ограничено – их единицы.

Полупроводниковая индустрия и IoT

К счастью, Интернет «перевернул» нашу жизнь, и человечеству, наконец, стало ясно, что следующим этапом развития техники будет подключение к Интернету сотен миллиардов умных киберустройств: дорогих и дешёвых, больших и маленьких, безобидных и взрывоопасных – любых. Наступила новая эпоха – эпоха Интернета вещей [2].

По данным всемирного исследования PwC Digital IQ® за 2017 год, Интернет вещей (IoT) занимает первое место среди восьми прорывных технологий, спо-

собных изменить бизнес-модели компаний или целых индустрий, опережая в этом рейтинге искусственный интеллект, дополненную реальность, технологию, связанную с созданием дронов и управление ими, блокчейн и целый ряд других «сверхновых» технологий [3].

Рынок Интернета вещей – это (в отличие от других) действительно безграничный рынок электроники ближайшего и даже отдалённого будущего. Вместе с тем развитие Интернета вещей в России и за рубежом сдерживается наличием ряда объективных проблем.

Проблема № 1 – макроэкономическая. Заключается она в желании лидеров окупить затраты на разработку устаревшей техники за счёт технологически отсталых стран. Интернет вещей будущего будет беспроводным и мировой подход в области IoT – это создание IoT «эволюционно», на элементной базе и RF-стандартах, исторически созданных для совершенно других целей. Такой подход будет продвигаться монополиями до тех пор, пока затраты на эту элементную базу не окупятся за счёт технологически отсталых стран (в их числе Россия) или пока ситуация с IoT не зайдёт в тупик. Российский путь в области IoT – это «следование за лидером» – продвижение на российский рынок решений, реализованных на импортной элементной базе, что способствует захвату рынка иностранными компаниями и уничтожению отечественной полупроводниковой индустрии.

Проблема № 2 – эргономическая. Заключается она в несоответствии архитектуры систем новым вызовам и задачам. С развёртыванием LTE и 5G Интернет будет подведён к каждому метру урбанизированного пространства и необходимость в «дальнобойных» локальных RF-технологиях Интернета вещей, широко разрекламированных сегодня, практически отпадёт. Существующие методы создания беспроводного Интернета вещей «ближнего действия» основаны на технологиях локальных беспроводных сетей прошлого века, использующих для адресации устройств, распределения каналов и борьбы с коллизиями центра-

лизованные контроллеры-координаторы и сетевые операционные системы – что крайне не эргономично, тем более сегодня, когда новым интерфейсом взаимодействия человека с виртуальным, а теперь и с реальным миром, становится смартфон. Однако и для соединения смартфона с окружающими его вещами предлагается использовать или «транс-континентальные» облачные соединения, или устаревшую технику беспроводных сетей прошлого века.

Проблема № 3 заключается в обеспечении безопасности [4, 5]. IoT (IoE) будущего будет беспроводным, т.е. легко доступным (для проникновения в сеть не потребуется даже электрического подключения к ней), и его главная проблема – кибербезопасность. Но существующие механизмы безопасности Интернета при его расширении до уровня IoT – т.е. через эфир «за браузер» – напрямую не применимы, что требует огромных затрат и радикальных изменений в идеологии и механизмах безопасности существующей сети Интернет. Кроме того, появление 30 млрд IoT-устройств к 2020 г. гарантирует появление в любом конкретном локальном, не лицензируемом RF-пространстве множества функционально разных IoT-систем. И уже в ближайшем будущем никакие системы борьбы с коллизиями не смогут обеспечить их ЭМС-совместимость как друг с другом, так и с уже существующими в нём радиосредствами.

Проблема № 4 – проблема импортозамещения и безопасности объектов критической инфраструктуры. Не секрет, что Интернет вещей может оказаться глобальным информационным оружием, целенаправленно размещаемым на территории потенциального противника. При расширении сети Интернет до уровня вещей этому информационному оружию становится подвержен не только «моральный дух», финансовые потоки, но даже сами объекты гражданской и критической инфраструктуры. Игнорировать подобные риски преступно. На сегодняшний день только импортозамещение может уберечь от вредоносных «закладок» в компьютерные технологии и обеспечить национальную безопасность.

НОВЫЕ ВОЗМОЖНОСТИ

Новым интерфейсом для взаимодействия человека с виртуальным миром и «миром» окружающих его реальных вещей становится смартфон. Но,

для осуществления этого взаимодействия и для построения самого «мира вещей» («умного дома», «умной квартиры», «умного цеха») нужны совершенно другие (сверхнадёжные) радиочастотные технологии и новые архитектуры. В новых условиях вещи должны получить возможность перерегистрации в разных системах, а распределённые прикладные процессы должны гарантированно автономно работать каждый в своей локальной радиосреде, имея возможность доступа и к облачным сервисам. Наконец, смартфону нужен такой коммуникационный сопроцессор для непосредственного прямого взаимодействия с «миром вещей», который гарантирует безопасность этого взаимодействия (независимо от уровня квалификации разработчика прикладных систем) и который станет технической основой для создания самого этого безопасного «мира вещей».

К сожалению, в отечественных программах развития страны и, в частности, в Национальной программе «Цифровая экономика Российской Федерации» Интернет вещей понимается весьма примитивно. Речь в этих программах идёт лишь об узкополосных радиоканалах большого радиуса действия для «счётчиков электроэнергии и электролампочек» с IP-адресами, как будто все «умные вещи» во всех квартирах и все станки во всех цехах Индустрии 4.0 обязаны общаться между собой исключительно посредством «дальнобойных» узкополосных радиоканалов через общие центральные базовые станции или через станции сотовых операторов. Локальные беспроводные сенсорные сети, созданные в прошлом веке для совершенно других целей, когда-то имели право на существование, но в настоящее время также являются анахронизмом, противоречащим современной концепции «туманных вычислений» (fog-computing), которая поддержана мировыми технологическими лидерами: компаниями Cisco, Microsoft, Dell, ARM, Intel и даже... Администрацией Президента РФ [6].

Смешно сказать, но главную проблему Интернета вещей – проблему безопасности – создатели Национальной программы «Цифровая экономика» предлагают решить весьма экзотическим образом. Для этого «к сетям IoT должны быть подключены системы средств оперативно-розыскных мероприятий (СОПМ) и внесены изменения в закон „О связи“» [7].

Таким образом, даже после «успешного» завершения Национальной программы «Цифровая экономика» в области IoT у России так и останутся всё те же, указанные выше, проблемы.

Рынок Интернета вещей – это быстрорастущий рынок, который к 2020 году составит \$7–10 трлн, а это четверть бюджета США или современного Китая.

Такой объём рынка при разумном подходе мог бы «поднять» (по примеру Южной Кореи и Тайваня) не только полупроводниковую индустрию России, но и всю страну вместе с её нефтегазовым бюджетом.

На этой «финансовой волне» автор предлагает решить Проблему № 1 – возрождение электронной индустрии страны, Проблему № 2 – исключение из архитектуры Интернета вещей беспроводных сетей прошлого века, привязанных к инфраструктуре (повсеместность обеспечат LTE и 5G) и Проблему № 3 – безопасность Интернета вещей (посредством создания защищённой и недоступной для кибератак локальной радиосреды) и создания самого «Мира Вещей» на основе российской C-UWB RF-технологии с криптографической защитой структуры радиосигнала.

Данная технология использует радиочастотный спектр на вторичной основе, обеспечивает бесконфликтность в отношении существующих RF-стандартов, высочайшую помехозащищённость и криптографическую уникальность каждого соединения. Таким образом появляется возможность простого (доступного для массового разработчика), универсального, а главное – безопасного подключения вещей к Интернету, без разрушения идеологии и механизмов безопасности существующей сети Интернет, т.е. её инфраструктуры. При этом автоматически будет решена и проблема импортозамещения (проблема № 4).

ПРЕДЛАГАЕМОЕ РЕШЕНИЕ

Предлагаемая инновация заключается в создании универсального, информационно-безопасного элемента – IoT-радиопроцессора (IP-блок, SoC, Chip-set, +Soft) с криптокодированием структуры радиосигнала. Данный радиопроцессор послужит инструментом создания локального (R=100–200 м) радиопространства глобальной информационной среды будущего и базовым элементом построения локального «Мира умных вещей». Это позволит

разместить «Мир вещей» в локальном радиочастотном пространстве на вторичной основе, без конфликтов с существующими радиочастотными стандартами и технологиями, обеспечив при этом непосредственную радиочастотную адресацию устройств друг другом, принципиальную недоступность для кибератак, высочайшую помехозащищённость и минимальную себестоимость подключения вещей к Интернету [8, 9].

На рисунке показано место IoT-радиопроектора в архитектуре систем.

В проекте реализуется новая парадигма в обеспечении безопасности беспроводного Интернета вещей, основанная на перенесении криптозащиты с информации на структуру радиосигнала. Другими словами, криптозащита переносится со сложнейших протоколов безопасности на аппаратуру, что существенно упрощает проектирование систем и автоматически гарантирует безопасность соединений массовому разработчику [9, 10]. Тем самым обеспечивается принципиальная недоступность соединений для кибератак и исключение из состава транспортной инфраструктуры IoT-систем целого транспортного уровня – уровня беспроводной локальной сети и соответствующего оборудования (сетевых ОС, контроллеров-координаторов, маршрутизаторов и т.п.), что позволяет значительно снизить себестоимость систем.

Для осуществления криптокодирования структуры радиосигнала может быть применена разработанная российская C-UWB RF-технология, базиру-

ющаяся на псевдослучайных кодовых криптопоследовательностях и использующая RF-спектр на вторичной основе. Предлагаемая технология основана на корреляционной обработке сложного широкополосного радиосигнала и принципе кодового разделения каналов [9, 10].

При этом для обеспечения безопасности в существующей сети Интернет не придётся ничего ломать. Посредством стандартной техники Интернета (VPN-соединения, SSL-протоколы) будет обеспечено безопасное взаимодействие прикладных процессов новой точки доступа (смартфон, планшет, компьютер) с Интернетом (web-серверами, сайтами и «облаками»), а посредством нового информационно-прозрачного, но криптографически защищённого по структуре радиосигнала беспроводного соединения, будет обеспечено безопасное взаимодействие этих прикладных процессов собственно с вещами (т.е. обеспечение следующего уровня расширения сети). Соответственно и прикладные процессы в рамках концепции «fog-computing» должны будут строиться с учётом новой архитектуры нижнего уровня сети и этих новых возможностей по обеспечению безопасности.

Такой подход позволит сохранить все существующие механизмы безопасности классической сети Интернет (всю её инфраструктуру – что называется «до браузера»), т.е. сохранить все механизмы, обеспечивающие безопасное взаимодействие прикладных процессов, происходящих в компьютерах и смарт-

фонах (fog-узлах) с сайтами, серверами и «облаками», одновременно обеспечив простоту, прозрачность, а главное – высочайший уровень безопасности информационного взаимодействия этих процессов с вещами, а вещам – безопасное взаимодействие напрямую между собой.

Эта новая концепция в обеспечении безопасности, в которой средства безопасности предоставляются массовому разработчику прикладных систем Интернета вещей не в виде непонятных ему стеков протоколов, а в виде готового беспроводного чипа (IP-блока для систем на кристалле), гарантирующего и автоматически обеспечивающего безопасность любого и каждого беспроводного соединения на периферии сети.

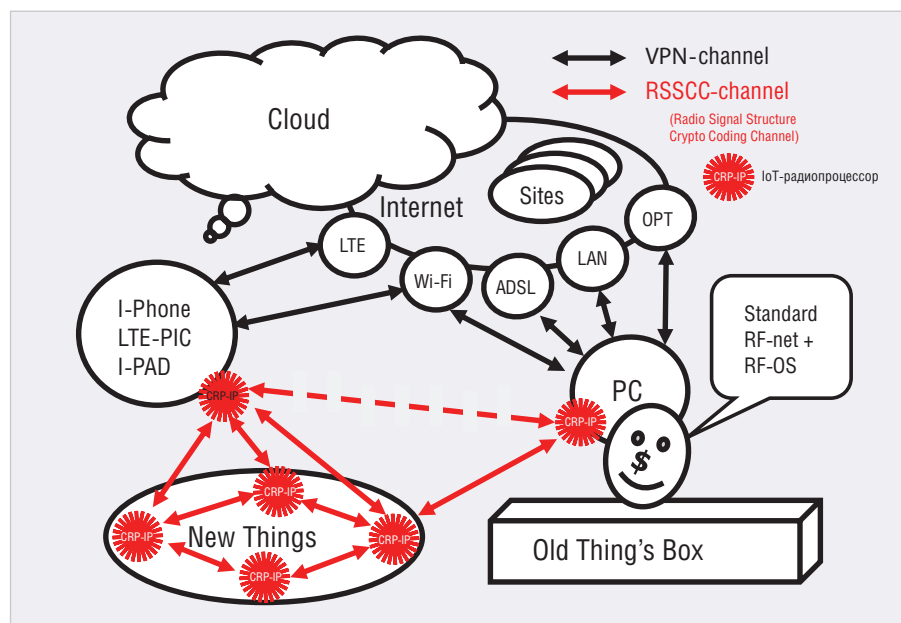
В свою очередь, корреляционная обработка радиосигнала позволяет с помощью принципа кодового разделения каналов перенести и процесс адресации устройств с логического (адресация на основе информации, полученной после демодуляции радиосигнала) на физический уровень обработки самого радиосигнала (до его демодуляции). Тем самым обеспечивается прямая, т.е. непосредственная адресация устройств друг другом без участия средств, выполнявших эти функции в традиционных радиосистемах (контроллеры-координаторы, сетевые операционные системы и т.п.).

Используя радиочастотный спектр на вторичной основе, C-UWB RF-технология на физическом уровне обработки радиосигнала (благодаря корреляционной обработке радиочастотного сигнала и кодовому разделению каналов) автоматически решает и проблему коллизий. Это позволяет обеспечить взаимодействие смарт-коммуникаторов с вещами, а вещей – напрямую между собой без участия привязанных к инфраструктуре посредников – контроллеров-координаторов и сетевых ОС, тем более без участия серверов, расположенных за рубежом, что удобно, надёжно, эргономично и безопасно.

Кроме того, для нашей российской C-UWB RF-технологии удалось предложить простые и эффективные методы подавления помех и повысить помехозащищённость радиосистем ещё на два порядка по сравнению с самой «стойкой» технологией ZigBee [11].

ОБЛАСТЬ ПРИМЕНЕНИЯ

Предлагаемый проект ориентирован на самый массовый (в будущем) сегмент



Место IoT-радиопроектора в архитектуре систем

мирового рынка Интернета вещей – на создание «мира» непосредственно взаимодействующих между собой умных вещей, окружающих человека ($R=100-200$ м), на подключение этого «мира» к сети Интернет и обеспечение взаимодействия с ним человека через новый интерфейс – смартфон (в будущем – смарт-коммуникатор).

Предлагаемый чип изначально предназначен для создания горизонтальных «туманных» архитектур (fog-computing), имеющих доступ к «облакам», где распределённые прикладные процессы будут гарантированно автономно работать каждый в своей локальной радиосреде («на своей земле», «на своём заводе», «в своей квартире»). Доступ к облачным сервисам будет осуществляться через новые стационарные (наподобие подключённых к Интернету компьютеров) или мобильные (наподобие смартфонов) точки доступа, в которые, также как и в вещи, будет имплантирован чип или IP-блок (в системы на кристалле) предлагаемого IoT-радиопроцессора. На основе этого чипа (IP-блока) будет возможно построение как собственно этого безопасного «мира умных вещей», подключённого к глобальной сети Интернет, так и непосредственное, информационно-прозрачное (доступное для массового разработчика), но в то же время безопасное взаимодействие человека с этим новым «миром вещей». Это взаимодействие будет осуществляться посредством нового интерфейса – смартфона, причём без «посредников» в виде традиционных, располагаемых на местности контроллеров-координаторов беспроводной локальной радиосети и сетевых операционных систем.

Таким образом, IoT-радиопроцессор – это чип микроконтроллера со встроенной памятью и безопасным беспроводным интерфейсом передачи данных для соединения с такими же чипами в локальном радиопространстве, имеющих интерфейсы для связи с глобальной транспортной инфраструктурой сети Интернет. Непосредственно к чипу могут подключаться всевозможные датчики температуры, света, напряжения, излучения, положения в пространстве и т.п. Повсеместность покрытия территорий этой «локальной» технологией будет обеспечена сетями LTE и 5G. Для этого в смартфоны будет имплантироваться предлагаемый чип (IP-блок) IoT-радиопроцессора. Данное решение ста-

нет своеобразной базовой технологией для «туманных вычислений». С помощью таких микрочипов, допускающих возможность соединения вещей между собой и подключения к Интернету, можно создать реально безопасную распределённую сеть устройств и развернуть (масштабировать) её на всю планету.

Выводы

1. Используемые в проекте подходы к построению Интернета вещей в корне меняют архитектуру, эргономику и себестоимость радиосистем. В свою очередь простота и прозрачность построения безопасного локального «мира вещей» и подключения вещей к Интернету, доступность этого процесса для массового разработчика, эргономичность архитектуры систем, простота обеспечения безопасности, уникальная помехозащищённость при многократном снижении себестоимости радиосистем – всё это делает представленный подход и технологию безальтернативными для создания беспроводного Интернета вещей и Индустриального Интернета будущего.

2. Предлагаемый IoT-радиопроцессор может сыграть такую же ключевую роль в создании мировой индустрии Интернета вещей, какую супергетеродин сыграл в создании радио-, а микропроцессор – компьютерной индустрии. России это позволит не только сохранить полупроводниковую индустрию страны, но и кардинально решить проблему импортозамещения и безопасности в этом сегменте электроники. При этом приборостроительным предприятиям и полупроводниковым фабрикам страны (за счёт представленных интеллектуальных преимуществ, а не технологических преимуществ отечественный завод) будет открыт новый безграничный, причём мировой рынок Всеобъемлющего Интернета (IoT+IIoT+IoE).

3. Проект может существенно повлиять на соотношение сил и распределение прибылей от полупроводниковой индустрии между Европой, Китаем, США и Россией, поскольку объём IoT-рынка по прогнозам практически всех аналитических изданий уже к 2020 году сравняется с четвертью бюджета США. Даже небольшая доля этого рынка могла бы позволить России не только сохранить полупроводниковую индустрию страны, но и кардинально

решить проблему импортозамещения и безопасности в этом самом крупном и самом массовом сегменте рынка электроники как ближайшего, так и весьма отдалённого будущего.

ЗАКЛЮЧЕНИЕ

К сожалению, ни профессионалы в Правительстве, закупившие за \$1 млрд полупроводниковую фабрику «Ангстрем-Т» и не знающие, что с ней дальше делать [12, 13, 14], предлагающие создать с нуля 100 дизайн-центров в «Ростехе» (стоимостью от \$5,0 млн каждый) и привлечь 40 тыс. «студентов» для сложнейшего и дорогостоящего процесса проектирования SoC-кристаллов [15], ни их ставленники – «экономисты-финансисты» в профильных министерствах, собравшие устаревшие «предложения» со всех предприятий ВПК (3–5 тыс. СБИС малых серий, которые даже теоретически в обозримые сроки невозможно разработать), выставившие счёт государству на 400 млрд рублей и страждущие в предвкушении распределения этих средств посредством «векторной детализации желаемого состояния подотрасли в метрически и топологически изоморфной форме базового структурного опытно-производственного норматива существующей структуры подотрасли, представляющего собой вектор, компоненты которого охватывают весь цикл воспроизводственного кругооборота... что позволит завершить программу импортозамещения унифицированной номенклатуры электронно-компонентной базы страны к 2021 году» [16], – все эти люди, десятилетиями распределяющие финансовые ресурсы государства, весьма далеки от понимания того, что на таких, с позволения сказать, «предложениях» полупроводниковую индустрию не построишь и что массовые прорывные технологии не «рождаются» от студентов, а «вынашиваются» десятилетиями в головах выдающихся, профессионально подготовленных людей.

Именно поэтому полупроводниковые фабрики страны простаивают, а российским трендом в области IoT стало «следование за лидером» – продвижение на российский рынок решений, реализованных на импортной элементной базе, что способствует захвату иностранными компаниями самого последнего (из возможных

для российских фабрик) сегмента рынка полупроводников (IoT-сегмента) и уничтожению отечественной полупроводниковой индустрии как таковой.

ЛИТЕРАТУРА

1. Алексенко А.Г., Галицын А.А., Иванников А.Д. Проектирование радиоэлектронной аппаратуры на микропроцессорах. – М.: Радио и связь, 1984. – 270 с.
2. Зараменских Е.П. Интернет вещей. Исследования и область применения. Монография / Е.П. Зараменских. – М.: ИНФРА-М, 2016. – 752 с.
3. <https://constanta.co/news/20180305-vsemirnoe-issledovanie-digital-iq-za-2017-god-pwc/>
4. Леонов А.В. Интернет вещей: проблемы безопасности. Омский научный вестник. 2015. № 2 (140). С. 215–218.
5. Кринен Г. Безопасность «Интернета Вещей»: существующие проблемы и их решение. Инноватор. 2017. № 1. С. 8–12.
6. <https://www.kommersant.ru/doc/3026455>
7. <https://www.kommersant.ru/doc/3924324>
8. Галицын А.А. Интегральный радиопроцессор – перспективная техническая основа Интернета вещей. Датчики и системы. 2015. № 1.
9. Галицын А.А. Технология C-UWB – основа для информационно-телекоммуникационных систем нового поколения. Электроника: наука, технология, бизнес. 2008. № 5.
10. Патент на изобретение № 2557451 RU. Способ динамической адресации корреспондентов мобильной радиосети и устройство для его реализации. Авт. Галицын О.И. – приоритет от 08.06.2012.
11. US Patent № 7.250.541 B2. Method for suppressing narrowband noise in a wideband communication system. / Inv.: M.Bobkov, A.Galitsyn, V.Kalugin. Priority date 22.08.2002.
12. <https://www.vedomosti.ru/business/articles/2019/01/09/791045-angstrom-t-pereshel-pod-kontrol-vebrf>
13. <http://government.ru/news/35766/>
14. <http://government.ru/news/35609/>
15. <http://government.ru/news/36007/>
16. Шнак В.В. Микроэлектроника как двигатель четвертой технологической революции. Тезисы доклада на конференции «Научная парадигма цивилизации в XXI веке: капитализм, социализм и четвертая технологическая революция». Челябинский государственный университет, Челябинск, 17–19 октября 2018 г. С. 76–77.



НОВОСТИ МИРА

QUALCOMM – ЛИДЕР РЫНКА ПОЛУПРОВОДНИКОВЫХ РЕШЕНИЙ В ОБЛАСТИ 5G

Qualcomm, ведущая в мире компания по производству полупроводниковых приборов, в ближайшие 2–5 лет сможет добиться значительных успехов в области телекоммуникаций 5G, считают в аналитической компании GlobalData.

5G – это мобильная сеть следующего поколения, которая по сравнению с современными сетями 4G обещает гораздо более высокую скорость соединения, меньшую задержку и повышенную надёжность. Предполагается, что эти преимущества будут иметь решающее значение для новых технологий, таких как автономные транспортные средства и дополненная реальность, которые, в свою очередь, окажут большое влияние на другие отрасли.

Международный союз электросвязи (ITU) разделяет сферы использования 5G на 3 основные категории:

1. Мобильная широкополосная связь с видео высокой чёткости и дополненной/виртуальной реальностью (AR/VR).

2. Массовая связь между электронными устройствами, обеспечивающая растущие потребности развивающегося Интернета вещей (IoT).

3. Сверхнадёжная связь с малой задержкой, которая чаще всего упоминается применительно к автономным транспортным средствам, но также важна для IoT в таких отраслях, как здравоохранение и производство.

В последних исследованиях GlobalData проанализированы основные технологические, макроэкономические и нормативные факторы, затрагивающие полупроводниковые компании, и показано, что



Qualcomm занимает лидирующую позицию в области 5G.

Сети 5G всегда позиционировались как революционная технология, обещающая фундаментальные перемены на производственном и бытовом уровне. Это привело к тому, что планка ожидания была завышена до такого уровня, что любой достигнутый результат станет разочарованием. В последние годы операторы связи из всех сил пытались превратить растущий спрос на услуги мобильной передачи данных в рост доходов, но 5G откроет ряд новых источников дохода, особенно на вертикальных рынках, таких как энергетика и коммунальные услуги, производство и здравоохранение.

Уход Intel из бизнеса смартфонов 5G позволил Qualcomm, сыгравшей большую роль в становлении стандарта 5G, ещё больше укрепить свои позиции на данном рынке. Недавно Qualcomm урегулировали юридический спор с Apple, которая теперь будет покупать у них модемные микросхемы и, как ожидается, выпустит смартфон 5G в

2020 году. Именно после достижения договорённостей между Apple и Qualcomm Intel заявила о выходе из бизнеса 5G-смартфонов. Тем не менее в Intel считают, что беспроводные системы пятого поколения всё ещё дадут им возможность продавать большое количество микросхем для использования в сети.

По оценкам GlobalData, число потребителей 5G в 2019 году составит менее 5 млн, но уже к 2023 году это число увеличится почти до 850 млн при феноменальном совокупном годовом росте (CAGR) в 271%. Ожидается, что доля мобильных абонентов 5G вырастет с 0,05% в 2019 году до более чем 8% к 2023 году.

По расчётам GlobalData, трафик данных 5G в 2019 году составит 0,09% от общего объёма по сравнению с 77% в 4G и 22% в 3G. Однако ожидается, что доля 5G будет быстро расти до тех пор, пока к 2023 году она не превысит долю 3G-трафика. Сети 4G по-прежнему останутся наиболее используемой технологией, обеспечивающей 3/4 всего трафика данных в 2023 году.

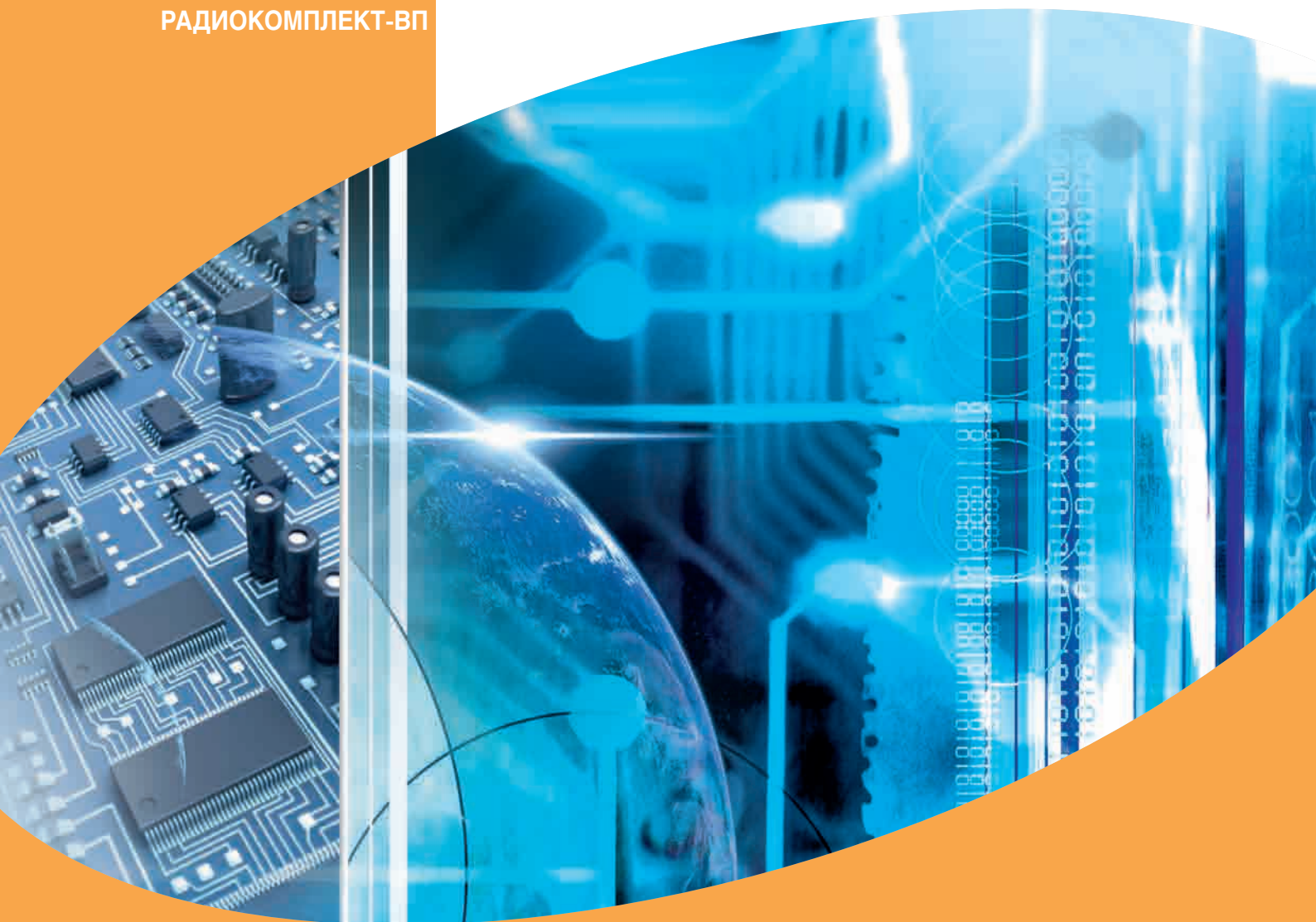
www.globaldata.com



РАДИОКОМПЛЕКТ-ВП

ПОСТАВЩИК ЭЛЕКТРОННЫХ КОМПОНЕНТОВ

российских и зарубежных производителей



- Комплексная поставка электронных компонентов импортного производства, стран СНГ и России
- Печатные платы, твердотельные накопители
- Инверторы, конвертеры, источники питания, зарядные устройства для всех типов аккумуляторов
- Постоянно в наличии весь ряд SMD-компонентов и электрических соединителей
- Работаем в соответствии с основными федеральными законами №223-ФЗ от 18.07.2011, №44-ФЗ от 05.04.2013, №275-ФЗ от 29.12.2012
- СМК соответствует требованиям ГОСТ ISO 9001-2011, ГОСТ РВ 0015-002-2012, ЭС РД 009-2014, ЭС РД 010-2015

НОВОСТИ МИРА

GLOBALDATA НАЗВАЛА 13 ЛИДЕРОВ ПОЛУПРОВОДНИКОВЫХ ТЕХНОЛОГИЙ В ОБЛАСТИ ПРОМЫШЛЕННОГО ИНТЕРНЕТА

По мнению аналитиков из GlobalData, IBM, Qualcomm, STMicroelectronics и Texas Instruments являются одними из ведущих мировых полупроводниковых компаний, которые в ближайшие 2–5 лет смогут наиболее успешно работать на рынке промышленного интернета.

Согласно выводам GlobalData, промышленный интернет является одним из десяти основных направлений, которые будут влиять на сектор полупроводников, наряду с центрами обработки данных, искусственным интеллектом (ИИ), высокопроизводительными вычислениями, внешней торговлей, автономными транспортными средствами, играми, 5G, рынком слияний и поглощений (M&A) и геополитикой.

Последние исследования GlobalData, в которых анализируются основные технологические, макроэкономические и нормативные вопросы, касающиеся полупроводниковых компаний, показывают, что Xilinx,

Micron, ASML Holding, Analog Devices, Rohm, Aixtron, Renesas, Infineon и Silicon Labs также входят в группу компаний-лидеров в области промышленного интернета.

Компании, которые инвестируют в правильные направления, тем самым пишут свою «историю успеха», в отличие от тех, кто эти направления игнорирует. В 1999 году General Electric (GE) была крупнейшей компанией в мире по рыночной стоимости, однако с 2015 года, несмотря на то что она всё ещё является промышленным лидером, GE отстаёт в области промышленного интернета.

В последнем докладе GlobalData Thematic Research говорится о том, что промышленный интернет является частью быстро развивающейся экосистемы интеллектуальных машин, работающих и взаимодействующих друг с другом по собственной логике. По прогнозам GlobalData, рынок промышленного Интернета к 2023 году составит \$145 млрд.

Лидерство на данном рынке захватили специалисты в области программного обеспечения, анализа данных и ИИ, развивающие сотрудничество с такими отраслями,

как производство, энергетика, фармацевтика, коммунальное хозяйство и сельское хозяйство. В этих отраслях в настоящее время активно внедряются технологии датчиков и ИИ, которые приводят к значительным изменениям в работе предприятий. Чтобы промышленный интернет работал эффективно, потоковые данные из множества источников должны собираться и анализироваться в режиме реального времени для последующей передачи в промышленные приложения.

Активное повсеместное внедрение датчиков обусловлено резким снижением их стоимости, что, в свою очередь, помогает стимулировать ценовую конкуренцию, поскольку на рынке появляется всё больше производителей. В 2004 году средняя цена датчика составляла \$1,3; а уже к 2020 году ожидается её снижение до 38 центов. Рынок датчиков очень динамичен и характеризуется очень высокой конкуренцией, при этом сами датчики становятся более интеллектуальными – в результате следует ожидать появления более удобных интерфейсов, которые облегчат взаимодействие с датчиками и сбор данных с них.

www.globaldata.com

swissbit®
INDUSTRIAL MEMORY SOLUTIONS



Серия S-40: карты памяти SD и MicroSD для эффективных промышленных применений

- 4–32 Гбайт (MLC NAND Flash)
- SD 3.0 (2.0), SDHC, Class 6
- Передача данных до 24 Мбайт/с
- Автономная система управления данными
- Защита от пропадания напряжения
- Долгое время хранения данных при экстремальных температурах
- Резервирование встроенного программного обеспечения
- Сложный механизм распределения нагрузки и управления сбоями блоками
- Обновление параметров и встроенного программного обеспечения
- Контроль изменений в комплектации
- Инструменты для диагностики

**Надежные, прочные,
экономичные**

ProSOFT®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU



Реклама

НОВОСТИ МИРА

ИТОГИ ИССЛЕДОВАНИЯ РЫНКА РЕШЕНИЙ ДЛЯ ПОВЫШЕНИЯ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ

В мире происходит активный переход от цифровизации активов к внедрению технологий «цифрового работника» как обязательного фактора сохранения лидерства на конкурентном рынке. Системы класса HSE 4.0 становятся глобальным трендом цифровой трансформации систем управления производственной безопасностью, охраной труда и окружающей средой (Health, Safety and Environment).

В «Исследования мирового и российского рынка современных решений для автоматической идентификации персонала на промышленных объектах с целью повышения производственной безопасности (HSE 4.0)» от J'son & Partners Consulting впервые собрана и структурирована информация о существующих и перспективных инновационных технологиях, направленных на идентификацию персонала, его действий и состояний, а также аспектов его взаимодействия с опасным оборудованием/машинами/инструментами и окружающей средой с целью повышения уровня производственной безопас-

ности. Акцент был сделан на технологии, позволяющие решать эти задачи в автоматическом real-time-режиме без участия оператора. При этом основной фокус внимания аналитиков J'son & Partners Consulting был сделан на изучении технологий, применимых и актуальных именно для процессинговых отраслей (горнодобывающая/нефтегазовая промышленность).

Все решения разделены на 8 классов, включая интеллектуальные системы обеспечения безопасности в периметре работы оборудования, интегрированные платформы автоматизации производственной безопасности, специализированные платформы позиционирования персонала и идентификации его состояний и действий в режиме реального времени, а также машинное зрение и ситуационную видеоаналитику для целей производственной безопасности.

Отдельная глава исследования посвящена обзору конкретных кейсов применения рассмотренных классов решений в мире. Это даёт комплексное представление о том, как лидеры рынка Oil & Gas и Mining внедряют и используют инновации для обеспечения высокого уровня производственной безопасно-



сти, каких стратегий они придерживаются в вопросах цифровизации HSE, какого уровня технологического развития уже удалось достичь в этом направлении и какие у компаний планы по дальнейшему освоению инноваций.

В отчёте также содержится информация, позволяющая оценить уровень развития в России технологий идентификации персонала для целей производственной безопасности, в том числе представлено описание российских компаний, работающих в этой нише, предлагаемых ими решений (функционал, архитектура, уровень технологичности и т.д.), опыта интеграции, накопленного к настоящему моменту, и планов по дальнейшему развитию.

Пресс-служба J'son & Partners Consulting



Преимущества

- Специально разработанные изделия
- Интеграция с MasterSCADA
- Готовые конфигурации IS-MSCADA-A5/AL – для систем до 1000 точек IS-MSCADA-C5/AL – для систем без ограничений



РОССИЙСКИЙ АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ СИСТЕМ АВТОМАТИЗАЦИИ И ДИСПЕТЧЕРИЗАЦИИ В ПРОМЫШЛЕННОСТИ

От разработчиков отечественных средств автоматизации — Advantix, FASTWEL и ИнСАР



ProSoft®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU

Рис. 100