DOI: 10.22184/1992-4178.2019.185.4.46.49

Система на кристалле SmartFusion2 от Microsemi: оптимальное решение для Интернета вещей

В. Ежов

УДК 621.3.049.774 | ВАК 05.27.01

Системы и компоненты Интернета вещей (IoT) должны отвечать целому ряду требований, в частности таких как низкое энергопотребление, компактные габариты, высокий уровень безопасности коммуникаций и защиты данных. Корпорация Microsemi – единственная компания, которая предлагает устройства на основе программируемой логики, полностью отвечающие всем требованиям к IoT-инфраструктуре. Системы на кристалле на базе ПЛИС (SoC FPGA) семейства SmartFusion2 от Microsemi позволяют создавать гибкие системы, которые отличаются минимальной потребляемой мощностью и самым высоким уровнем защиты, доступным для ПЛИС. В этих микросхемах применены лучшие в своем классе решения для обеспечения безопасности, предотвращающие возможность несанкционированного доступа, незаконного копирования данных или установки вредоносного кода.

Корпорация Microsemi, ставшая в 2018 году частью компании Microchip Technology, известна своими разработками в области ПЛИС, отличающимися повышенной надежностью и возможностью применения в жестких условиях эксплуатации. Благодаря характерному для микросхем программируемой логики этой компании уникальному сочетанию характеристик, их можно применять в широком спектре приложений, в том числе в коммуникационных и автомобильных системах, военном и космическом оборудовании, промышленности, медицинской аппаратуре, центрах обработки данных и других областях.

Такие особенности, как чрезвычайно низкая потребляемая мощность, оптимальное соотношение цены и функциональных возможностей, а также усовершенствованные средства обеспечения безопасности, позволяют применять ПЛИС от Microsemi в перспективной сфере Интернета вещей. Корпорация Microsemi предлагает широкий спектр устройств программируемой логики малой и средней емкости на основе флеш-технологии, в том числе радиационно-стойкие ПЛИС. В портфолио компании представлены как автономные ПЛИС, так и СнК на базе ПЛИС (SoC FPGA), в состав которых входит процессорная подсистема. Последний класс устройств наиболее эффективен для создания проектов в области Интернета вещей, поскольку обеспечивает максимальные функциональные возможности при минимальных габаритах и потребляемой мощности.

Оптимальный выбор для разработчика IoT-системы – СнК семейства SmartFusion2, особенности которой рассмотрим подробнее.

СнК SmartFusion2 содержит энергонезависимую матрицу ПЛИС четвертого поколения, выполненную по флеш-технологии, полноценную процессорную подсистему на базе процессора ARM Cortex-M3 с набором периферии, а также высокоскоростные коммуникационные интерфейсы (рис. 1). ПЛИС на основе флеш-памяти не требует применения внешней памяти для загрузки конфигурации. Поэтому устройства готовы к работе практически сразу после включения, кроме того, отсутствует возможность считывания конфигурационных данных во время загрузки, что обеспечивает защиту конфиденциальной информации. Конфигурационная флеш-память не подвержена однократным сбоям (Single-Event Upset – SEU) из-за воздействия ионизирующих излучений, что позволяет применять их, например, в условиях космического пространства.

Следует отметить, что надежности своих устройств компания Microsemi уделяет повышенное внимание. Для этого, в частности, в СнК SmartFusion2 реализован целый ряд мер. Например, микросхемы оснащены средствами исправления одиночных ошибок и обнаружения двойных ошибок (Single Error Correct Double Error Detect – SECDED) для ряда узлов, включая Ethernet-буферы, PCIe-буфер, встроенную сверхоперативную память процессора Cortex-M3, буферы сообщений CAN, USB-буферы, а также контроллеры DDR-памяти с опциональным режимом SECDED. Кроме того, в СнК SmartFusion2 буферы, оснащенные устойчивыми к SEU защелками, используются в DDR-мостах, кэш-памяти команд, SPI FIFO-памяти. При включении устройства и по запросу производится проверка целостности флеш-памяти, чтобы гарантировать сохранность данных.

Используемая в СнК матрица ПЛИС, изготавливаемая по 65-нм технологическому процессу, построена на основе 4-входовых LUT (LookUp Table) с цепями переноса, оптимизированных для низкого энергопотребления и высокой производительности. Кроме того, матрица ПЛИС содержит отдельные триггеры, которые можно использовать независимо от LUT. 4-входовые LUT можно конфигурировать так, чтобы реализовать любую 4-входовую комбинаторную функцию или арифметическую функцию, в которой выход LUT и вход переноса могут быть включены по схеме «исключающего ИЛИ» для формирования выхода суммы.

В состав ПЛИС входит до 236 блоков 2-портовых СОЗУ (Large SRAM) объемом 18 Кбит, которые обеспечивают скорость обмена данными до 400 МГц, и до 240 блоков 3-портовых 1-кбит СОЗУ (Micro SRAM) с двумя портами для чтения и одним портом для записи. В СнК SmartFusion2 интегрировано до 240 высокопроизводительных математических блоков, оптимизированных для цифровой обработки сигнала и содержащих умножители, сумматоры и управляющие регистры.

Одна из наиболее сильных сторон ПЛИС от Microsemi, в частности СнК SmartFusion2, – рекордно низкая потребляемая мощность как в статическом, так и в динамическом режимах. Это обеспечивает длительное время работы устройств от батарей – одно из ключевых требований IoT-инфраструктуры. В устройствах реализован режим особо низкого потребления Flash*Freeze, в котором статическое потребление микросхемы может составлять менее 1 мВт. В дежурном режиме энергопотребление порядка 10 мВт. При включении питания и во время конфигурирования ПЛИС на базе флеш-памяти экономятся сотни мВт мощности, в результате суммарный выигрыш по энергопотреблению СнК SmartFusion2 может достигать 50% по сравнению с конкурирующими решениями.

При проектировании системы Интернета вещей один из важнейших факторов – обеспечение информационной безопасности. В СнК SmartFusion2 наряду с традиционными

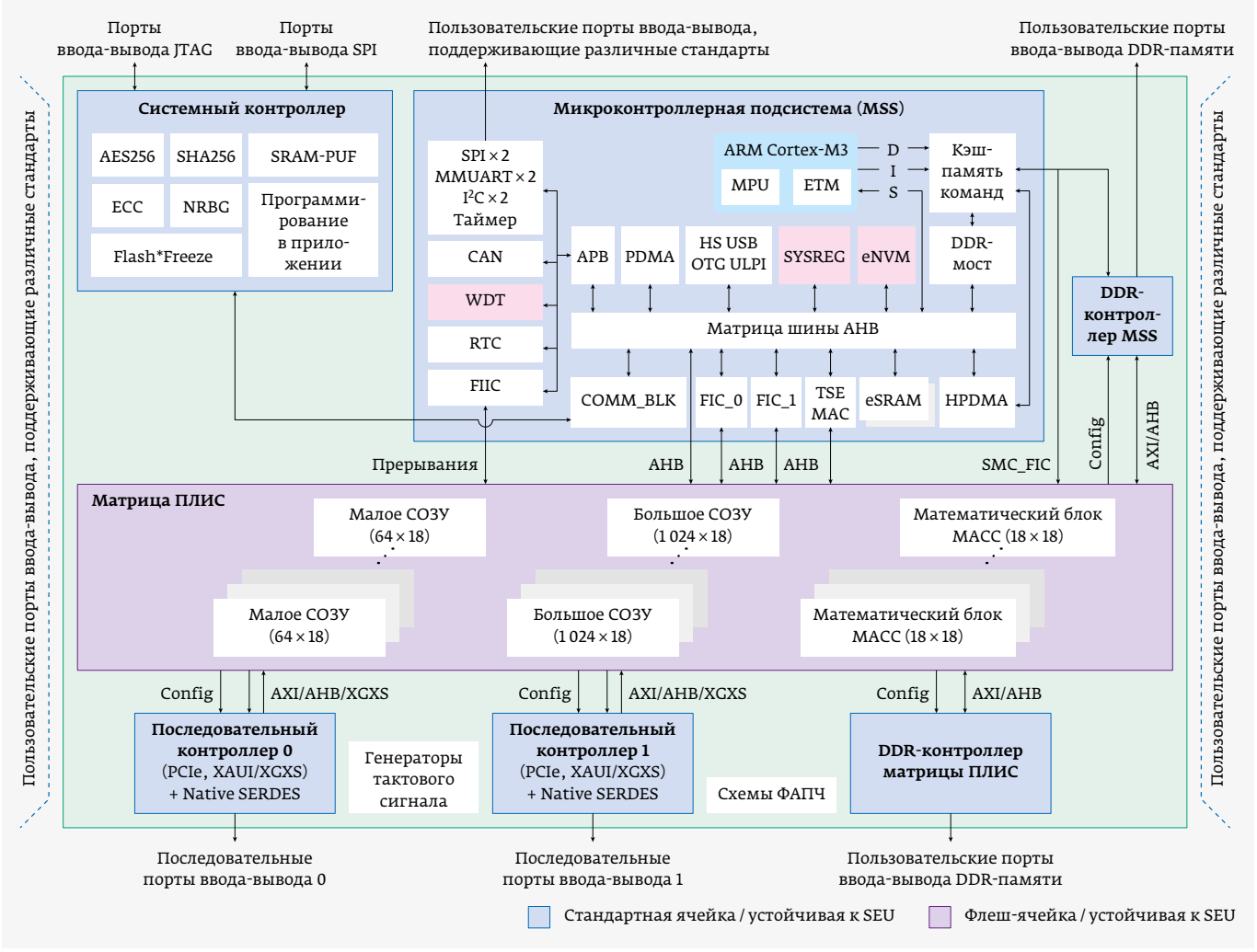


Рис. 1. Блок-схема СнК SmartFusion2

используются уникальные сервисы, которые раньше не применялись в сфере ПЛИС. В микросхемах реализованы функции защиты не только информации о проекте (IP-защита), но и данных. Первый тип защиты, который предотвращает внесение изменений в проект и обеспечивает контроль количества копий проекта, представлен во всех моделях семейства и включает следующие возможности:

- загрузку пользовательского ключа шифрования с помощью уникального секретного ключа, встроенного в микросхему в процессе производства;
- проверку корректности программирования устройства даже в слабо защищенных условиях;
- сохранение всей цепочки технологических процессов для исключения незаконного копирования информации о проекте;
- дифференциальный анализ энергопотребления (differential power analysis – DPA) и усиленные функции защиты от несанкционированного вмешательства;
- возможность обнуления (очистки) всех критичных данных, хранящихся в устройстве, в момент несанкционированного вмешательства.

Наряду с этим две модели семейства SmartFusion2 – M2S080 и M2S120 – обеспечивают такие функции защиты, как криптография на основе эллиптических кривых (Elliptic Curve Cryptography – ECC) для безопасной загрузки пользовательских ключей и реализация физически неклонируемой функции (Physical Unclonable Function – PUF) для аутентификации устройства.

В СнК SmartFusion2 встроены также усовершенствованные функции защиты данных, которые хранятся и обрабатываются в конечном приложении, например:

- сервис недетерминированного генератора случайных двоичных последовательностей (NRBG);
- криптографический сервис пользователя (реализующий такие стандарты шифрования, как AES-128/-256, SHA-256 и HMAC);
- аппаратные средства сетевой защиты (firewalls) доступа к памяти микроконтроллерной подсистемы (MSS).

Кроме того, в моделях M2S080 и M2S120 реализованы сервис ECC-вычислений и сервис регистрации и регенерации пользовательских PUF-ключей для приложений, требующих усиленных мер защиты данных.

Микроконтроллерная подсистема (microcontroller subsystem – MSS) СнК SmartFusion2 включает в себя аппаратный 32-разрядный процессор ARM Cortex-M3, работающий на тактовой частоте 166 МГц. Устройство содержит кэш команд объемом 8 кбайт, встроенную макроячейку трассировки (embedded trace macrocell – ETM) для упрощения разработки и отладки приложений, а также модуль защиты памяти (memory protection unit – MPU) для поддержки операционной системы реального времени. В процессоре, производительность которого достигает 1,25 DMIPS/МГц, реализовано умножение за один цикл и аппаратное деление. Для отладки предусмотрены интерфейсы JTAG (4-проводный), 2-проводный SWD (Serial Wire Debug) и SWV (Serial Wire Viewer).

Микроконтроллерная подсистема содержит встроенное ОЗУ (eSRAM) объемом 64 кбайт, энергонезависимое ПЗУ (eNVM) объемом до 512 кбайт, трехскоростной модуль Ethernet (Triple Speed Ethernet – TSE) со скоростями 10/100/1000 Мбит/с, контроллер USB2.0 High Speed OTG с интерфейсом ULPI. Контроллер CAN2.0B, удовлетворяющий требованиям ISO 11898-1, содержит 32 передающих и столько же принимающих буферов. В состав периферии MSS входят интерфейсы SPI, I^2C, многорежимные UART (по два блока каждого типа), а также аппаратный сторожевой таймер, один 64-разрядный или два 32-разрядных таймера общего назначения, часы реального времени, DDR-мост (4-портовый буферированный мост чтения/записи данных в DDR-память) с 64-разрядным AXI-интерфейсом.

MSS содержит также неблокирующую многоуровневую матрицу шины AHB, позволяющую подключать десять ведущих и семь ведомых устройств, а также два AHB/APB-интерфейса для подключения матрицы ПЛИС (в режиме ведущий/ведомый). Кроме того, в состав MSS входят два контроллера прямого доступа к памяти (DMA):

- 8-канальный периферийный DMA-контроллер (PDMA) для обмена данными между MSS-периферией и памятью;
- высокопроизводительный DMA-контроллер (HPDMA) для обмена данными между eSRAM- и DDR-памятью.

СнК SmartFusion2 содержит набор узлов для генерирования тактовых сигналов, в том числе два RC-генератора (частотой 1 и 50 МГц), до двух прецизионных генераторов с кварцевой стабилизацией частоты (32 кГц – 20 МГц) и до восьми схем формирования тактовых сигналов (Clock Conditioning Circuits – CCC) с блоками ФАПЧ и программируемой частотой и фазой сигнала.

Микросхемы оснащены высокоскоростными последовательными интерфейсами с поддержкой основных протоколов передачи данных. В состав устройств входит до 16 модулей последовательно-параллельного преобразования (SERDES), каждый из которых поддерживает протоколы PCI Express 2.0, XGXS/XAUI (для реализации 10-Гбит/с трансивера Ethernet), Serial Rapid IO и SGMII.

В состав высокоскоростных интерфейсов памяти СнК SmartFusion2 входит до двух контроллеров DDR-памяти (в том числе контроллер DDR-памяти микроконтроллерной подсистемы (MDDR) и контроллер DDR-памяти матрицы ПЛИС (FDDR)) с поддержкой LPDDR/DDR2/DDR3. Контроллеры DDR-памяти обеспечивают максимальную частоту тактового сигнала до 333 МГц, поддерживают различную разрядность шины DRAM (x16, x18, x32, x36), включение/отключение коррекции ошибок (SECDED) и возможность изменения порядка команд и данных для оптимизации работы с памятью. Кроме того, предусмотрена поддержка SDRAM-памяти.

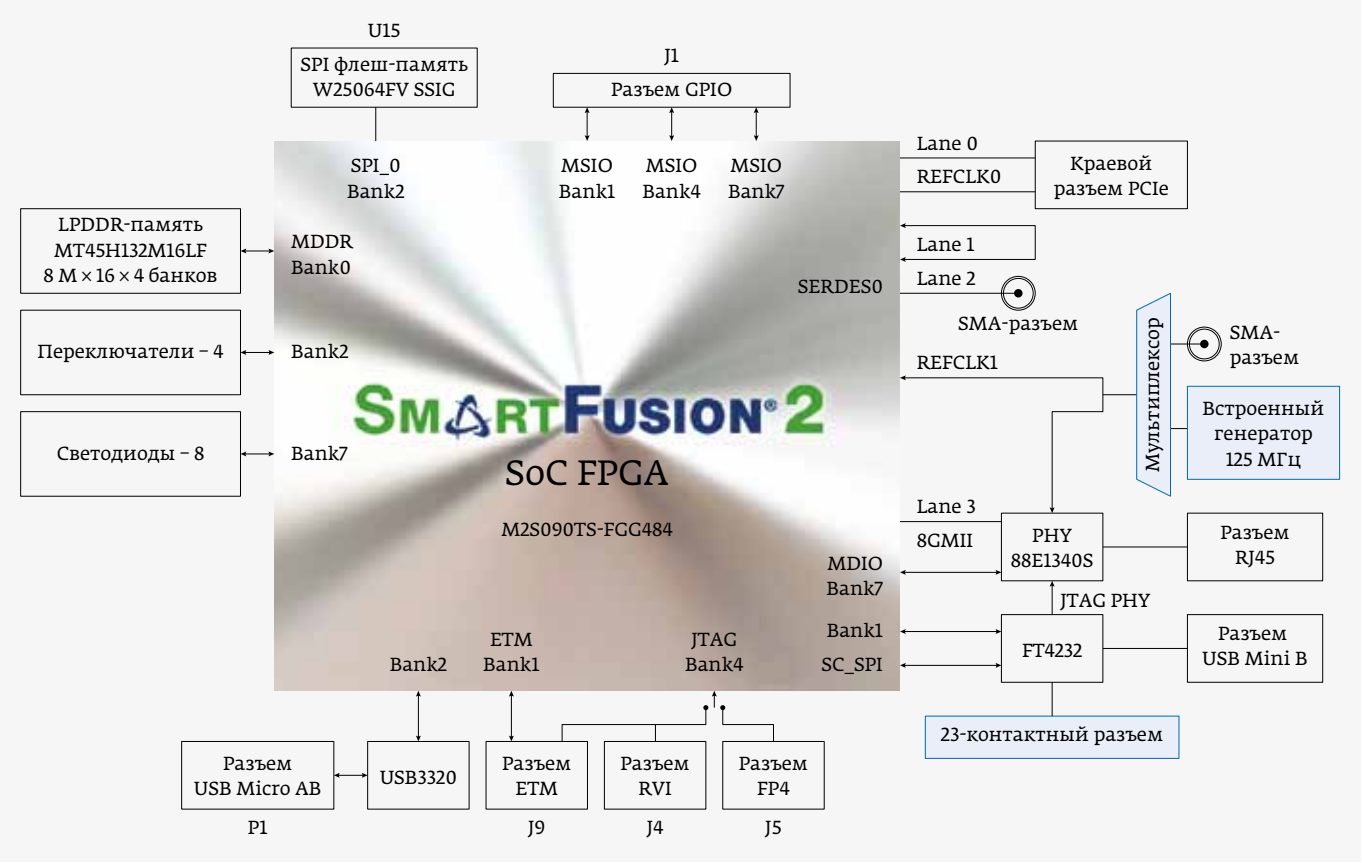


Рис. 2. Структурная схема оценочного комплекта M2S090TS-EVAL-KIT для разработки встраиваемых систем защиты на базе СнК SmartFusion2

Корпорация Microsemi предлагает ряд типовых решений для Интернета вещей на базе СнК SmartFusion2. Как уже было отмечено выше, одна из основных проблем IoT-инфраструктуры – обеспечение безопасности, предусматривающей защиту M2M-коммуникаций, данных и IP-блоков проекта. Для быстрой разработки встраиваемых систем защиты Microsemi предлагает оценочный комплект M2S090TS-EVAL-KIT на базе СнК SmartFusion2, который обеспечивает эффективную платформу для разработки надежных и оптимизированных по стоимости проектов в области безопасности (рис. 2).

Оценочный комплект содержит микросхему SmartFusion2 с матрицей ПЛИС объемом 90 тыс. логических элементов в корпусе FGG484. Ресурсов этой микросхемы достаточно для создания проектов на базе трансиверов ввода-вывода для построения интерфейсов PCI Express и Gigabit Ethernet. PCIe-совместимая плата оценочного комплекта дает возможность быстро создать и протестировать прототип системы, используя любой ПК или ноутбук, оснащенный слотом PCIe. Комплект позволяет исследовать возможности СнК SmartFusion2 в области обеспечения безопасности, например, криптографию на основе эллиптических кривых, применение генератора псевдослучайных чисел, физически неклонируемой функции (PUF) и др.

В состав платы входит разъем RJ45 для интерфейса с сетями 10/100/1000 Ethernet, 512 Мбит LPDDR, 64 Мбит SPI флеш-память, разъем USB-UART, разъемы для подключения интерфейсов I^2C, SPI, а также разъем для GPIO. В комплекте представлен 12-В источник питания, однако возможно также питание платы от краевого PCIe-разъема. Кроме того, набор комплектуется JTAG-программатором FlashPro4 и золотой лицензией на программный пакет инструментов Libero SoC для разработки проектов на базе ПЛИС.

* * *

В заключение остается отметить, что СнК SmartFusion2 от Microsemi – оптимальное и высокоинтегрированное решение для создания продуктов для инфраструктуры Интернета вещей, которое обеспечивает низкое энергопотребление, широкие функциональные возможности, отличается компактными размерами и масштабируемой безопасностью коммуникаций, данных и IP-блоков проекта.

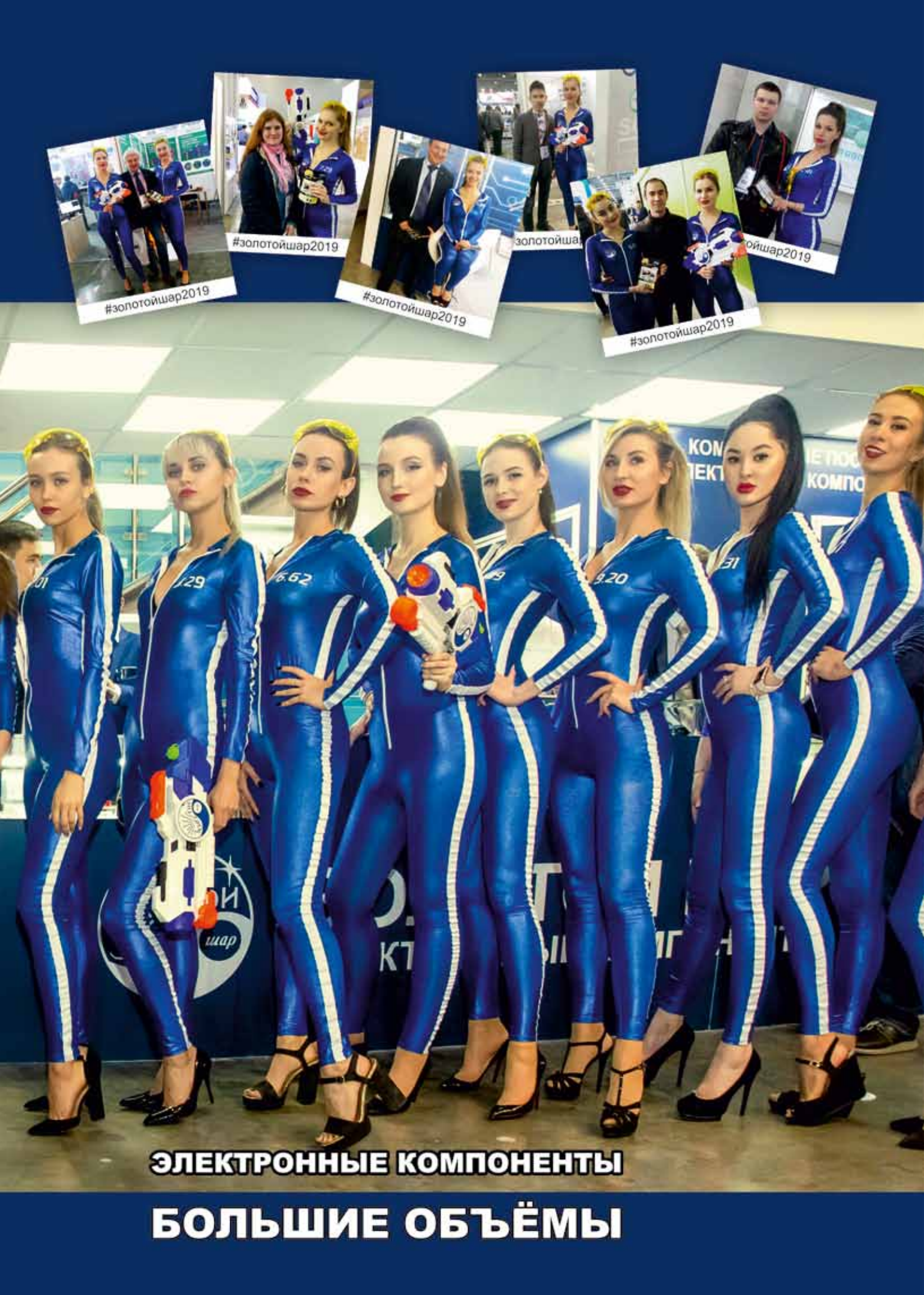
Для получения более подробной технической информации по продукции Microchip Technology и заказа продукции/образцов обращайтесь в холдинг «Золотой Шар». ●

ЗОЛОТОЙ ШАР

КОМПЛЕКТНЫЕ ПОСТАВКИ
ЭЛЕКТРОННЫХ КОМПОНЕНТОВ

+7 (495) 234-01-10 www.zolshar.ru

ШИРОКИЙ АССОРТИМЕНТ



ЭЛЕКТРОННЫЕ КОМПОНЕНТЫ

БОЛЬШИЕ ОБЪЁМЫ