МИКРОКОНТРОЛЛЕР АО «ПКК МИЛАНДР» С ПОДДЕРЖКОЙ СОВРЕМЕННЫХ МЕТОДОВ УПРАВЛЕНИЯ ЭЛЕКТРОПРИВОДАМИ И КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

СТАНИСЛАВ ГУСЕВ, ведущий инженер отдела разработки цифровых ИС, АО «ПКК Миландр»,
СЕРГЕЙ ШУМИЛИН, директор Центра проектирования интегральных микросхем, АО «ПКК Миландр»

АО «ПКК Миландр» является одной из наиболее динамично развивающихся компаний на рынке отечественных интегральных микросхем и оборудования на их основе. Главным направлением работы компании является проектирование и производство современных микроконтроллеров на базе высокопроизводительных вычислительных ядер.

В настоящее время линейка микроконтроллеров компании состоит из широкого ряда микросхем разного назначения, начиная со стойких к воздействию специальных факторов микроконтроллеров, ориентированных на применения в экстремальных условиях, и заканчивая недорогими коммерческими микросхемами для оборудования гражданского назначения.

Одной из наиболее перспективных систем на кристалле, запущенных недавно в производство, является микроконтроллер на основе двух ядер Cortex-M4F с блоками обработки переменных с плавающими запятыми, ядра Cortex-M0 в составе криптостойкой подсистемы, широкого набора периферийных устройств с высокоскоростными периферийными интерфейсами и развитыми контроллерами АЦП и ШИМ, что делает систему пригодной не только для выполнения специализированных задач, но и для использования в качестве контроллера общего назначения в современных цифровых системах. В таблице 1 представлены основные параметры нового микроконтроллера.

Структурная схема разрабатываемого кристалла представлена на рисунке 1. Структурно микроконтроллер состоит из двух частей:

- открытой области на основе двух ядер ARM Cortex-M4F с широким набором цифро-аналоговых устройств и интерфейсных контроллеров;
- «защищенной» области на основе ядра Cortex-M0 с блоками S- и L- преобразований и длиночисленной арифметики для реализации криптографических алгоритмов.

Таблица 1. **Основные параметры микроконтроллера**

	Параметры микроконтроллера
Тактовая частота, МГц	150
Процессорное ядро	2 × Cortex M4F + Cortex M0
Питание, В	3,0/3,63
Регулятор питания	LDO или DCDC+LDO
Температура, °C	–40…125
Потребление, мА	300
Толерантность 5 В	нет
Количество и параметры АЦП	6 × 8-канальных 12-разрядных АЦП 2 MSPS
Дифференциальный режим АЦП	есть
Количество ШИМ	9 ШИМ × 2 канала + 4 × таймера
HRPWM	есть
Другие специализированные блоки для электропривода	4 × CAP, 2 × QEP, 3 × COMP, 3 × DAC, CORDIC
Размер флэш-памяти, Кбайт	1024
Размер RAM, Кбайт	256
Размер RAM криптографической подсистемы, Кбайт	128 (ОЗУ данных) + 2 (память ключей)
Номенклатура корпусов	PGA144, BGA144, LQFP144
Число GPIO	96
Интерфейсы	2 × CAN, 1 × I2C, 2 × SPI, 4 × UART, 1 × USB 2.0, 1 × Ethernet, 1 × STD 1553
Состав криптографического вычислителя	8 × S-преобразований, 1 × L-преобразование, 1 × P-байт, 4 × P-бит, 1 × DES-раунд, сопроцессор длинночисленной арифметики
Поддерживаемые криптографические алгоритмы	ГОСТ Р 34.12-2015 («Кузнечик»), «Магма», ГОСТ Р 34.11-2012 («Стрибог»), ГОСТ 34.10-2012, DES, AES, RSA

Для вычислительных ядер ARM Cortex-M4F в открытой части микроконтроллера предусмотрены два режима работы – Lock Step и Dual Core.

Режим Lock Step предназначен для решения критических задач, требующих надежного контроля бессбойного хода выполнения программы. В этом режиме первое ядро микроконтроллера является ведущим и осуществляет обращение к памяти и регистрам, выполнение программы пользователя и управление всей системой. Второе ядро получает все данные, запрошенные ведущим ядром, дублирует его работу с задержкой в два такта рабочей частоты микроконтроллера, сравнивает данные и результат их обработки с ведущим ядром, вызывает аппаратное прерывание в случае их расхождения.

Режим Dual Core предназначен для задач, требующих максимальной производительности. В этот режим микроконтроллер переходит программным образом из режима Lock Step. После перехода в режим Dual Core оба процессорных ядра становятся независимыми, могут приступить к выполнению задач и имеют равноправный доступ к ресурсам системы. Этот режим рекомендуется для выполнения задач, требующих высокой производительности системы. Он особенно эффективен для слабосвязанных между собой задач, осуществляющих управление подсистемами микроконтроллера. Например, пока одно из ядер выполняет сложные специализированные алгоритмы, второе может использоваться для общего управления системой и связи по высокоскоростным интерфейсам.

Каждое из вычислительных ядер имеет собственный DMA-контроллер и два собственных блока кэш-памяти для инструкций (64 слова) и констант (8 слов). Наличие собственных блоков кэш-памяти для каждого процессора позволяет сохранить максимальную производительность каждого из ядер в режиме Dual Core. Системная рабочая частота составляет 160 МГц. При включении механизмов защиты памяти от одиночных сбоев в банках ОЗУ максимальная частота ограничивается величиной 150 МГц.

В состав микросхем входит энергонезависимая флэш-память программ объемом 1 Мбайт, 256 Кбайт ОЗУ данных. При этом из ОЗУ данных также возможно выполнение программы. ОЗУ микроконтроллера, разделенное на четыре банка, обеспечивает бесконфликтный доступ обоих ядер Cortex-M4F. Кроме того, допускается работа микросхемы с внешними ИС памяти с помощью контроллера внешней системной шины с поддержкой кодирования ECC для

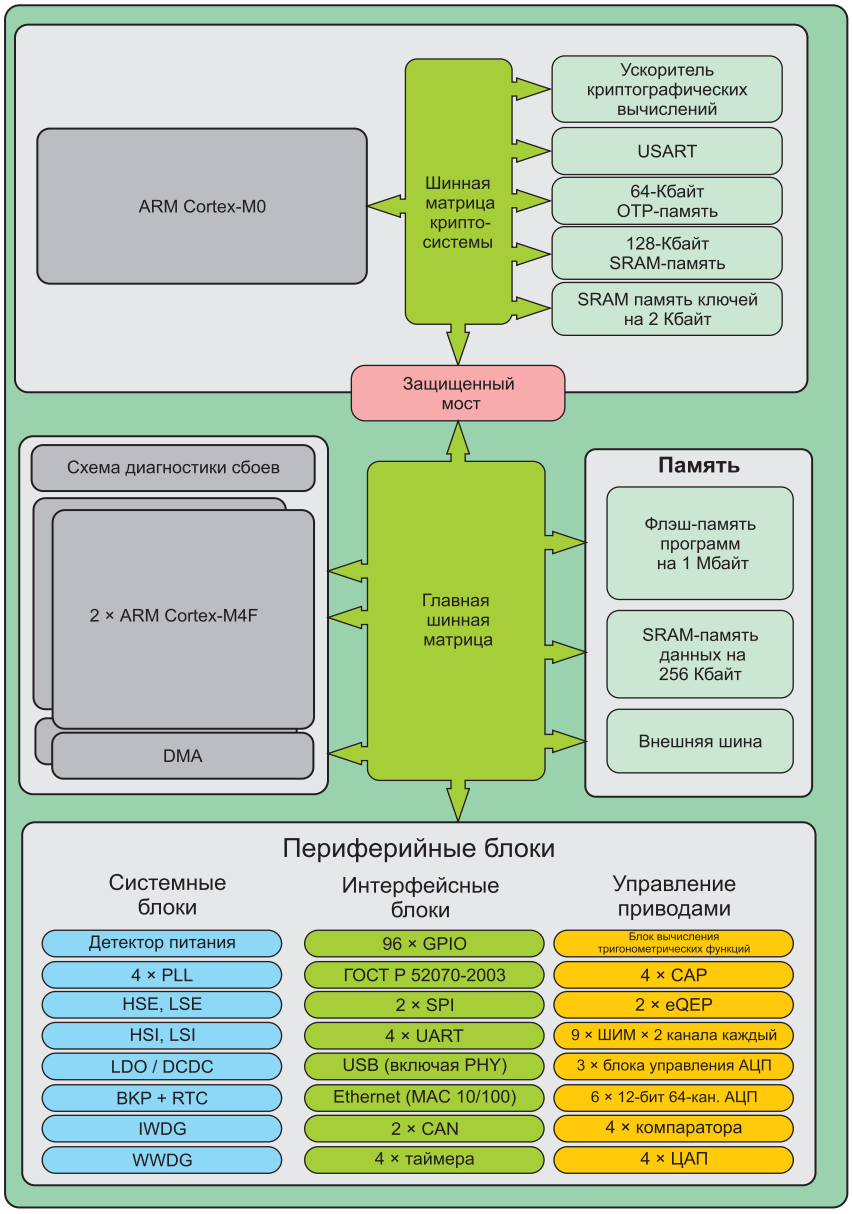

Рис. 1. **Структурная схема специализированного микроконтроллера для управления электроприводами**

автоматического исправления одиночных ошибок.

Для передачи данных в состав микросхемы включены базовые интерфейсы, например UART (4 блока), SPI (2 блока), I2C (1 блок), CAN (2 блока), ГОСТ Р 52070–2003, а также высокоскоростные Ethernet 10/100 и USB 2.0. Контроллер USB содержит приемопередатчики канального и физического уровней, позволяющие подключать микросхемы к разъему без использования внешних согласующих ИС. Каждому контроллеру интерфейса выделена отдельная функция порта ввода-вывода. Общее число пользовательских выводов равно 96. Каждый из них можно настраивать отдельно для использования как вывод одного из периферийных блоков или в качестве выводов общего назначения.

При разработке контроллера наибольшее внимание уделялось реализации современных алгоритмов векторного управления приводами на его основе, для работы которых требуется развитая система взаимодействующих между собой контроллеров АЦП и блоков ШИМ-генераторов, квадратурных энкодеров и модулей захвата для обработки данных датчиков положения вала, блоков сравнения аналоговых сигналов, цифро-аналоговых преобразователей и системы аварийного отключения.

В микроконтроллер интегрированы 9 независимых блоков ШИМ по 2 канала в каждом. Структурная схема блоков представлена на рисунке 2. Все блоки ШИМ объединены в цепочку и могут синхронизоваться друг с другом. Кроме того, в микроконтроллере реализованы 4 блока таймера общего назначения, также имеющих развитые функции ШИМ-генераторов. Блоки ШИМ микроконтроллера обладают гибкими

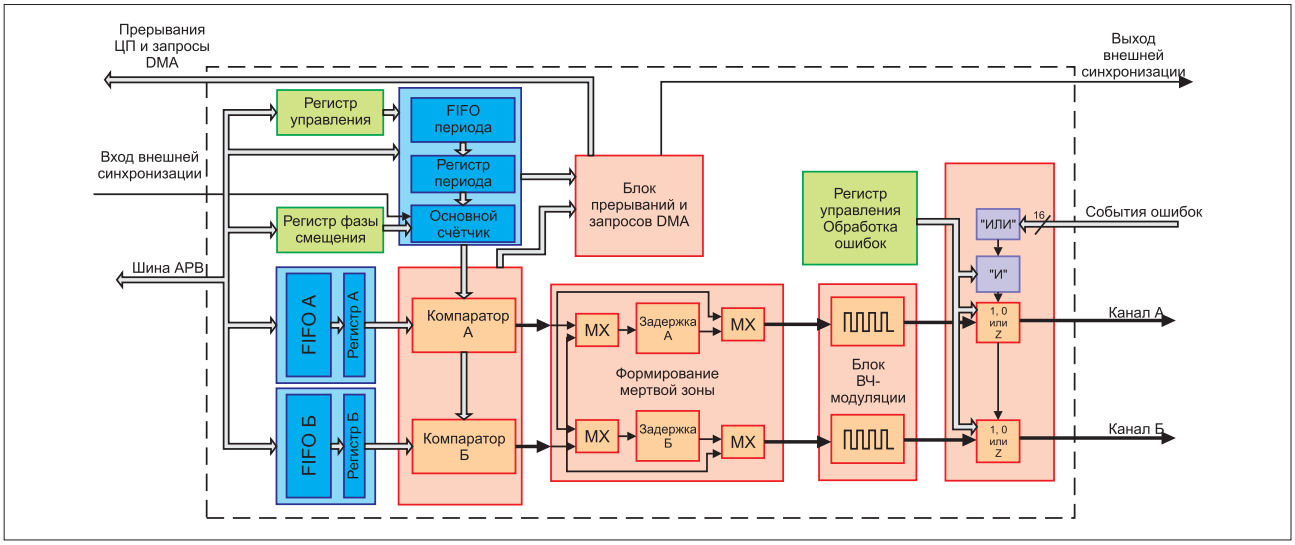

Рис. 2. **Блок широтно-импульсной модуляции**

возможностями конфигурирования выходов в комплементарном и в независимом режимах. В них реализованы возможности аппаратного отключения по внешним и внутренним событиям, аппаратное управление мертвой зоной, блок высокочастотного модулятора для управления силовыми ключами с использованием импульсного трансформатора.

Каждый из блоков контроллеров осуществляет управление двумя аналоговыми 8-канальными 12-разрядными блоками АЦП (см. рис. 3), работающими в обычном и дифференциальном режимах, и позволяет автоматически выполнять цепочки до 32 преобразований с записью результата в таблицу из 64 регистров. Для удобства обращения со стороны DMA регистры результатов можно также организовать в FIFO. Управление преобразованиями двух блоков АЦП в рамках одного контроллера могут выполняться независимо друг от друга, последовательно либо поочередно с задаваемым смещением, что позволяет увеличить частоту преобразований. Запуск цепочки преобразований может осуществляться программно и при помощи управляющего сигнала от блоков ШИМ. Таким образом, начало преобразования можно синхронизировать с периодом регулирования токов системы. Микроконтроллер содержит 3 независимых контроллера преобразований, каждый их которых управляет двумя преобразователями.

Для обработки показаний датчиков положения в систему интегрированы 2 блока квадратурных энкодеров и 4 блока захвата, позволяющие работать с датчиками разных типов.

Отдельной подсистемой микроконтроллера является модуль криптографической обработки информации. Подсистема представляет собой программируемый контроллер на вычислительном ядре ARM Cortex-M0 с собственным загрузчиком, собственной изолированной памятью программ и данных и специальный блоком ОЗУ с возможностью экстренного сброса для хранения ключей и секретной информации. Секретные данные и ключи загружаются в подсистему с помощью выделенного интерфейса UART.

В защищенной подсистеме реализованы модули криптографических ускорителей, позволяющие производить шифрование и дешифрование в соответствии с требованиями наиболее распространенных на текущий момент российских и зарубежных стандартов. Скорость выполнения алгоритмов в тактах системной частоты для алгоритмов DES и AES представлена в таблицах 2–3.

В модуле имеется шлюз с двумя блоками FIFO для обмена данными по ини-

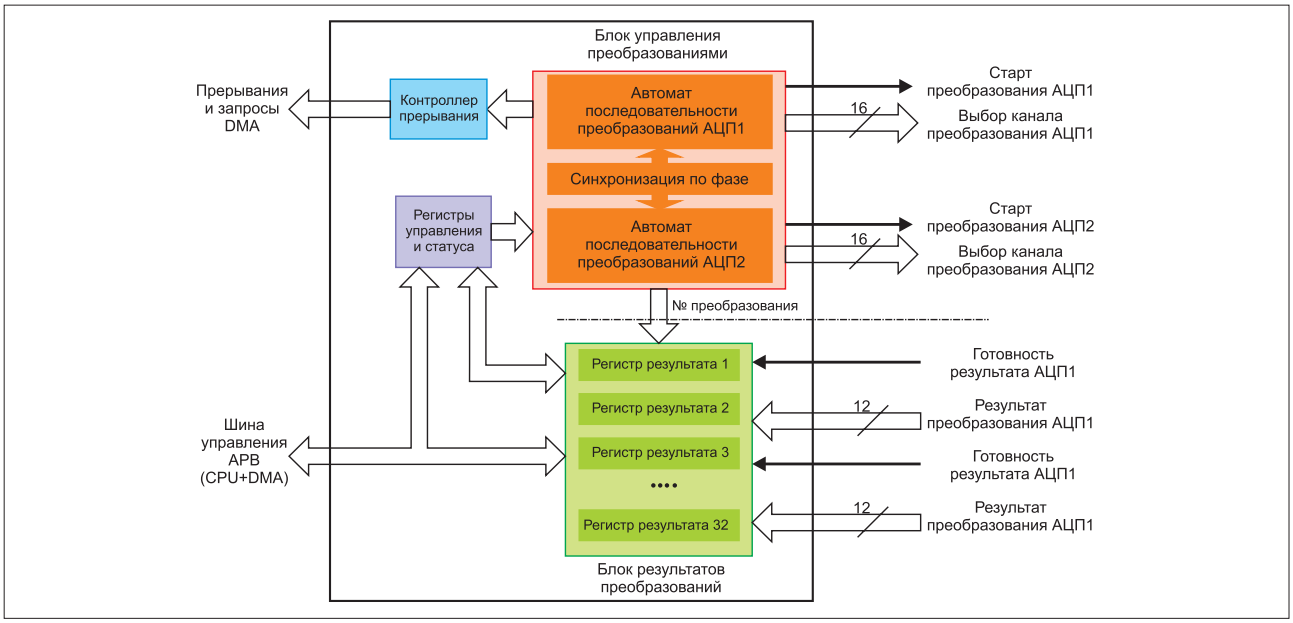

Рис. 3. **Контроллер АЦП**

циативе открытого ядра, регистрами статуса и управления. Со стороны открытого ядра он виден как периферийный модуль. Доступ со стороны основной системы микроконтроллера возможен для чтения статуса, записи в управляющий регистр, записи и чтения данных из блоков FIFO. Для ускорения реакций и упрощения обмена имеется набор прерываний (шлюз – открытое ядро, шлюз – закрытое ядро, закрытое ядро – открытое ядро).

Внешним питанием микросхемы служит источник напряжения 3,3 В. Для питания цифрового ядра микроконтроллера в ИС интегрированы два LDO-регулятора и DC/DC-преобразователь. После включения микросхемы DC/DC-преобразователь выключен, активны два LDO-регулятора. Первый из них понижает уровень питания с 3,3 до 1,6 В, второй на основе полученных с первого регулятора 1,6 В формирует 1,2 В для питания цифровых схем. Чтобы уменьшить энергопотребление при функционировании, можно включаться DC/DC-преобразователь, который предназначен для формирования 1,6 В вместо первого LDO-регулятора. При этом второй регулятор, оставаясь включенным, стабилизирует и выравнивает питание 1,2 В.

Блок батарейного домена также имеет собственный регулятор для формирования 1,2 В. На вход встроенного регулятора напряжения может подаваться батарейное питание. Батарея подключена к внешнему выводу микроконтроллера. В случае пропадания основного питания 3,3 В батарейный домен получает питание от встроенного регулятора напряжения 1,2 В. Для этого в системе реализован специальный модуль автоматического переключения питания батарейного домена, анализирующий уровни батарейного и основного питания и переключающий его с целью эффективного использования заряда внешней батареи.

Батарейный домен включает в себя часы реального времени, сторожевой таймер и набор регистров, сохраняющих системные настройки и другие важные данные пользователя на время отключения питания. Таблица ключей, размещенная в криптостойкой области микросхемы, также включена в батарейный домен питания.

Питание АЦП, ЦАП, умножителей частоты и генераторов осуществляется по выделенным выводам и развязано с основным питанием для сокращения взаимопроникающих помех.

Микросхема будет выпускаться в 144-выводном металлокерамическом корпусе BGA/PGA и в 144-выводном пластиковом LQFP-корпус. В настоящее время изготавливаются экспериментальные образцы, которые будут предложены заказчикам в конце 2018 г.

Таблица 2. **Время обработки данных в криптографической подсистеме микроконтроллера по алгоритмам DES (длина блока – 8 байт)**

Направление шифрования	Голое ассемблерное шифрование блока. Время обработки, кол-во тактов системной частоты	Шифрование блока в режиме ECB (Си-обвязка). Время обработки, кол-во тактов системной частоты
Шифрование	280	310
Дешифрование	297	327

Таблица 3. **Время обработки данных в криптографической подсистеме микроконтроллера по алгоритмам AES (длина блока – 16 байт)**

Направление шифрования	Голое ассемблерное шифрование блока. Время обработки, кол-во тактов системной частоты			Шифрование блока в режиме ECB (Си обвязка). Время обработки, кол-во тактов системной частоты		
Длина ключа	128	192	256	128	192	256
Шифрование	921	1105	1289	961	1145	1329
Дешифрование	1088	1308	1528	1128	1348	1568