

Микроконтроллер АО «ПКК Миландр» на базе процессорного ядра RISC-V для приборов учета электроэнергии

С. Шумилин¹

УДК 621.3 | ВАК 05.27.01

Решения на базе системы команд RISC-V всё чаще появляются на рынке. Уже серийно выпускаются микроконтроллеры китайских производителей, интересные решения предлагает компания Microchip. Растет экосистема программного обеспечения (ПО) и средств разработки для данной архитектуры. Компания АО «ПКК Миландр» также включилась в эту деятельность и уже начала поставку заинтересованным предприятиям инженерных образцов своего нового микроконтроллера K1986BK025 на базе процессорного ядра RISC-V для приборов учета электроэнергии. Об этом устройстве рассказывается в статье.

Микроконтроллер K1986BK025 на базе ядра RISC-V – это второе поколение микроконтроллеров для счетчиков электроэнергии. Первое поколение – микросхемы K1986BK2x – разработаны на базе процессорного ядра ARM Cortex-M0 и выпускаются уже более пяти лет. На их основе сейчас производят счетчики «Милур».

Но время не стоит на месте и новые правила рынка диктуют новые требования к микросхемам. Нужно обеспечить больше функций в соответствии с этими требованиями по минимальному функционалу приборов учета. Нужно попасть в требуемую цену, так как конкурировать придется с такими крупными компаниями, как например TI и NXP. Кроме того, новые «интеллектуальные» счетчики электроэнергии могут ограничивать потребление электроэнергии. А это значит, что новая система должна обеспечивать и информационную безопасность, чтобы злоумышленники не могли отключить или, наоборот, включить электричество по своему усмотрению. Все это и привело к появлению новой микросхемы K1986BK025.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ K1986BK025

Структурная схема микроконтроллера K1986BK025 представлена на рис. 1. Основные модули и характеристики микроконтроллера:

- процессорное ядро: RISC-V (BM-310 – компании CloudBEAR);
- тактовая частота: 60 МГц;
- напряжение питания (основное): 2,2–3,6 В;

- напряжение питания (АЦП): 3,0–3,6 В;
- напряжение питания (батарейное): 1,8–3,6 В;
- объем флеш-памяти программ: 256 + 8 Кбайт;
- объем памяти ОЗУ: 112 Кбайт;
- объем однократно-программируемого ПЗУ: 16 Кбайт;
- метрологический измерительный АЦП: сигма-дельта, 24 бита (семь каналов);
- аппаратный блок вычисления показаний потребляемой энергии;
- инструментальный АЦП: 10 бит, с датчиком температуры;
- интерфейсы: 5 × UART, 3 × SPI, 1 × I²C;
- число пользовательских выводов: 55;
- батарейный домен объемом 512 байт с часами реального времени и детектором фиксации протекновения;
- четыре блока 32-разрядных таймеров с четырьмя каналами захвата событий и ШИМ;
- сторожевой таймер;
- блок подсчета циклического избыточного кода (CRC) с изменяемым полиномом;
- блок поддержки вычислений для реализации симметричных криптографических алгоритмов;
- блок генератора случайных чисел;
- блок детектора изменения тактовой частоты;
- блок детектора изменения напряжения питания (основного и батарейного);
- блок оптического детектора;
- блок генерации шума в цепи питания;
- защитная экранная сетка;
- интерфейс отладки: JTAG;
- тип корпуса: QFN88 (10 × 10 мм);
- рабочая температура: от –50 до 85 °С.

¹ АО «ПКК Миландр», заместитель генерального директора по науке, shumilin.sergei@milandr.ru.

ПРОЦЕССОРНОЕ ЯДРО

Как уже было отмечено, сердцем микросхемы является 32-битное процессорное ядро RISC-V (в конфигурации RV32IMC) с обозначением VM-310, которое было разработано нашим партнером компанией CloudBEAR. Это не единственное их процессорное ядро. Компания предлагает целую линейку ядер, начиная от небольших микроконтроллерных ядер и заканчивая высокопроизводительными 64-битными многопроцессорными кластерами.

Компания АО «ПКК Миландр» ведет разработку новых продуктов на базе ядер из всех «весовых категорий» продуктов CloudBEAR. В кремнии сейчас доступны только K1986BK025 на базе ядра VM-310. Но и другие продукты, в том числе на базе 64-битных ядер, скоро увидят свет. Ядро VM-310 – это 32-битное ядро RISC-V с трехстадийным конвейером, с возможностью выполнения операции умножения за два такта. Поддержка операций с плавающей запятой в данной версии микросхемы не была реализована (хотя ядро позволяет это сделать). Производительность ядра VM-310 в тесте CoreMark составляет 3,0 CoreMark / МГц. Таким образом, его можно сравнить с ARM Cortex-M3. При этом ядро в новой микросхеме занимает всего 0,3 мм². А с учетом того, что большинство задач по вычислению параметров потребления электроэнергии выполняется аппаратно контроллером метрологического АЦП, то основная вычислительная мощность ядра может использоваться для коммуникационных задач в приборе учета.

ЦЕНА

Цена – один из основных критериев для выбора микросхемы. Основной вклад в стоимость микросхемы вносит кристалл. Чем больше его площадь – тем он дороже, чем более сложная технология изготовления – тем он также дороже. Но при этом, чем более сложная технология, тем на меньшей площади можно реализовать требуемый функционал, а значит, устройство будет дешевле. В общем, выбор технологии не всегда очевиден. Микросхемы первого поколения K1986BK2х были разработаны с использованием

технологического процесса 180 нм. Примерно треть кристалла относилась к аналоговой части (собственно сами сигма-дельта АЦП, питание, ввод-вывод) и при переходе на более «тонкие» процессы эта часть практически не уменьшается. Но в соответствии с новыми требованиями объем функционала должен быть увеличен практически в четыре раза. В микросхеме второго поколения реализовано 256 Кбайт флеш-памяти против 64 Кбайт в микросхемах первого, ОЗУ 112 Кбайт против 16 Кбайт, пять блоков UART против двух, три блока SPI против одного и еще криптография. После долгих прикидок и расчетов было принято решение, что если уделить особое внимание площади, то с применением технологического процесса 90 нм можно попасть в требуемый коридор стоимости. С использованием технологического процесса 65 нм или ниже решить эту задачу было бы легче, но большие затраты на разработку в целом сделали бы проект более рискованным

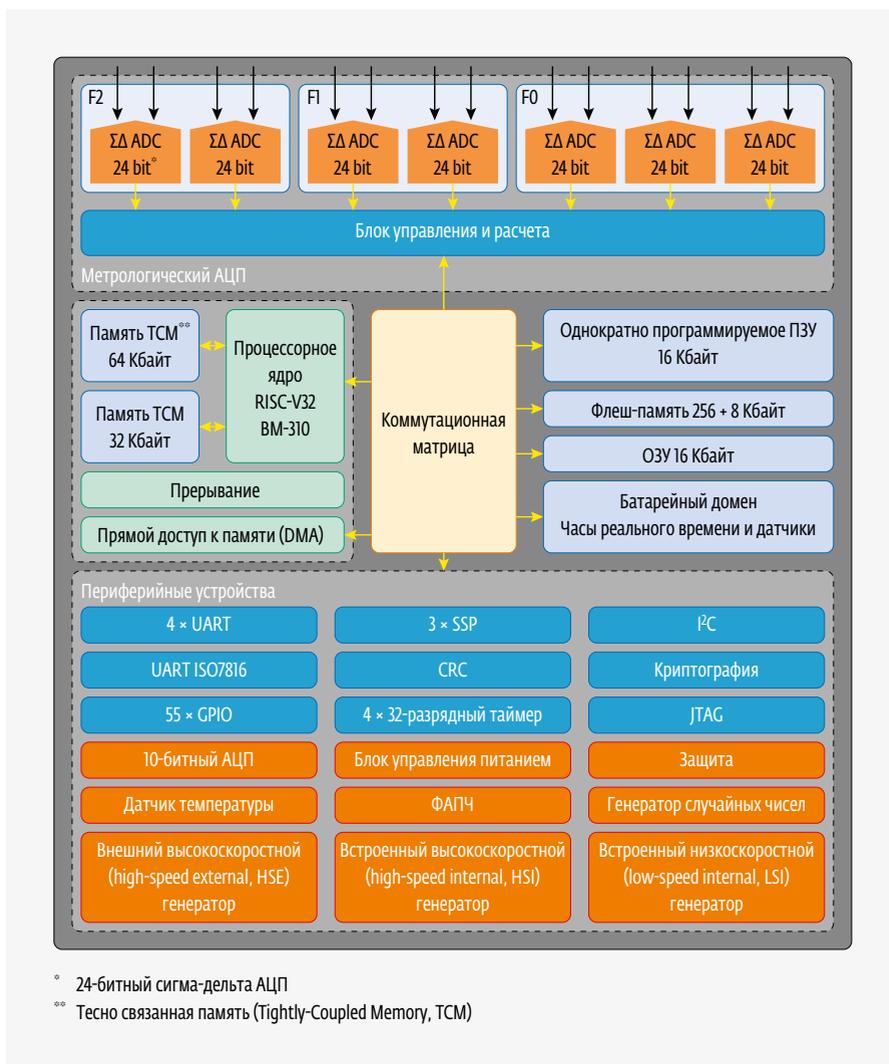


Рис. 1. Структурная схема микроконтроллера K1986BK025

по финансам. В результате мы получили действительно компактный кристалл, который по площади более чем в два раза меньше предыдущего (рис. 2).

МЕТРОЛОГИЧЕСКИЙ АЦП

Если процессорное ядро – это сердце микроконтроллера, то метрологический АЦП – его мозг, так как именно он определяет предназначение микросхемы. В микроконтроллере K1986BK025 реализован блок из семи каналов 24-битных сигма-дельта АЦП (см. рис. 1). Все каналы разбиты на три пары F0-F2 (канал напряжения и канал тока в каждой) для трехфазной сети и еще одного независимого канала тока (отнесен к F0) – для контроля тока по нейтрали. Каждый из семи каналов оцифровывает входной сигнал с выходной частотой отсчетов до 16 кГц. Кроме этого, в каждой паре каналов F0-F2 реализована возможность рассчитывать среднеквадратические значения тока/напряжения, вычислять активную и реактивную мощности, потребляемую активную и реактивную энергию, частоту сигнала в каналах напряжения, превышение пикового значения, падение сигнала ниже установленного уровня. Эти дополнительные блоки позволяют снизить нагрузку на процессор, что в свою очередь снижает потребляемую мощность всего кристалла. Также каждый АЦП имеет независимый канал прямого доступа к памяти (DMA), обеспечивая возможность сохранения данных в ОЗУ без участия процессора.

Список основных параметров и возможностей блока сигма-дельта АЦП:

- семь независимых АЦП с выходной частотой отсчетов 4/8/16 кГц (четыре канала тока и три канала напряжения). Эти каналы образуют три блока для измерения параметров каждой фазы F0-F2;
- в блоке каналов F0 можно реализовать автоматический выбор канала тока для последующих расчетов мощностных характеристик. Если разница токов в каналах блока F0 превышает 6%, то формируется прерывание. Кроме этой функции, в остальном блоки F0-F2 идентичны;
- все каналы АЦП имеют независимые калибровочные коэффициенты наклона характеристики;
- каждый канал тока имеет независимый интегратор;

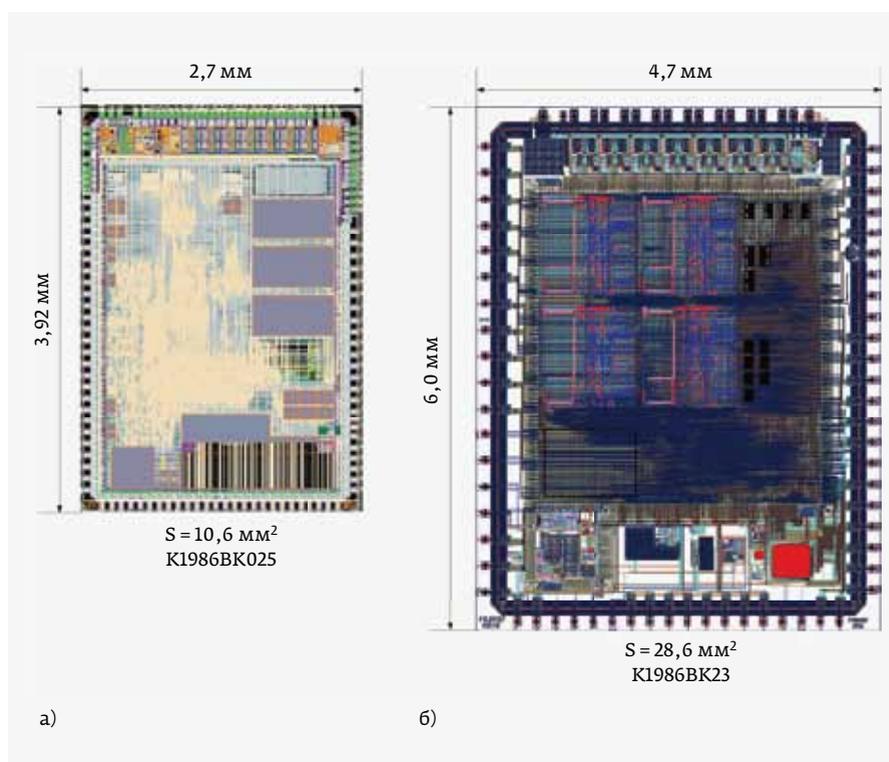


Рис. 2. Топологии микросхем K1986BK025 (а) и K1986BK23 (б)

- в каждом блоке АЦП (F0-F2) независимо рассчитывается период сигнала по каналу напряжения. Количество периодов, в течение которых рассчитывается эта величина, можно задавать равным 1/2/4/8/16/32/64/128;
 - в каждом блоке есть проверка на пропадание периодического сигнала в канале напряжения;
 - в каждом блоке проверяется «просадка» напряжения ниже заданного уровня, а также превышение сигналами в каналах тока и напряжения установленного лимита;
 - есть возможность скорректировать фазы сигналов в каналах напряжения с точностью до 0,02%;
 - вычисляются среднеквадратические значения, квадрат среднеквадратических значений токов и напряжений, а также выполняется их независимая калибровка;
 - при вычислении активной и реактивной энергии значение накопленной энергии в течение периода сохраняется в отдельных регистрах (для положительной и отрицательной энергии);
 - вычисляются полная мощность и энергия;
 - вычисляется сдвиг фаз по отношению к фазе 0.
- Таким образом, основные функции по расчету потребленной энергии выполняются с минимальным участием процессора.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Как уже было отмечено ранее, новые интеллектуальные счетчики электроэнергии должны уметь отключать потребителя от сети по соответствующей команде. Кроме того, передача показаний потребленной энергии осуществляется автоматически по различным каналам связи. А это значит, что вопросы информационной безопасности будут стоять особенно остро. Поэтому в микросхеме K1986BK025 реализованы все требования, необходимые в части информационной безопасности, она может найти свое применение и в других областях – тахографах, электронных пломбах, для идентификации и аутентификации элементов IoT. Все средства обеспечения информационной безопасности, которыми оснащена микросхема K1986BK025, можно разделить на две части: криптографию и инженерную защиту.

Криптография

В микросхеме реализовано всё для защиты информации в соответствии с ГОСТ Р 58940-2020, в том числе:

- блоки сопроцессоров для поддержки блочных шифров «Кузнечик», «Магма» и AES;
- блок генератора случайных чисел;
- блок вычисления CRC по произвольному полиному;
- блок специальной энергозависимой памяти для ключевой информации с батарейным питанием;
- однократно программируемое ПЗУ первоначального загрузчика, в которой реализуется уникальная идентификация каждой микросхемы.

Симметричная криптография реализуется на базе сопроцессоров, которые ускоряют самые тяжелые операции. Это позволяет получить скорость шифрования с пиковой производительностью до 10 Мбит/с. При необходимости алгоритмы асимметричной криптографии реализуются программным путем.

Инженерная защита

Чтобы затруднить применение различных инженерных методов воздействия как на сам счетчик электроэнергии, так и отдельно на микросхему, реализованы специальные методы инженерной защиты:

- три вывода для детекторов проникновения (электронные пломбы);
- блок детектора изменения тактовой частоты;
- блок детектора изменения напряжения питания;
- блок оптического детектора;
- блок генерации шума в цепи питания;
- защитная экранная сетка;
- защита от несанкционированного считывания памяти.

Выводы для детекторов проникновения – это три отдельных вывода микроконтроллера, через которые



Рис. 3. Демонстрационная плата для микросхемы K1986BK025

фиксируются сигналы от внешних электронных пломб, даже в случае отсутствия питания. Таким образом, какие-либо попытки механического воздействия на счетчик будут обнаружены и зафиксированы. Кроме механизмов защиты корпуса прибора, реализуются методы защиты уже самой микросхемы от более изощренных атак.

Для исключения ситуации с «разгоном» или наоборот «торможением» тактовой частоты процессора реализован детектор изменения частоты, который непрерывно сравнивает внешний источник тактирования с внутренним RC-генератором. И при возникновении отклонений, выходящих за заданные границы, фиксирует это событие или может переключить микросхему на внутренний (реализованный на кристалле) аварийный источник тактирования.

Для корректного запуска микросхем по включению основного питания, а также обнаружения факта выхода питания из допустимых диапазонов, реализован блок детектора напряжения. Кроме того, блок обеспечивает контроль уровня заряда батарейки, на которой работает микросхема при отсутствии основного питания. Таким образом исключаются какие-либо манипуляции или попытки сбить работу микросхемы через питающие напряжения.

Для исключения утечки ключевой информации по «паразитным» каналам, например цепям питания,

в микросхеме реализован блок зашумления основного питания с помощью псевдослучайного генератора. Блок формирует случайным образом изменяемое дополнительное потребление, маскируя основной профиль потребления.

Для противодействия более серьезным полунинвазивным и инвазивным атакам (атака на микросхему, когда есть доступ к кристаллу микросхемы или даже отдельным цепям кристалла) реализован оптический детектор. Так как обычно кристалл микросхемы находится в корпусе, то доступ света к нему невозможен. Если же корпус микросхемы вскрыт и на кристалл попадает свет, то оптический датчик сформирует сигнал тревоги.

Если же злоумышленник прошел еще дальше, то для ограничения доступа к внутренним цепям микросхемы в верхних слоях топологии кристалла реализована защитная сетка. В ней перемежаются цепи земли, питания и информационная цепь, по которой передается случайный полином. В случае физического нарушения целостности сетки также формируется сигнал тревоги. Программное обеспечение должно контролировать все сигналы тревоги и в случае их возникновения фиксировать факт атаки.

Кроме того, микросхема может быть настроена так, чтобы криптографическая ключевая информация была автоматически стерта при обнаружении фактов атаки. Это требует использования так называемого доверенного ПО. Для пользовательской программы в микросхеме реализовано 16 Кбайт однократно программируемого ПЗУ и 256+8 Кбайт перепрограммируемой флеш-памяти. Запуск микросхемы происходит из встроенной однократно программируемой памяти. Изначально, при изготовлении микросхем, данная память чистая, и для серийных изделий загрузка стартового доверенного загрузчика будет происходить при тестировании и отбраковке. Это позволяет обеспечить уникальную идентификацию каждой микросхемы, гарантировать целостность метрологического и криптографического ПО, и стартовый загрузчик является корнем доверия для пользовательской программы, исполняемой из флеш-памяти. А также при необходимости можно обеспечить защиту от считывания пользовательской программы во флеш-память. На время исследования для инженерных образцов в стартовую память записан типовой загрузчик для серии микроконтроллеров 1986BE. При необходимости может быть выпущена отдельная партия микросхем со стартовым загрузчиком, адаптированным под задачи потребителя.

СРЕДСТВА РАЗРАБОТКИ

Для первоначального знакомства с микроконтроллером разработана демонстрационная плата (рис. 3).

Она предназначена для прототипирования приборов учета, большое число ВЧ-разъемов нужно для подключения измерительных трансформаторов. Это позволяет не ориентироваться на какой-то конкретный их тип, а легко подключить именно те трансформаторы или шунты, которые применяют разработчики приборов учета. Также это дает возможность подключить различные измерительные приборы для снятия точностных характеристик АЦП. Кроме того, отсутствие высокого напряжения (220 В) позволяет избежать поражения электрическим током. Для более массового продвижения микросхемы ведется разработка миниатюрной тестовой платы в форматах Arduino Uno или Arduino Mega.

Eclipse+GCC

Разработка программ может осуществляться в среде на базе Eclipse с компилятором GCC и отладкой с использованием OpenOCD, GDB. Для отладки в среде Eclipse подходят классические отладчики J-Link и их клоны, а также отладчики производства компании АО «ПКК Миландр» [1].

IAR

Также разработку можно осуществлять в более привычной для многих среде IAR Embedded Workbench компании IAR Systems, которая включает средства отладки, компиляции и оптимизации. Для отладки используются либо фирменное устройство I-jet for RISC-V, либо если заказать Evaluation Kit for RISC-V, то вместе с ним вы получите устройство I-jet Lite debug probe (которое поддерживает в том числе и ARM), а также 30-дневную лицензию на саму среду.

Более подробную информацию по настройке и запуску сред IAR и Eclipse для работы с микроконтроллером K1986BK025 можно найти в [2].

Таким образом новый микроконтроллер K1986BK025 обладает богатыми функциональными возможностями. Надеемся, что потребители (разработчики приборов учета) воспримут его положительно и будут успешно применять в своих устройствах.

ЛИТЕРАТУРА

1. Внутрисхемный гальванически развязанный USB-программатор. https://ic.milandr.ru/products/programmno_otladochnye_sredstva/programmatory/vnutriskhemnyy-galvanicheski-razvyazannyy-usb-programmator-dlya-mikrokontrollerov-s-yadrom-cortex-m/ (дата обращения 30.03.2021).
2. Новые микроконтроллеры для приборов учета K1986BK025. <https://forum.milandr.ru/viewtopic.php?f=35&t=4254> (дата обращения 30.03.2021).

ПАМЯТЬ FLASH

- В МИНИМАЛЬНОМ КОРПУСЕ
- ЕЩЕ БОЛЬШЕЙ ЕМКОСТИ
- ДЛЯ СПЕЦИАЛЬНЫХ ПРИМЕНЕНИЙ

Постоянные запоминающие устройства flash-типа с длительным хранением, оперативным обновлением массивов данных и программного обеспечения производства компании «Миландр».

Ключевые преимущества:

- Компактность
- Дешевизна
- Механическая прочность
- Скорость работы
- Низкое энергопотребление
- Надежность

Компанией АО «ПКК «Миландр» серийно поставляются и вновь разрабатываются микросхемы ПЗУ:

1636PP52Y*	1 Мбит	128Кx8
1636PP51Y	1 Мбит	128Кx8
1636PP3Y*	4 Мбит	512Кx8
1636PP1Y	4 Мбит	512Кx8
1636PP4Y*	16 Мбит	2Мx8
1636PP2Y	16 Мбит	2Мx8
1636PP6Y*	64 Мбит	4Мx16, 8Мx8
9023PP018*	128 Мбит	4Мx32

* - поддерживает SPI-интерфейс



АО «ПКК МИЛАНДР»

+7 (495) 981-54-33

+7 (495) 981-54-36 (факс)

ic@milandr.ru

WWW.MILANDR.RU



ТЕХПОДДЕРЖКА:

+7 (495) 221-13-55

forum.milandr.ru

support@milandr.ru

SUPPORT.MILANDR.RU