Отечественные USB микроконтроллеры фирмы «ПКК Миландр».

Основные показатели производительности

Сергей ШУМИЛИН

ЗАО «ПКК Миландр» является отечественным дизайн-центром, специализирующимся в области разработки и производства заказных интегральных микросхем. Фирма занимается проектированием цифровых, аналоговых, цифро-аналоговых микросхем и схем памяти для различных применений. Основным направлением в области разработки цифровых микросхем является проектирование «систем на кристалле» на базе микропроцессорных ядер под специальные требования заказчика. Так, на основе 8-разрядного микропроцессорного ядра, разработанного для микроконтроллеров 1886ВЕ1 и 1886ВЕ2 (функциональных аналогов микроконтроллера PIC17C756), были разработаны два новых микроконтроллера с условными обозначениями 1886ВЕ3У и 1886ВЕ4У с встроенным контроллером USB-интерфейса. В настоящее время выпущены работающие экспериментальные образцы кристаллов. Микроконтроллер 1886ВЕ3У предназначен для создания криптографических систем, а 1886ВЕ4У — для создания систем сбора, обработки информации и управления. Сравнительные характеристики микроконтроллеров представлены в таблице 1.

Таблица 1. Сравнительные характеристики микроконтроллеров

Параметр	1886ВЕ2	1886ВЕ3У	1886ВЕ4У
Микропроцессорное ядро	58 инструкций, функциональный аналог PIC17C756 компании Microchip	58 инструкций, совместимое с PIC17 компании Microchip	58 инструкций, совместимое с PIC17 компании Microchip
Память программ	Flash 64 кбайт	Flash 64 кбайт	Flash 64 кбайт
Оперативная память данных	1024 байт	1024 байт	1024 байт
Энергонезависимая память данных	нет	256 байт, с возможностью установки защиты от записи и стирания	256 байт
Тактовая частота	33 МГц	35 МГц	35 МГц
Напряжение питания ядра	4,5–5,5 В	4,5–5,5 В	4,5–5,5 В
Напряжение питания портов ввода-вывода	4,5–5,5 В	3,0–5,5 В	3,0–5,5 В
Интерфейс USB	нет	Full Speed (12 Мбит/с) Low Speed (1,5 Мбит/с)	Full Speed (12 Мбит/с) Low Speed (1,5 Мбит/с)
Число пользовательских конечных точек USB и размер буфера FIFO	нет	2 конечные точки по 64 байта	4 конечные точки по 64 байта
Интерфейс USART	2	1	1
Интерфейс SPI	1	нет	1
Интерфейс I²C	1	нет	нет
АЦП	12 каналов, 10 разрядов	нет	нет
Таймеры	4	1	1
ШИМ/Захват	3	нет	нет
Интерфейс NAND Flash	нет	1	1
Поддержка ГОСТ 28147-89	нет	есть	нет
Встроенный регулятор напряжения	нет	На 3,3 В	На 3,3 В
Рабочий диапазон температур	–60...+ 85 °С	–60... + 85 °С	–60... + 85 °С
Тип корпуса	64-выводной H18.64	48-выводной H16.48 64-выводной LQFP 64	48-выводной H16.48 64-выводной LQFP 64

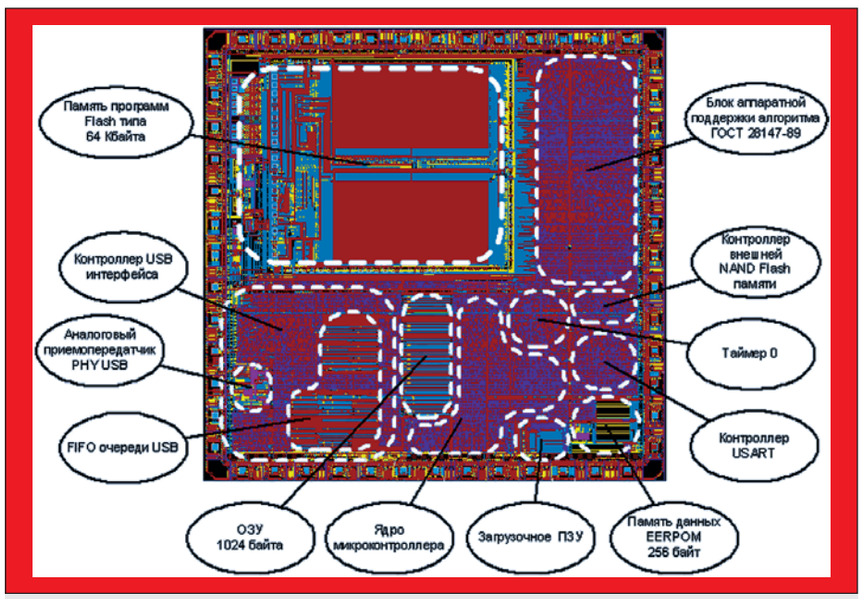

Рис. 1. Топология кристалла 1886ВЕ3У

Микроконтроллер 1886ВЕ3У (рис. 1) предназначен для реализации криптографических систем. Он позволяет обрабатывать достаточно большие потоки информации, поступающие по интерфейсам USB или RS-232. С помощью блока поддержки алгоритма шифрования по ГОСТ 28147-89 данные потоки могут кодироваться и либо передаваться далее, либо сохраняться во внешней энергонезависимой памяти типа NAND Flash. Алгоритм шифрования в соответствии с ГОСТ 28147-89 является основным алгоритмом криптографической защиты информации в России и применяется в аппаратуре различного назначения.

Микроконтроллер 1886ВЕ4У (рис. 2) предназначен для различных систем сбора и обработки информации. По своим характеристикам он схож с микроконтроллером 1886ВЕ3У, но в нем вместо блока аппаратной поддержки алгоритма шифрования интегрирован контроллер интерфейса SPI и увеличено число конечных точек USB до 4 штук. С помощью данного микроконтроллера можно реализовать высокопроизводительный USB интерфейс в различной аппаратуре.

Размер очереди каждой конечной точки составляет 64 байта. Контроллер USB-интерфейса содержит 128 байт памяти для пользовательского дескриптора устройства USB, позволяю-

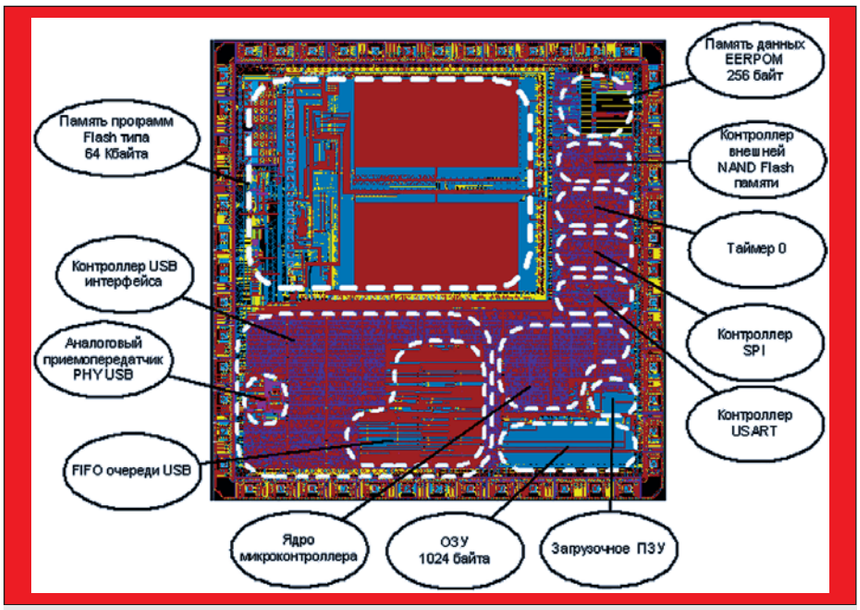

Рис. 2. Топология кристалла 1886ВЕ4У

щего задать произвольные идентификаторы Vendor ID и Product ID, а также прочие характеристики устройства, в том числе и строковые описания. Контроллер USB-интерфейса может оперировать в режимах Full Speed (до 12 Мбит/с) и в Low Speed (до 1,5 Мбит/с). Конечные точки могут работать в режимах Bulk, Interrupt и Isochronous.

Основной задачей при разработке контроллера USB-интерфейса стало обеспечение максимальной производительности данного периферийного блока, но при минимальном использовании ядра микроконтроллера. Кроме того, новый блок должен быть простым и удобным в использовании для будущих разработчиков, не требующим глубокого знания самого интерфейса. Следовательно, работа контроллера USB-интерфейса (рис. 3) должна быть максимально автоматизирована. Контроллер автоматически принимает и разбирает пакеты от хост-контроллера, проверяет целостность данных, в случае необходимости автоматически выдает подтверждение хост-контроллеру об успешном приеме пакета. При передаче данных хост-контроллеру

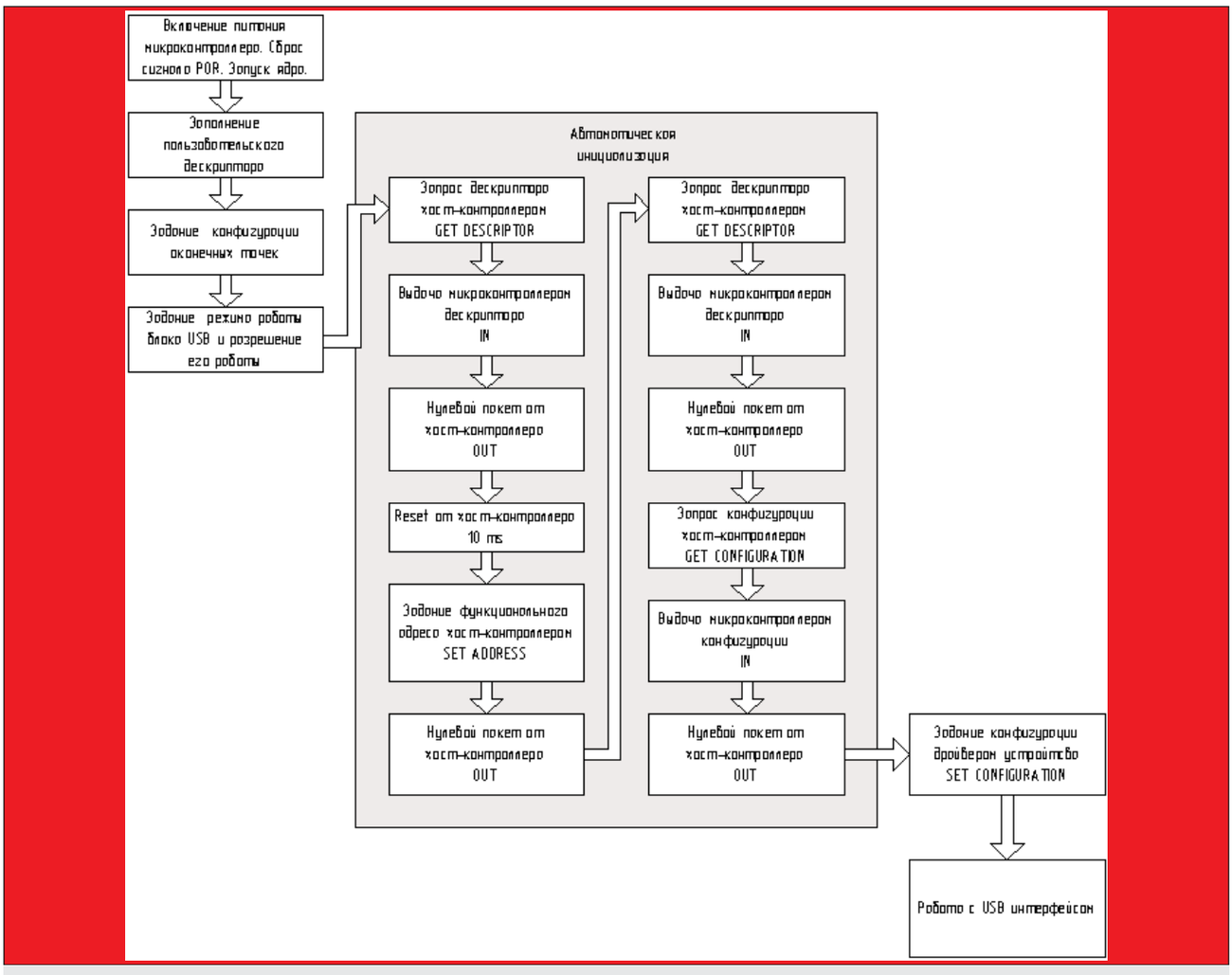

Рис. 3. Процесс автоматической инициализации USB-интерфейса

Рис. 4. Блок-схема алгоритма передачи данных Bulk OUT

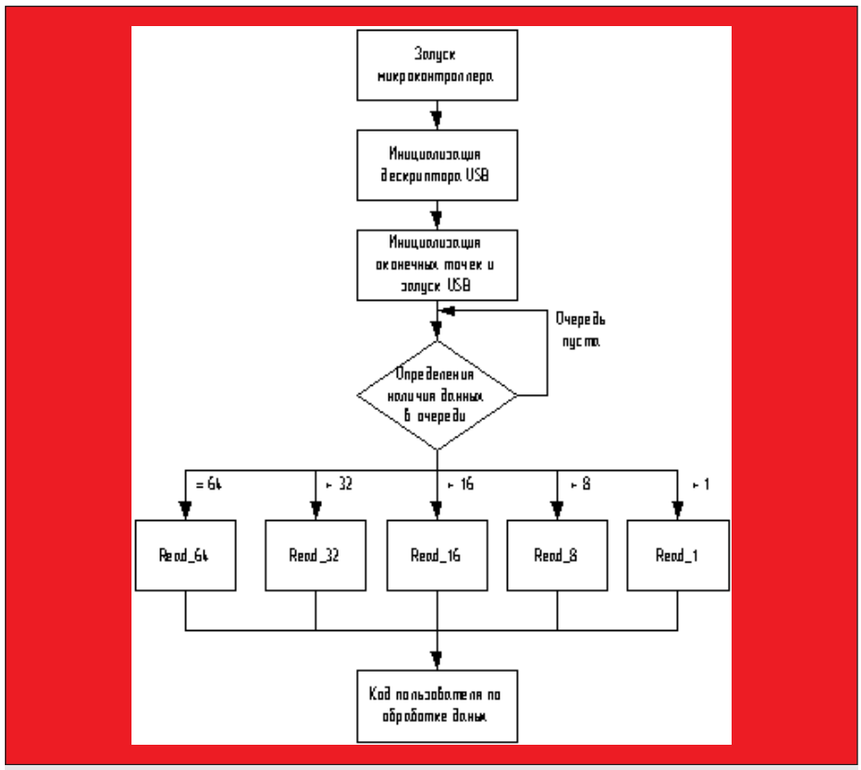

Рис. 5. Блок-схема усложненного алгоритма передаче данных Bulk OUT

автоматически выполняется формирование пакетов и проверяется подтверждение о принятии данных от хоста. Вся эта работа по организации обмена между микроконтроллером и ведущим контроллером полностью скрыта от микропроцессорного ядра. Такого рода автоматизация значительно упрощает работу с интерфейсом, но приводит к повышению сложности и увеличению размера блока. Кроме того, механизм автоматической инициализации USB-интерфейса не позволяет изменять структуру полей дескриптора. Все это потребовало внимательной проработки и верификации данного блока на этапе создания микросхем и проверки его работоспособности на различных системах. Для этого были разработаны различные программы, позволяющие оценить правильность функционирования данного интерфейса.

Работа программы по обмену данными через USB-интерфейс, выполняемой в микропроцессорном ядре, сводится к работе с буферами FIFO используемых конечных точек. Определение состояния данных очередей может проводиться на основе значений флагов Empty и Full, отображаемых в соответствующих регистрах состояния, либо на основании значения числа слов в очереди, отображаемого в отдельном регистре для каждой конечной точки. Работа микропроцессорного ядра с очередями может происходить одновременно с приемом или передачей пакетов USB.

В ходе исследований образцов микросхем при работе с USB-интерфейсом были достигнуты скорости, близкие к максимально возможным, при использовании не более 20% процессорного времени на обслуживание данного блока. При частоте микроконтроллера 32 МГц (8 MIPS), контроллер USB-интерфейса был сконфигурирован для режима Full Speed (12 Мбит/с) с максимальным размером пакета в 64 байта при работе с конечными точками Bulk IN (передача данных от микроконтроллера к хосту) и Bulk OUT (передача данных от хоста к микроконтроллеру). Причем практически все время, затраченное на работу с USB-интерфейсом, микроконтроллер занимается записью или чтением данных из очередей контроллера USB. Таким образом, если совместить процесс обработки с чтением или записью данных, этот показатель можно увеличить. Как уже упоминалось ранее, работать с контроллером USB-интерфейса можно либо по значениям флагов Empty и Full, либо по значениям счетчиков слов в очереди. Очевидно, что при постоянном опрашивании флагов на наличие данных скорость чтения или записи в буфер значительно снизится (блок-схема алгоритма передачи данных от хост-контроллера к микроконтроллеру представлена на рис. 4).

Таблица 2. Характеристики скорости передачи данных Bulk OUT

Число команд в программе обработки данных на один получаемый байт	Средняя скорость, кбайт/с При работе по флагам	Средняя скорость, кбайт/с При работе по счетчику	Объем кода инициализации USB-устройства	Объем кода чтения одного байта
0	917	1048	350	5 при работе по флагам. Функция: Read_64 - 1.094 Read_32 - 1.188 Read_16 - 1.375 Read_8 - 1.75 Read_1 - 7
1	851	1048		
5	790	1048		
10	530	655		
15	327	458		
25	262	262		
35	196	196		
50	131	131		

Используя для работы значение счетчика слов в очереди можно значительно ускорить работу (блок-схема усложненного алгоритма представлена на рис. 5). Определив число слов в очереди, затем можно произвести безусловное считывание из очереди заданного числа байт.

При передаче данных от хост-контроллера к микроконтроллеру были получены результаты, представленные в таблице 2 и на рис. 6.

На диаграмме рис. 6 по вертикальной оси отображается скорость передачи, а по горизонтальной — число команд по обработке одного принятого байта. Чем больше такого рода обработка, тем меньше скорость передачи. Как видно из диаграммы, по мере увеличения сложности обработки значения скоростей работы по флагам и по счетчику сравниваются.

При передаче данных от микроконтроллера к хост-контроллеру были получены схо-

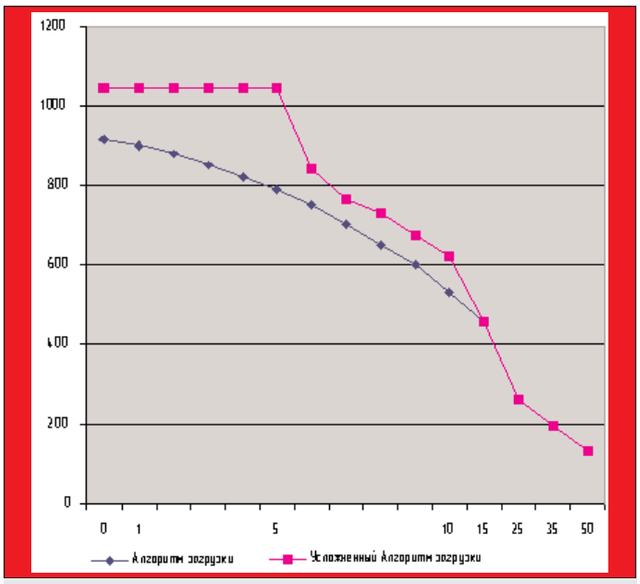

Рис. 6. Диаграмма производительности при передаче Bulk OUT

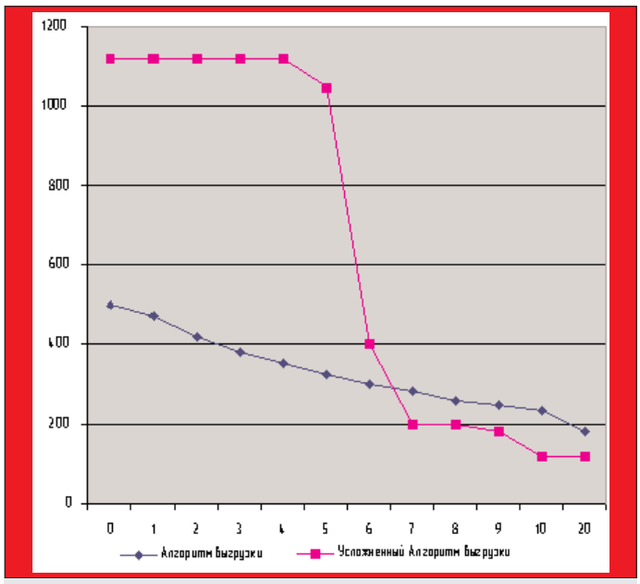

Рис. 7. Диаграмма производительности при передаче Bulk IN

Таблица 3. Характеристики скорости передаче данных Bulk IN

Число команд в программе обработке данных на один отправляемый байт	Средняя скорость, кбайт/с При работе по флагам	Средняя скорость, кбайт/с При работе по счетчику	Объем кода инициализации USB-устройства	Объем кода чтения одного байта
0	500	1120	350	5 при работе по флагам. Функция: Write_64 - 1.094 Write_32 - 1.188 Write_16 - 1.375 Write_8 - 1.75 Write_1 - 7
1	470	1120		
2	417	1120		
3	380	1120		
4	351	1120		
5	324	1048		
6	300	400		
7	284	200		
8	257	200		
9	249	180		
10	235	120		
20	180	120		

жие результаты, отображенные в таблице 3 и на рис. 7.

При передаче данных по USB обычный алгоритм так же опирается на значение флагов очереди, что приводит к большим затратам по передаче одного байта. При работе со счетчиком удельное число команд на передачу также можно сократить. Для этого реализуются функции безусловной записи 64, 32, 16, 8 и 1 байта.

Как видно из диаграмм на рис. 6 и 7, при увеличении сложности обработки данных более 5–6 команд на один принимаемый или отправляемый байт происходит резкое падение скорости обмена по шине USB. Это обусловлено тем, что уменьшение скорости передачи внутри микроконтроллера приводит к уменьшению числа байт, передаваемых в одном пакете по шине USB и, следовательно, увеличения доли служебной информации при обмене.

Другим узким местом в микроконтроллере 1886ВЕ3У является блок аппаратной поддержки криптографического алгоритма ГОСТ 28147-89. Данный блок аппаратно реализует одну базовую итерацию преобразования исходных данных на основе ключа размером 256 бит, констант замены размером 32 бита и синхропосылки размером 32 бита. Преобразование одновременно производится над блоком данных размером в 64 бита. Таким образом, блок фактически является 64-битным спецвычислителем базовой итерации криптографического алгоритма. После задания программным путем необходимого числа итераций будет выполнено полное преобразование данных. Кроме порта данных, через который осуществляется шифрование основного потока информации, в блоке предусмотрен порт, выполняющий эти же преобразования с накоплением ранее полученных результатов, что позволяет одновременно с кодированием осуществлять выработку иммитовставки. С помощью данного блока аппаратной поддержки шифрования могут выполняться все режимы, регламентированные ГОСТ, а именно: шифрование и дешифрование в режиме простой замены, в режиме гаммирования и в режиме гаммирования с обратной связью. Скорость кодирования с помощью данного блока достигает 8 Мбит/с. С помощью данного блока можно так же произвести расчет хеш-функций в соответствии с ГОСТ Р34.11-94. Вся процедура шифрующего преобразования занимает 260 мкс. Ключ и константы преобразования загружаются программно на каждом цикле шифрования 64 бит данных. Размер ключа 256 бит, таблица констант постоянна и составляет 64 байта. Генерация ключей и перемешивающее преобразование в данном устройстве были реализованы программно.

После вычисления очередного ключа (за время 270 мкс) осуществляется кодирование данных в блоке. Время вычисления ключей на разных этапах различно, поэтому общая продолжительность генерации ключей составляет 950 мкс. Только после шифрования всех подслов стартового вектора хэширования осуществляется перемешивающее преобразование длительностью 1500 мкс. В результате общее время вычисления шаговой хэш-функции составляет 3000 мкс. Общий объем программы — всего 1 кбайт памяти.

В настоящее время фирма ведет дальнейшую работу по расширению серии микроконтроллеров 1886ВЕ. В частности, разрабатываются новые интерфейсные блоки, такие как CAN 2.0B, Ethernet 10BaseT, бесконтактный ISO 14443 A/B и другие. Ведется работа и в области криптографической защиты информации — разработан блок аппаратной поддержки модульной арифметики для реализации алгоритмов электронной цифровой подписи по ГОСТ Р 34.10-2001. Кроме того, ведется разработка микромощного микроконтроллера с потреблением менее 0,5 мА на 1 МГц, а также планируется создание новых аналоговых блоков — 12-разрядного АЦП, инструментального усилителя с программируемым коэффициентом усиления и др.