

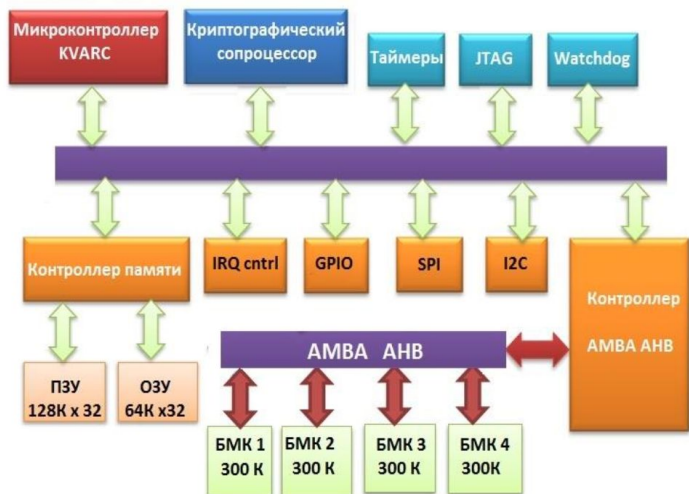


Актуальность использования отечественной платформы:

- ❑ Ограничения использования отечественными предприятиями ОПК иностранных технологий и ЭКБ в связи с введением Евросоюзом и США санкций политического, экономического и военного характера;
- ❑ Угрозы безопасности при использовании импортной платформы из-за возможности наличия несанкционированных программно-аппаратных закладок;
- ❑ Следствием импортозависимости в области ЭКБ является постоянное гарантированное отставание тактико-технических характеристик (ТТХ) российской радиоэлектронной аппаратуры (РЭА), создаваемой из доступной покупной, а, следовательно, не новейшей импортной ЭКБ, от ТТХ аппаратуры зарубежных конкурентов-противников

К5512БП1Ф от АО «НИИМА

«Прогресс»

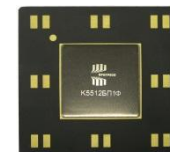


Микросхема К5512БП1Ф – программируемая полузаказная «СБИС-полуфабрикат»:

- ❑ Микропроцессорное ядро - 32-разрядный RISC микроконтроллер KVARC с тактовой частотой до 150 МГц – для переноса программной части проекта.
- ❑ Четыре блока БМК по 300К вентилей – для переноса аппаратной части проекта, реализованной на ПЛИС.
- ❑ Внутренняя память – ОЗУ 64К x 32 для поддержки работы микропроцессора.
- ❑ ПЗУ –128К x 32 – для хранения программ.
- ❑ Набор интерфейсов и шин - SPI, I2C, GPIO.
- ❑ Таймеры.

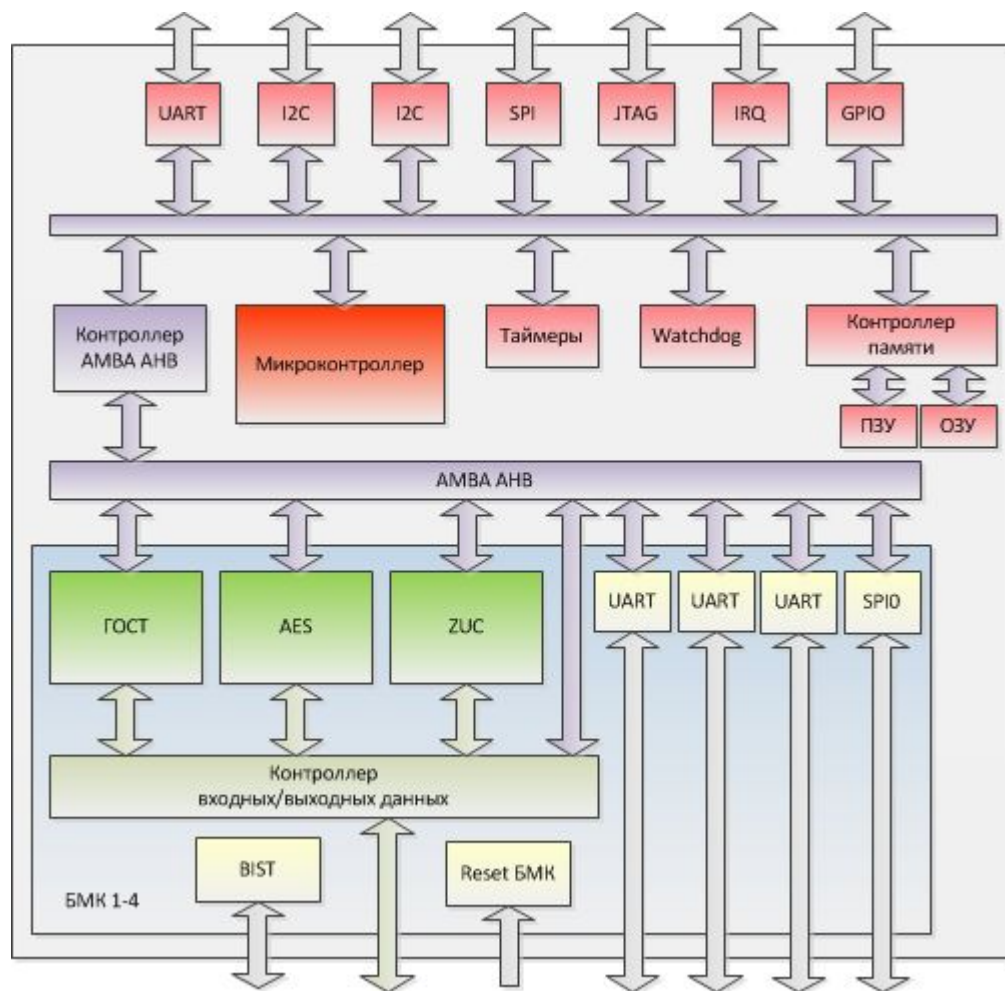
Функциональные и технологические особенности:

- ❑ Возможность создания узкоориентированных схем путем зашивки специализированного программного обеспечения.
- ❑ Реализация различных схем с жесткой логикой путем встраивания их в конструкцию БМК не меняя базовые слои и конструкцию всей СБИС. Меняются только слои коммутации.
- ❑ Значительно сокращаются сроки и стоимость разработки.
- ❑ Устраняется необходимость проведения квалификационных испытаний разрабатываемых микросхем.



Технология изготовления (отечественная фабрика)	КМОП 0,18 мкм HCMOS8D
Корпус металлокерамический;	типа CPGA
Количество выводов	325
Напряжение питания, В	1,8 и 3,3
Рабочая частота микропроцессора, МГц	до 150
Рабочая частота сопроцессора модульной арифметики, МГц;	до 50
Средняя потребляемая мощность, мВт не более	400
Температурный диапазон, °С	- 40 ... +125

Структурная схема СБИС



- ❑ IP ядра шифрования размещены в БМК 1-4;
- ❑ Архитектура IP ядер построены по конвейерному принципу, что позволяет достигать высоких скоростей шифрования и расшифрования;
- ❑ IP ядра шифрования имеют регистры шины AMBA AHB для конфигурирования;
- ❑ Данные для шифрования и расшифрования заходят непосредственно в БМК 1-4, минуя микроконтроллер и его периферию для поддержки высоких скоростей работы;
- ❑ Входные данные для всех IP ядер шифрования поступают в БМК 3;
- ❑ Выходные данные всех IP ядер шифрования выходят из БМК 2;
- ❑ IP ядро ГОСТ 28147-89 размещено в БМК 3, IP ядра ZUC и AES размещены в БМК 2;
- ❑ Тактовая частота работы IP ядер шифрования – 120 МГц;
- ❑ Тактовые частоты входного и выходного интерфейсов – 30 МГц.

Интерфейсы СБИС

- ❑ Используются стандартные интерфейсы, входящие в состав периферии микроконтроллера: UART, SPI, I2C;
- ❑ Для управления регистрами IP-ядер шифрования используется интерфейс AMBA 3 AHB-lite;
- ❑ Для загрузки и выгрузки данных для шифрования используется интерфейс Avalon stream

AMBA 3 AHB-lite, пример чтения и записи:

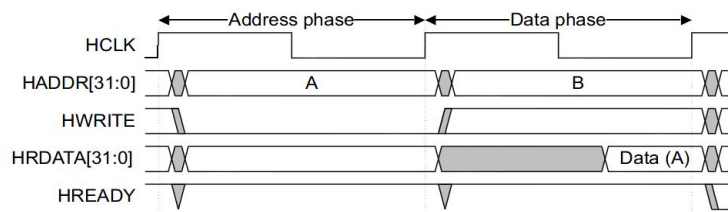


Figure 3-1 Read transfer

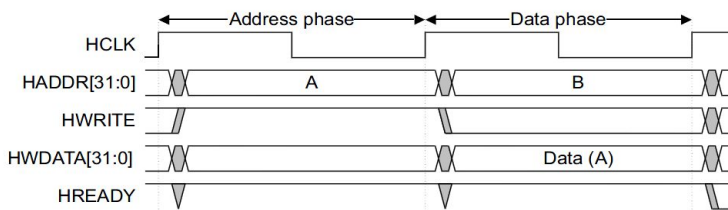
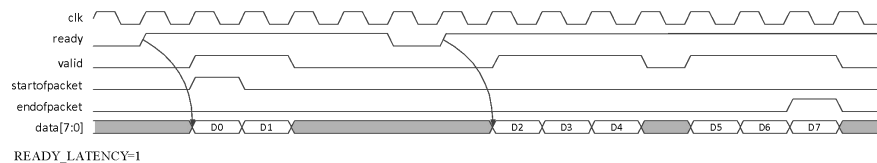
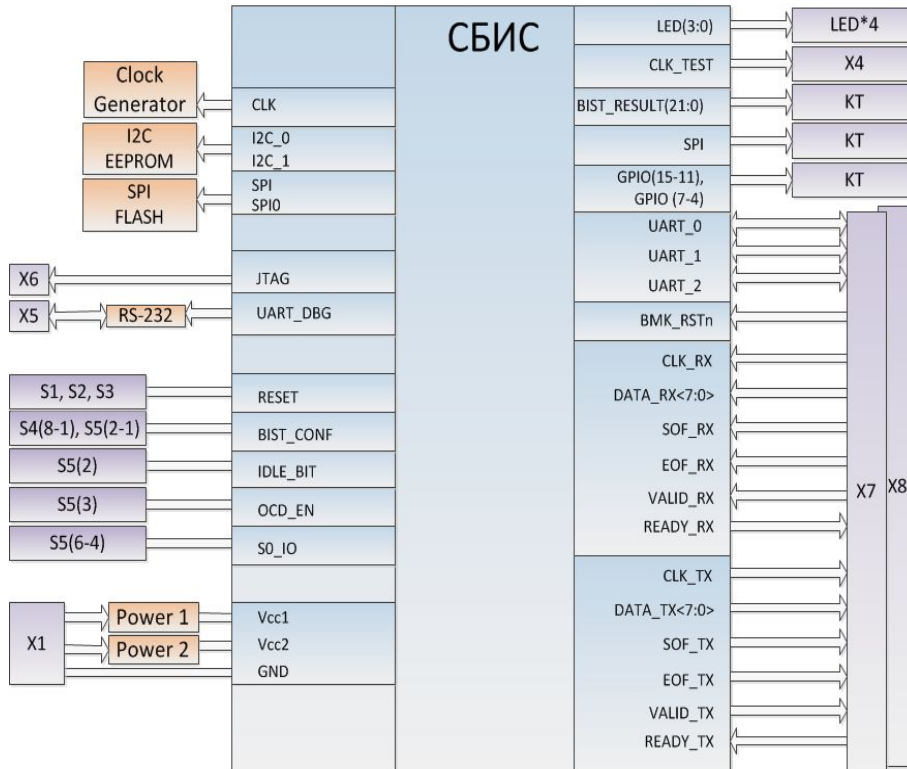


Figure 3-2 Write transfer

Avalon stream, пример транзакции:

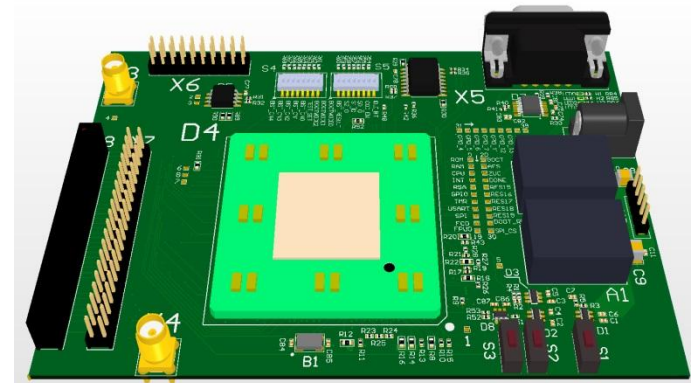


Структурная схема модуля



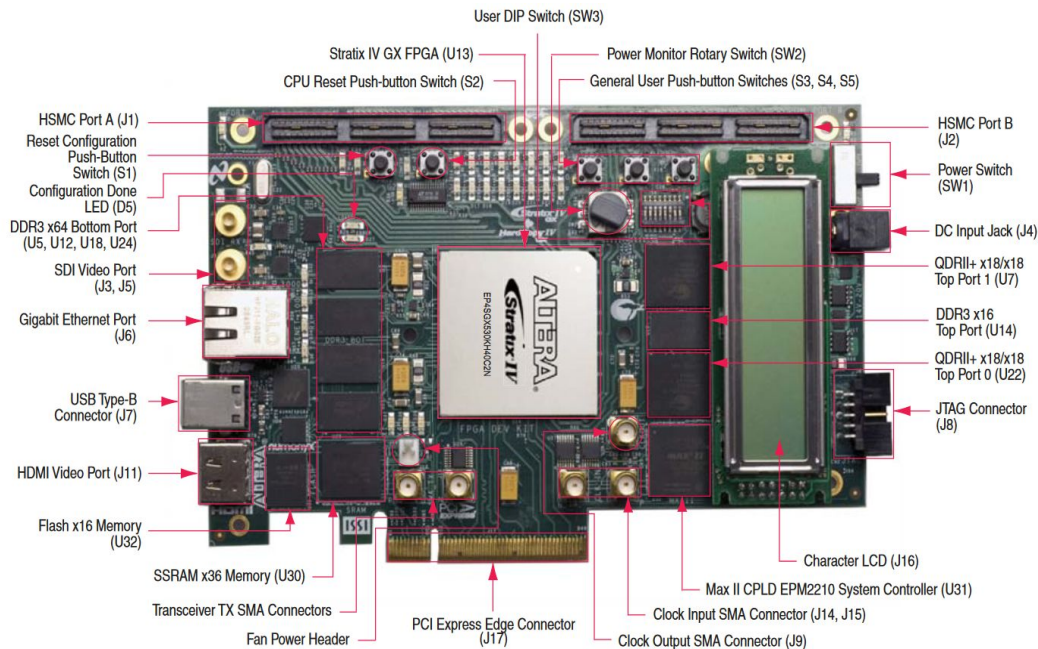
Электронный модуль состоит из платы с установленными на ней:

- ❑ СБИС;
- ❑ Микросхемой памяти EEPROM;
- ❑ Микросхемой флэш-памяти с интерфейсом I2C;
- ❑ Микросхемой интерфейса RS-232;
- ❑ Преобразователями напряжения;
- ❑ Светодиодами;
- ❑ Кварцевым генератором тактового сигнала;
- ❑ Переключателями, кнопками и разъемами.



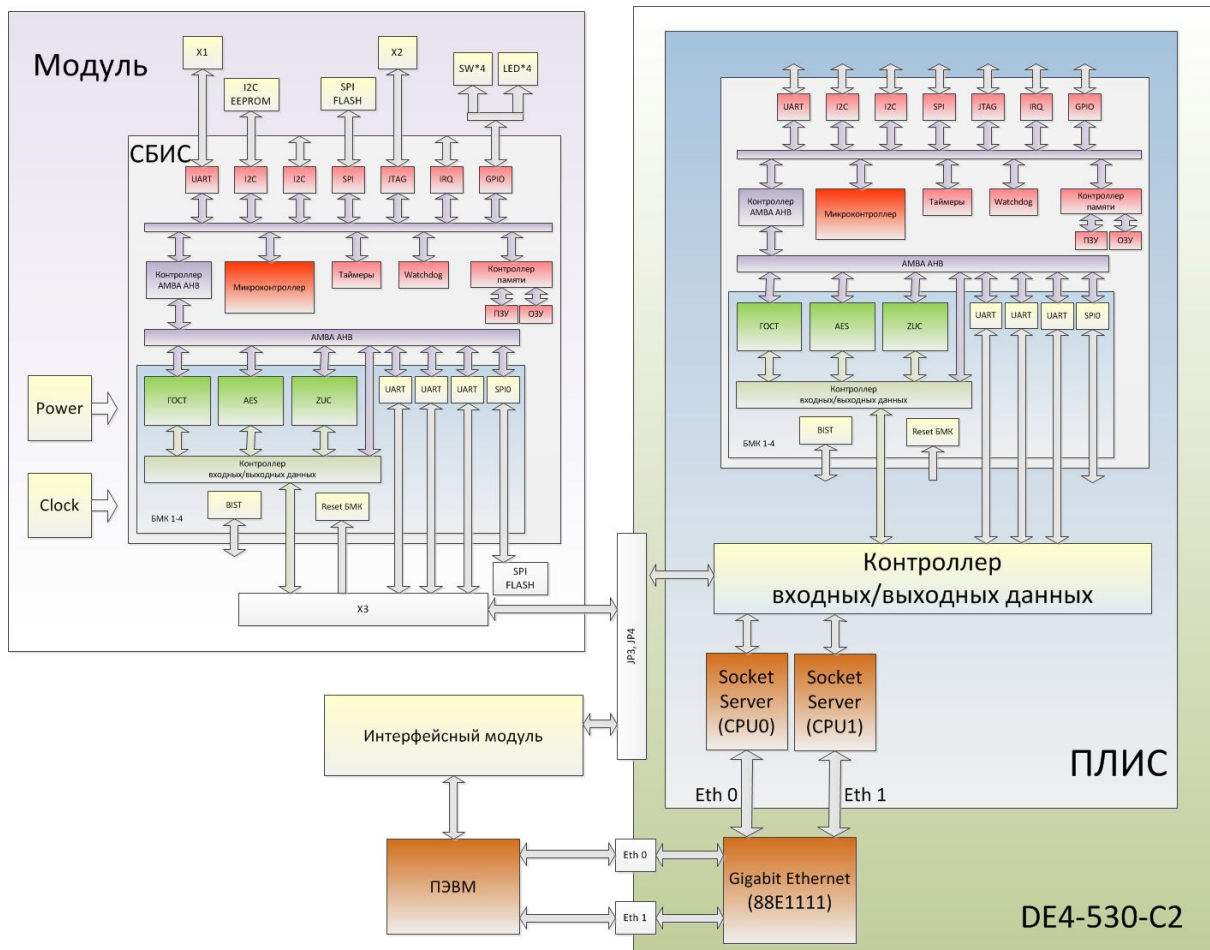
Отладочная плата для разработки и тестирования

Плата Altera DE4-530, содержит:



- ПЛИС Altera Stratix IV GX
 - 531,200 logic elements (LEs)
 - 27,376K total memory Kbits
 - 1,024 18x18-bit multipliers blocks
 - 4 PCI Express hard IP Blocks
 - 744 user I/Os
 - 8 phase locked loops (PLLs)
- Кварцевые генераторы;
- Микросхемы памяти DDR3, QDR II;
- Микросхема 10/100/1000BASE-T Ethernet PHY с разъемом RJ-45;
- CPLD MAX II для управления;
- PCI Express x8 разъем;
- USB-blaster для загрузки прошивки ПЛИС;
- Преобразователи напряжения;
- Дисплей LCD
- Светодиоды;
- Переключатели, кнопки и разъемы.

Блок-схема подключения модуля к отладочной плате



Плата Altera DE4-530 используется:

- На первом этапе: для тестирования и отладки RTL. Создается проект для ПЛИС, повторяющий структуру СБИС. Он содержит модели микроконтроллера с периферией, а также IP ядра шифрования. Помимо «СБИС в ПЛИС» проект содержит контроллер входных и выходных данных и два софт-процессора для загрузки и выгрузки данных через Ethernet.
- После изготовления модуля: модуль подключается к отладочной плате, через нее производится загрузка данных и конфигурирование для проведения различных тестов.

Маршрут проектирования

АО «Концерн «Созвездие»

- Разработка алгоритмов и архитектуры;
- Разработка RTL алгоритмов шифрования;
- Разработка алгоритмов;
- Адаптация RTL с учетом интерфейсов и требований целевой СБИС;
- Софт-тестирование;
- Тестирование на отладочной плате



АО «НИИМА «Прогресс»

- Разработка нетлиста и топологии;
- Верификация с учетом задержек в кристалле;



АО «Концерн «Созвездие»

- Изготовление модуля;
- Тестирование в составе модуля;
- Применение в составе изделий



ПАО «Микрон»

- Производство кристалла, тестирование;
- Корпусирование

Адаптация RTL с учетом интерфейсов и требований целевой СБИС (с точки зрения разработчика ПЛИС):

- Оценка ресурсов, разделение на отдельные составные части (отдельные БМК);
- Нельзя использовать PLL, hard IP ПЛИС;
- Адаптация дерева тактовых сигналов;
- Использование памяти в соответствии с установленной в БМК;
- Нельзя использовать ряд конструкций, которые де-факто поддерживаются всеми современными синтезаторами ПЛИС (например, начальное значение регистра).



Спасибо за внимание!