

Проблемные вопросы создания отечественных средств вычислительной техники в защищенном исполнении



Ренат Юсупов, старший вице-президент Крафтвэй
февраль 2020 г.

Как регулируется отечественность и защищённость

- **Минпромторг:**
 - ПП 878, реестр отечественных СВТ и ТКО
 - Гособоронзаказ
- **Минкомсвязь:**
 - ПП 1236, реестр отечественного ПО
- **ФАС:**
 - 44-ФЗ, О контрактной системе в сфере закупок.....
 - 223-ФЗ, О закупках товаров, работ, услуг отдельными видами юрлиц
- **ФСТЭК:**
 - Приказ – 17, требования к защите информации ГИС
 - Приказ - 25, требования к СВТ
 - Приказ - 31, 235, 239 требования к защите информации объектов КИИ
- **ФСБ:**
 - Закон "О государственной тайне" N 5485-1
 - Временные требования
- **МО**

Что такое отечественные СВТ в защищённом исполнении

- Отечественный процессор. **ДА**
- Отечественные контроллеры (со встроенным ПО) **НЕТ**
 - Ввод/вывод (сетевые, USB, низкоскоростные) (исключение – КПИ-2)
 - Отображение информации
 - Мониторинг и управление (пример – BMC)
 - Информационная безопасность (пример – Apple T2)
- Отечественные материнские платы. **ДА**
- Отечественные электронные модули (со встроенным загружаемым ПО) **НЕТ**
 - Накопители информации
 - Модули памяти
 - RAID, HBA
 - Ускорители
 - Модули защиты информации (МДЗ, шифротехника)
- Отечественные шасси и системы охлаждения **ДА**
- Отечественные дисплейные устройства **НЕТ**
- Отечественное периферийное оборудование **НЕТ**
- Отечественная кабельная продукция **ДА**

Легенда: **реализовано** **в разработке** **нет информации**

Отечественные СВТ в защищённом исполнении. ЭКБ и электронные модули

Цель: Построение отечественной защищённой платформы СВТ

■ Процессоры:

- Процессоры: Эльбрус - 1С+, 4С, 8С, 8СВ (VLIW), R-2000 (SPARC)
- Байкал – Т (MIPS), М (ARM);
- Элвис – 1892ВМ14Я (ARM), ВМ10Я и ВМ7Я (MIPS);
- Комдив – 32, 64 (MIPS)

■ Микросхемы контроллеров

- SSD – Крафтвер 1942ВК018

■ Электронные модули

- Материнские платы (Аквариус, Депо, Крафтвер...)
- Модули доверенной загрузки
- Модули на ПЛИС

Не имея полного комплекта отечественных ЭКБ нельзя гарантировать отсутствие недеklarированных возможностей СВТ.

ТИПОВАЯ АРХИТЕКТУРА ОТЕЧЕСТВЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ 2019



ТИПОВАЯ АРХИТЕКТУРА ОТЕЧЕСТВЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ 2020



ТИПОВАЯ АРХИТЕКТУРА ОТЕЧЕСТВЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ 2021

 Уязвимые

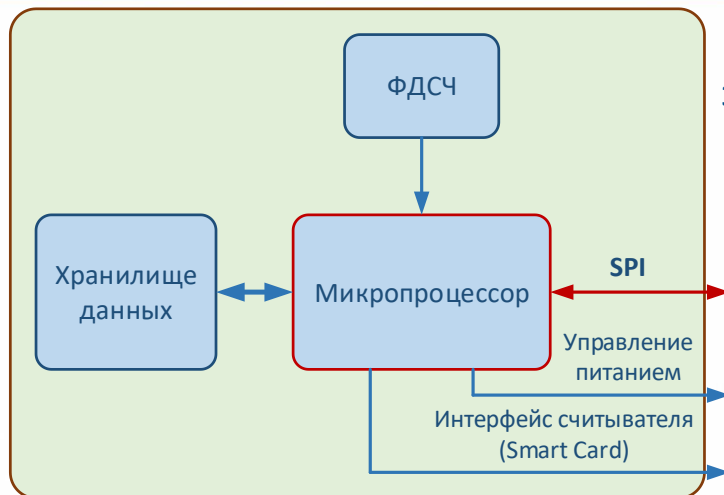
 В разработке

 Отечественные



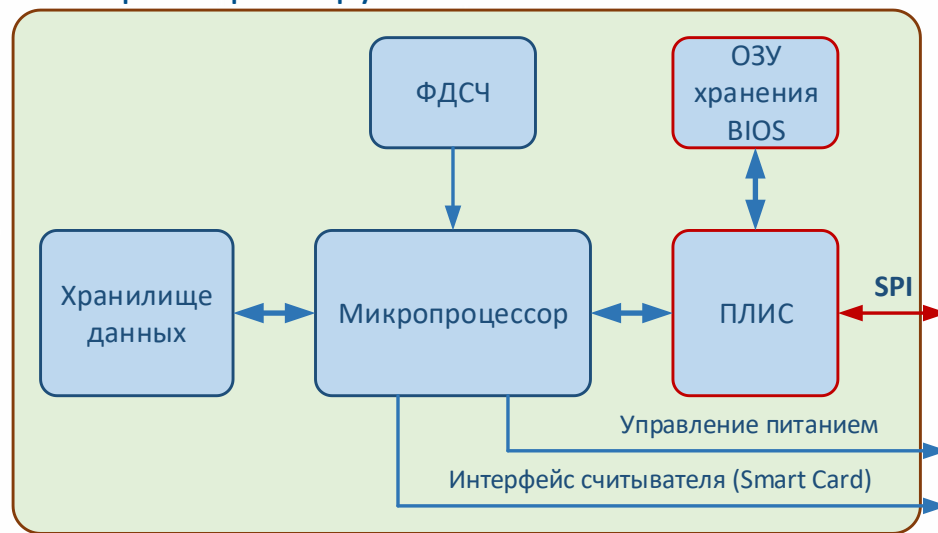
Варианты реализации «ядра доверия».

Модуль доверенной загрузки.

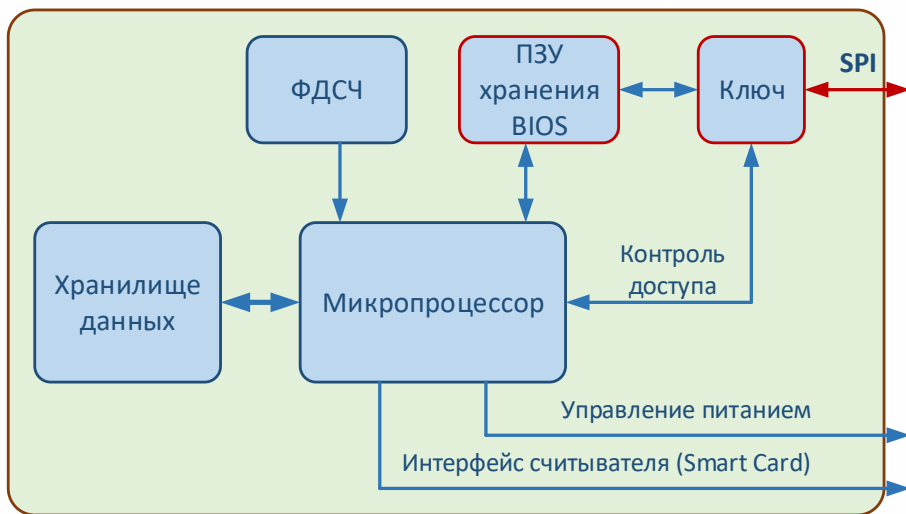


1. Схема контроля и загрузки BIOS с эмуляцией загрузочной памяти на микропроцессоре

2. Схема контроля и загрузки BIOS с эмуляцией контроллера загрузочной памяти на ПЛИС



3. Схема контроля доступа BIOS к загрузочной памяти на АПМДЗ

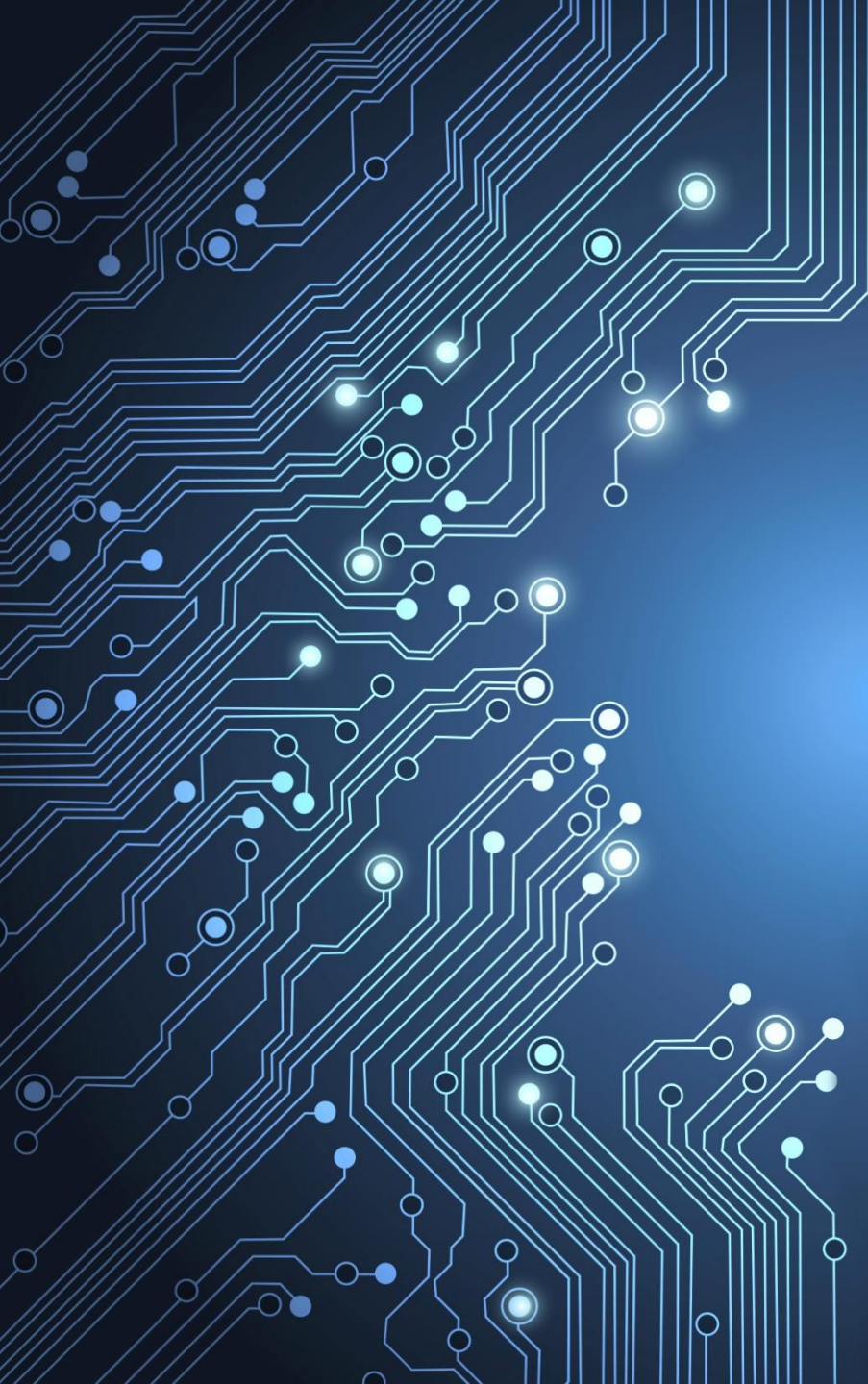


Варианты реализации ядра доверия СВТ. Микросхема «ядра доверия».

Требования к микросхеме «ядра доверия»

- Управление электропитанием и режимами энергопотребления СВТ
- Управления инициализацией СВТ
- Формирование защищённого сетевого канала
- Аутентификация и идентификация
- Защищённое хранилище
- Генерация случайных чисел
- Контроль аппаратных и программных компонент СВТ
- Обнаружение событий безопасности с возможностью блокировки работы СВТ
- Аппаратное экранирование/отключение внешних интерфейсов
- Высокоскоростное потоковое специальное преобразование блочной передачи данных
- Дистанционное отображение состояния и управление настройками СВТ

Наличие микросхемы безопасности в каждом отечественном защищённом СВТ решит проблему информационных угроз недоверенных микросхем контроллеров и электронных модулей.

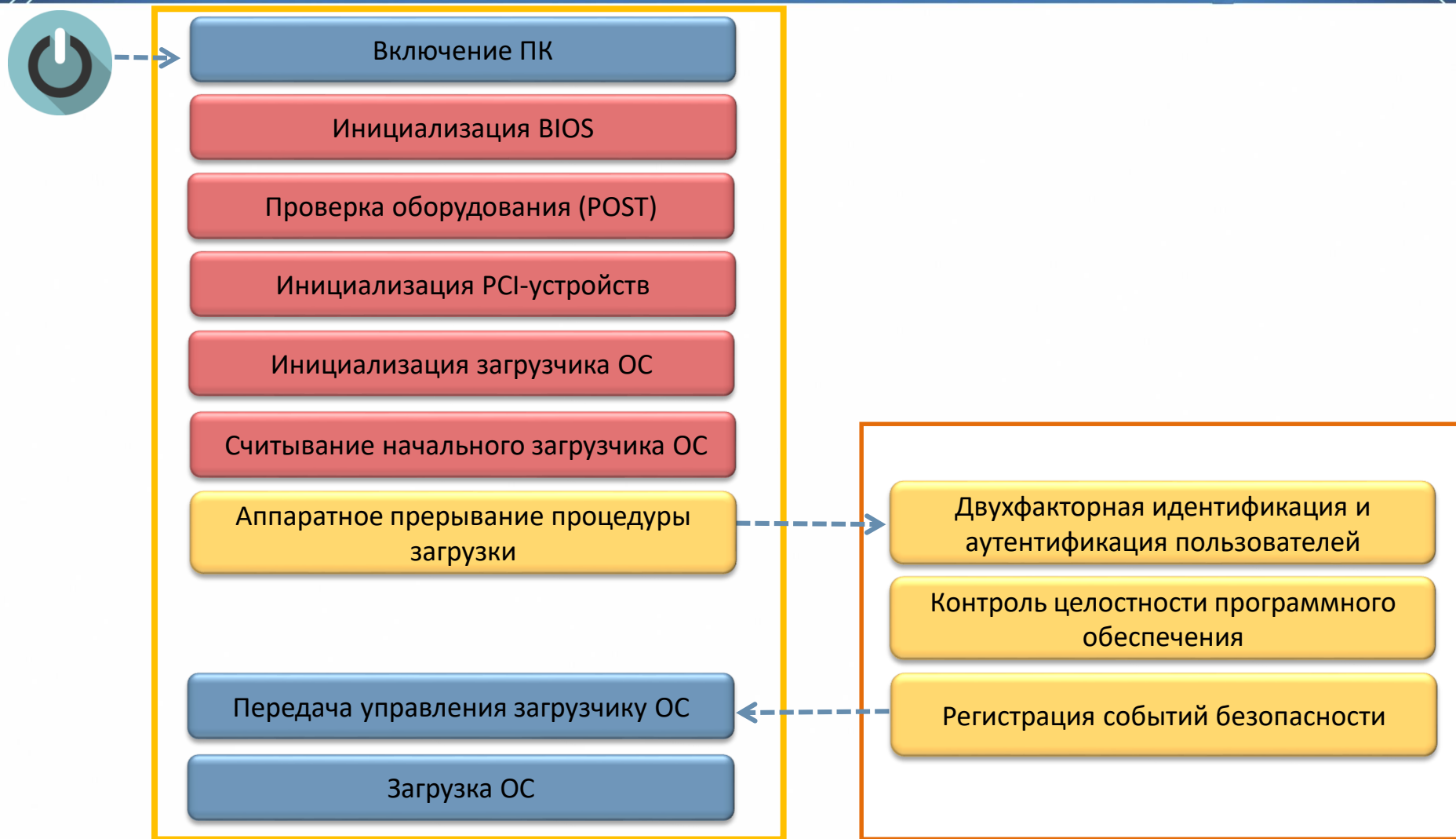


Проектирование
отечественных
защищённых СВТ.

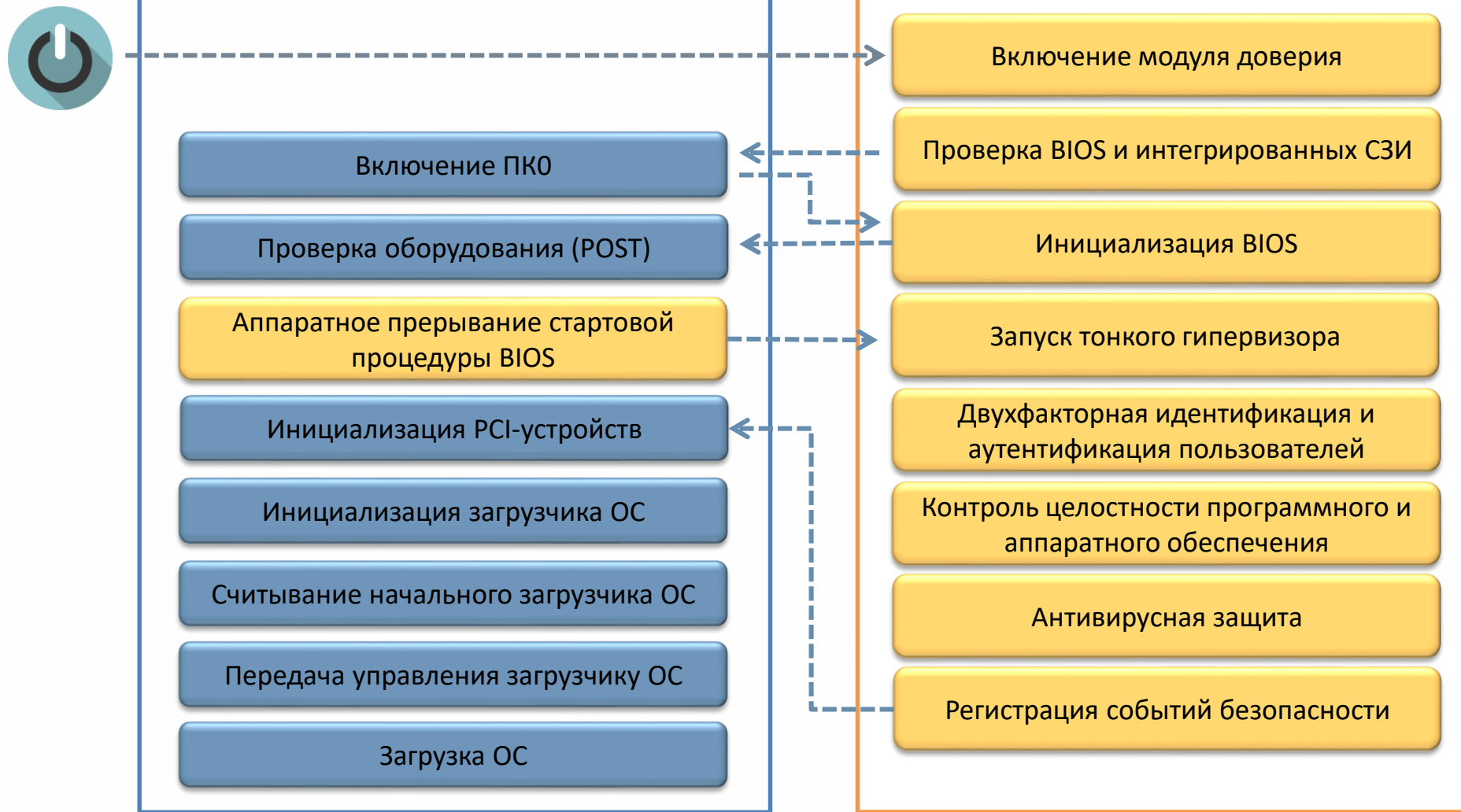
*Задачи и методы
решения.*

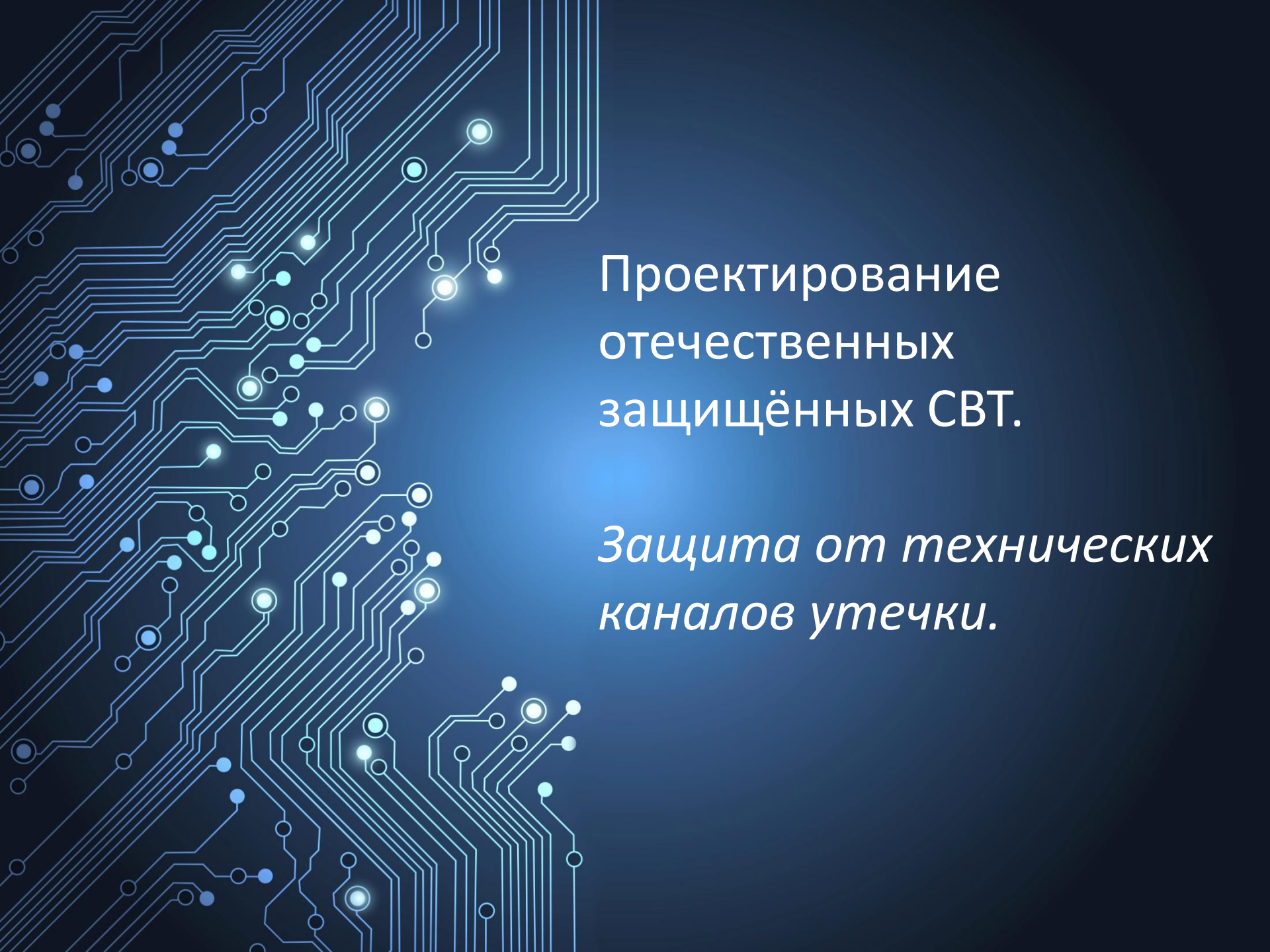
- Встраивание «ядра доверия» в схемотехнику материнской платы
 - управление инициализацией
 - контроль программных и аппаратных модулей
 - контроль электропитания и режимов работы
 - «прозрачный контроль» в режиме эксплуатации
- Переработка BIOS:
 - интеграции с «ядром доверия»
 - встраивание дополнительных функций безопасности (пример: антивирус UEFI)
 - среда исполнения низкоуровневых приложений
 - соответствие отраслевым стандартам UEFI

Работа СЗИ (СДЗ) в типовом СВТ.



Работа СЗИ (СДЗ) в защищённом СВТ. Реализация





Проектирование
отечественных
защищённых СВТ.

*Защита от технических
каналов утечки.*

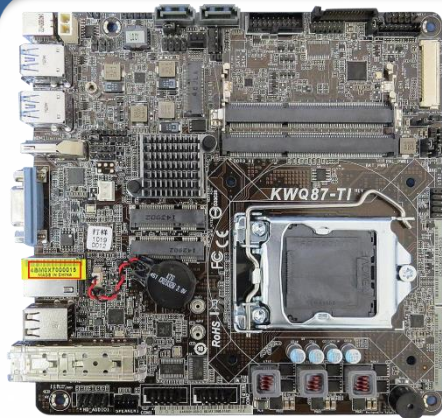
Практика создания СВТ с защитой от технических каналов утечки

- Использование в ЭКБ материнских плат микроконтроллеров не имеющих встроенных прошивок
- Глубокая переработка BIOS с заменой, удалением или ограничением функциональности потенциально небезопасных модулей
- Интеграция в BIOS модуля низкоуровневой виртуализации устройств ввода-вывода («тонкий» гипервизор) для контроля потоков и подключаемых устройств
- Аппаратная фильтрация контроллеров мониторинга и управления.

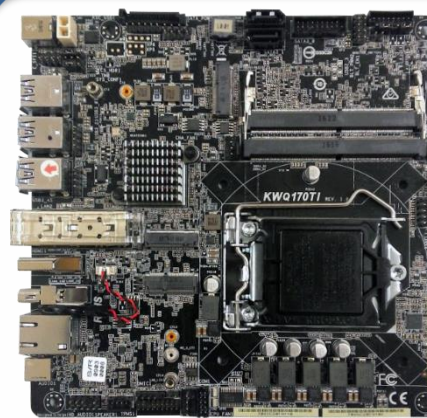
Методы защиты от технических каналов утечки информации:

- Трассировка печатных плат с учётом снижения побочных электромагнитных излучений
- Отключение линий ввода/вывода при отсутствии полезной нагрузки
- Экранирование на материнской плате микросхем формирователей высокочастотных сигналов
- Согласование по импедансу высокочастотных линий ввода/вывода с дополнительной фильтрацией сигналов
- Дополнительное экранирование внутренних устройств и соединительных шлейфов
- Специализированный дизайн шасси и кабелей.

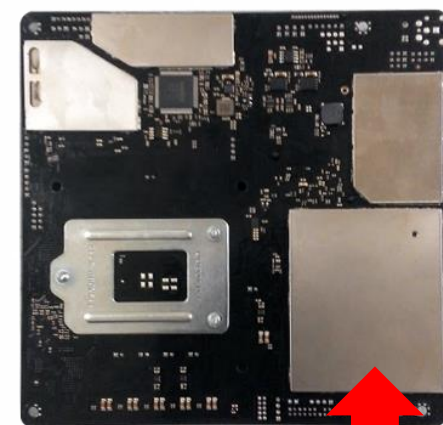
Некоторые особенности материнских плат с защитой от технических каналов утечки по ПЭМИ



Прежде



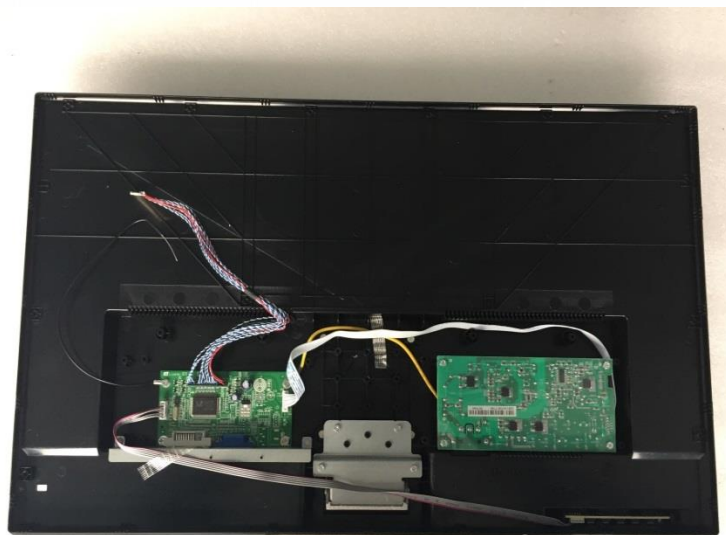
Сейчас



Формирователи высокочастотных
сигналов помещены в EMI-экраны

Некоторые особенности дисплейных устройств с защитой от технических каналов утечки

Прежде



Сейчас



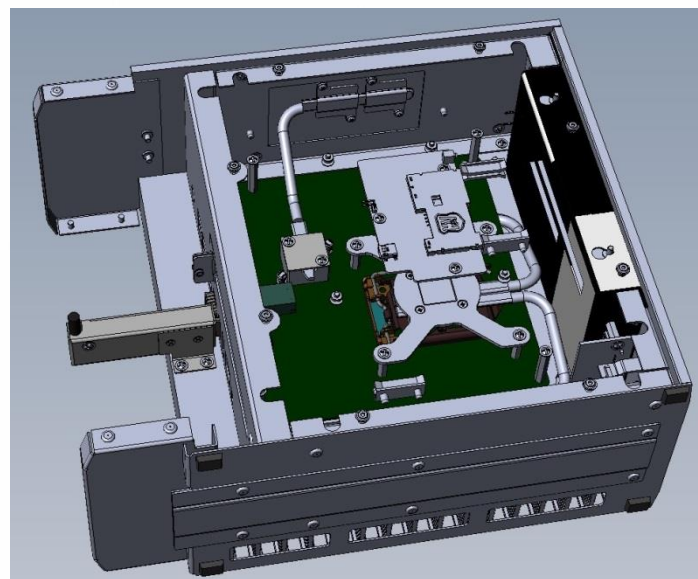
Электронные платы помещены в EMI-экраны
Кабели экранированы

Некоторые особенности конструктивов шасси с защитой от технических каналов утечки

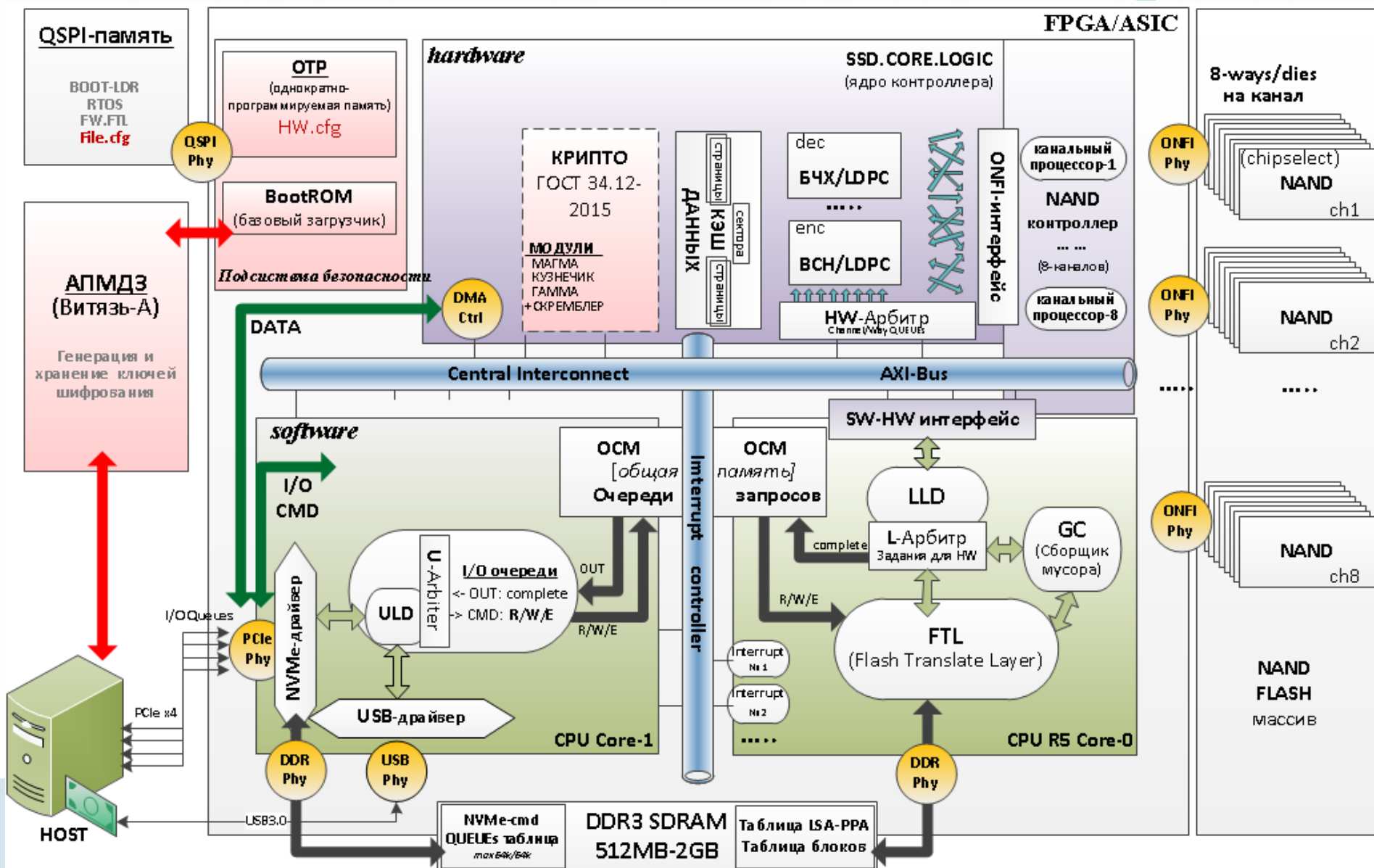
Прежде



Сейчас



Разработка отечественных контроллеров для СВТ в защищённом исполнении



Разработка отечественных контроллеров для СВТ в защищённом исполнении



Потребность в отечественных микросхемах контроллеров для проектирования защищённых СВТ

- Микросхемы сетевых контроллеров
- Микросхема контроллера «ядро доверия»
- Микросхемы контроллеров RAID/HBA для серверов и СХД
- Микросхема управления и мониторинга для серверов и СХД (ВМС)
- Микросхемы формирователей видеосигналов HDMI/DP
- Микросхема управления «emdedded controller»
- Микросхемы контроллеров интерфейсов USB