



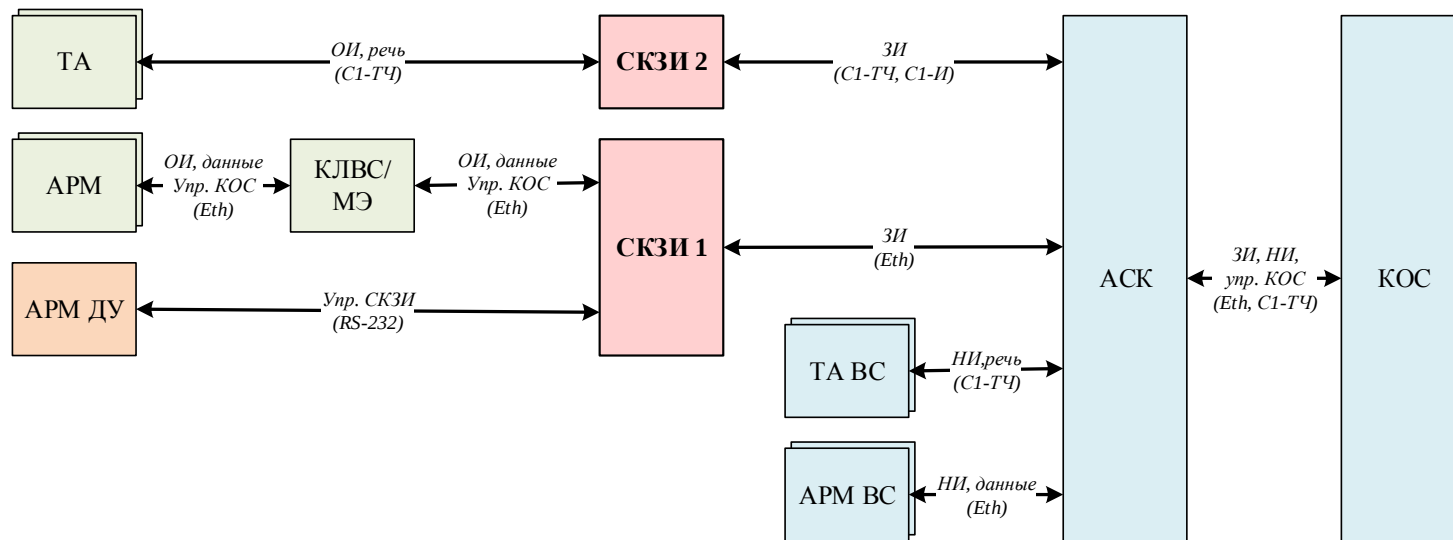
# **Исследование возможности реализации программного средства доверенной загрузки операционных систем семейства КПДА в специализированных изделиях**

*Руководитель проектов по разработке встраиваемых решений,  
заместитель начальника отдела, к.т.н, ТРИЗ 1 **Боровиков А.Ю.***

*Научный сотрудник **Карпов А.П.***

# Обобщенная структурная схема комплекса связи

## СТРУКТУРНАЯ СХЕМА

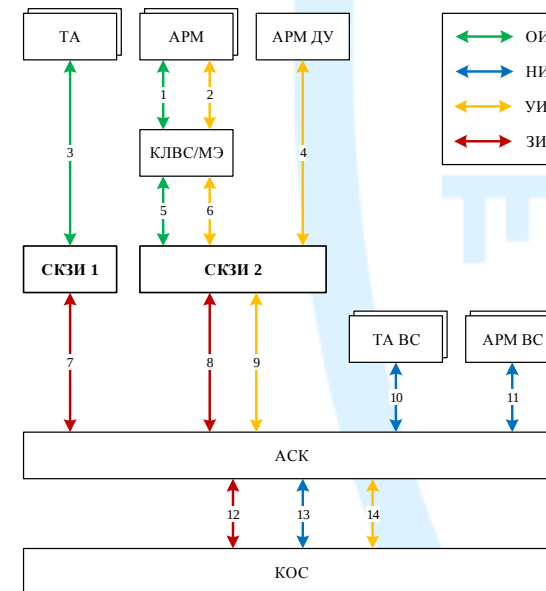


## ДОВЕРЕННОЕ УПРАВЛЕНИЕ СКЗИ

Типовым требованием при встраивании СКЗИ в комплексы связи является доверенное управление СКЗИ. Необходимость реализации данных функций обусловлена возможностью реализации угроз информационной безопасности за счет недоведения (либо доведения искаженных) команд управления СКЗИ

**Для обеспечения доверенного управления СКЗИ необходима реализация на техническом средстве управления СКЗИ комплекса организационно-технических мер защиты от актуальных угроз информационной безопасности**

## СХЕМА ИНФОРМАЦИОННЫХ ПОТОКОВ



## РУКОВОДЯЩИЕ ДОКУМЕНТЫ

1. Нормативные документы ФСБ России
2. Требования к объектам применения СКЗИ

# Угрозы безопасности информации и меры защиты, оцениваемые при анализе комплекса связи

## Угрозы

- ☐ Утечка информации в каналы связи по каналам управления
- ☐ Навязывание ложной информации по каналам связи

## Опасные события

- ☐ Недоведение команд управления до СКЗИ

## Факторы

- ☐ Несанкционированный доступ к аппаратно-программному обеспечению и командам управления СКЗИ
- ☐ Сбои и неисправности аппаратного обеспечения
- ☐ Недекларируемые функции, уязвимости и опасные функциональные возможности программного обеспечения

## Меры защиты информации

- ✓ Средства доверенной загрузки операционной системы на этапе начального старта
- ✓ Средства защиты информации на этапе работы операционной системы
- ✓ Механизмы защиты информации уровня специального программного обеспечения
- ✓ Механизмы защиты от физического доступа к аппаратному обеспечению и неиспользуемым разъемам
- ✓ Механизмы повышения отказоустойчивости аппаратного обеспечения
- ✓ Выполнение требований ГОСТ Р 56939-2016 при разработке специального программного обеспечения
- ✓ Тестирование специального программного обеспечения
- ✓ Исследования специального программного обеспечения по требованиям регулятора

# Проблемы при разработке и проведении исследований специализированных изделий

| Компонент                                        | Проблема                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Модуль процессора                                | <ul style="list-style-type: none"><li><input type="checkbox"/> Отсутствие гарантий проектирования</li><li><input type="checkbox"/> Отсутствие конструкторской документации</li><li><input type="checkbox"/> Отсутствие сопровождения на всем жизненном цикле</li></ul>                                                                                                                                                            |
| Встроенное программное обеспечение               | <ul style="list-style-type: none"><li><input type="checkbox"/> Отсутствие исходных текстов</li><li><input type="checkbox"/> Отсутствие программной и эксплуатационной документации</li><li><input type="checkbox"/> Возможное наличие опасных функциональных возможностей и недекларированных функций (ОФВ, НДВ)</li><li><input type="checkbox"/> Большие объемы бинарного кода и наличие зашифрованных фрагментов кода</li></ul> |
| Операционная система                             | <ul style="list-style-type: none"><li><input type="checkbox"/> Монолитность архитектуры</li><li><input type="checkbox"/> Ошибки и уязвимости</li><li><input type="checkbox"/> Трудоемкость проведения работ по оценке влияния ОС на механизмы защиты информации</li><li><input type="checkbox"/> Возможное наличие ОФВ, НДВ</li></ul>                                                                                             |
| Прикладное и специальное программное обеспечение | <ul style="list-style-type: none"><li><input type="checkbox"/> Ошибки и уязвимости</li><li><input type="checkbox"/> Возможное наличие ОФВ, НДВ</li><li><input type="checkbox"/> Трудоемкость пооператорной инспекции исходных текстов больших объемов</li></ul>                                                                                                                                                                   |

# Технические предложения по созданию специализированных изделий

| Компонент                                        | Предложения                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Модуль процессора                                | <ul style="list-style-type: none"><li>✓ Применение аппаратных платформ отечественного производства</li></ul>                                                                                                                                                                                                                                                                                                                                                                  |
| Встроенное программное обеспечение               | <ul style="list-style-type: none"><li>✓ Применение отечественной базовой системы ввода-вывода с минимальным использованием заимствованного бинарного кода</li><li>✓ Применение средств доверенной загрузки операционной системы</li></ul>                                                                                                                                                                                                                                     |
| Операционная система                             | <ul style="list-style-type: none"><li>✓ Использование отечественных операционных систем с микроядерной отказоустойчивой архитектурой и минимальным набором необходимых модулей</li><li>✓ Применение СЗИ уровня операционной системы</li></ul>                                                                                                                                                                                                                                 |
| Прикладное и специальное программное обеспечение | <ul style="list-style-type: none"><li>✓ Разработка прикладного и специального программного обеспечения в соответствии с требованиями национальных стандартов по разработке безопасного программного обеспечения.</li><li>✓ Минимизация использования модулей заимствованных библиотек</li><li>✓ Реализация механизмов защиты на уровне специального программного обеспечения</li><li>✓ Исследования специального программного обеспечения по требованиям регулятора</li></ul> |

# Преимущества использования защищенных операционных систем реального времени семейства КПДА

- ✓ Микроядерная отказоустойчивая архитектура реального времени
- ✓ Поддержка многих отечественных и иностранных процессорных платформ и архитектур
- ✓ Развитые средства разработки и отладки
- ✓ Для ЗОСРВ «Нейтрино» получены сертификаты соответствия МО РФ по требованиям:
  - Требования безопасности информации к ОС
  - Профиль защиты ОС типа А второго класса защиты. ИТ.ОС.А2.ПЗ
  - Профиль защиты ОС типа В второго класса защиты. ИТ.ОС.В2.ПЗ
  - Требования к межсетевым экранам
  - Профиль защиты МЭ типа Б второго класса защиты. ИТ.МЭ.Б2.ПЗ
  - Профиль защиты МЭ типа В второго класса защиты. ИТ.МЭ.В2.ПЗ
  - 2-ой уровень контроля отсутствия НДВ
  - Соответствие реальных и декларируемых возможностей
- ✓ Для ЗОСРВ «ТрастОС» получено заключение о соответствии «Временным требованиям к программному обеспечению, используемому в автоматизированных системах ИТКС специального назначения» и может использоваться в автоматизированных системах, хранящих и обрабатывающих информацию ограниченного доступа
- ✓ Высокая отработанность – начиная с 2011 года Нейтрино успешно применяется многими российскими предприятиями ОПК и гражданской промышленности

# Оценка возможности применения существующих средств доверенной загрузки в специализированных изделиях

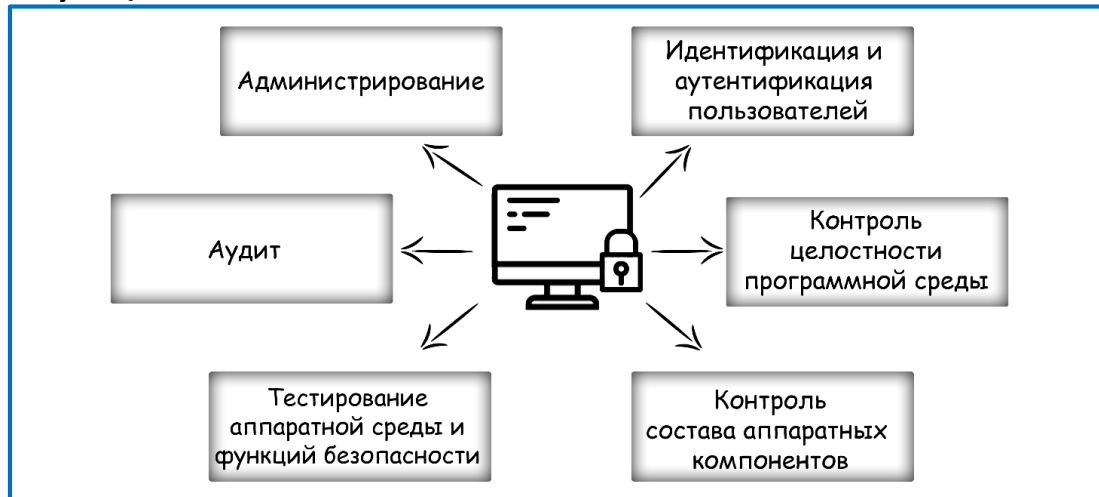
## Определение

**Средства доверенной загрузки** – это программные и программно-технические средства, используемые в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом и реализующие функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки.

Приказ ФСТЭК России от 27.09.2013 года № 119 определяет типы и классы защиты для средств доверенной загрузки

| Тип СДЗ                                 | Класс 6        | Класс 5        | Класс 4        | Класс 3        | Класс 2        | Класс 1        |
|-----------------------------------------|----------------|----------------|----------------|----------------|----------------|----------------|
| СДЗ уровня базовой системы ввода-вывода | -              | -              | ИТ.СДЗ. УБ4.ПЗ | ИТ.СДЗ. УБ3.ПЗ | ИТ.СДЗ. УБ2.ПЗ | ИТ.СДЗ. УБ1.ПЗ |
| СДЗ уровня платы расширения             | -              | -              | ИТ.СДЗ. ПР4.ПЗ | ИТ.СДЗ. ПР3.ПЗ | ИТ.СДЗ. ПР2.ПЗ | ИТ.СДЗ. ПР1.ПЗ |
| СДЗ уровня загрузочной записи           | ИТ.СДЗ. 336.ПЗ | ИТ.СДЗ. 335.ПЗ | -              | -              | -              | -              |

## Функции безопасности



## ПРОБЛЕМА - ОТСУТСТВИЕ КОМПЛЕКТУЮЩИХ И НЕСООТВЕТСТВИЕ ТТХ ТС ДУ СДЗ УРОВНЯ ПЛАТЫ РАСШИРЕНИЯ

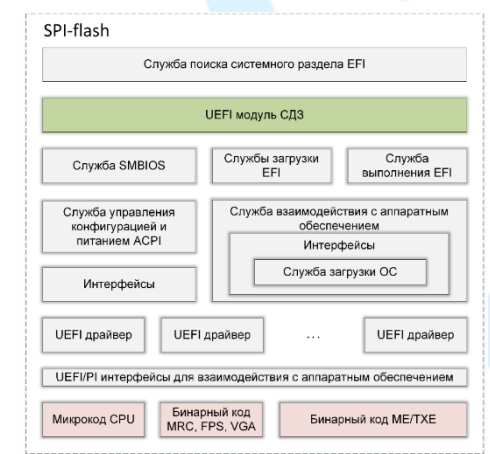


## РЕШЕНИЕ – ПРОГРАММНЫЕ СДЗ УРОВНЯ БСВВ



## Программные СДЗ уровня БСВВ и их классическая архитектура

| Производитель                | Наименование                   |
|------------------------------|--------------------------------|
| АО «Крафтвэй корпорэйшн ПЛС» | ПК «Электронный замок «ВИТЯЗЬ» |
| АО «ИнфоТекс»                | ПК «ПМДЗ ViPNet SafeBoot»      |
| ООО «Газинформсервис»        | СДЗ «SafeNode System Loader»   |
| ОКБ САПР                     | МДЗ «Аккорд-МКТ»               |
| ООО «Код Безопасности»       | ПК «Соболь»                    |
| ООО «НумаТех»                | МДЗ «Numa Arce»                |



# Обоснование трудоемкости проведения исследований программных средств доверенной загрузки

## Опасные функциональные возможности (ОФВ)

Ошибки

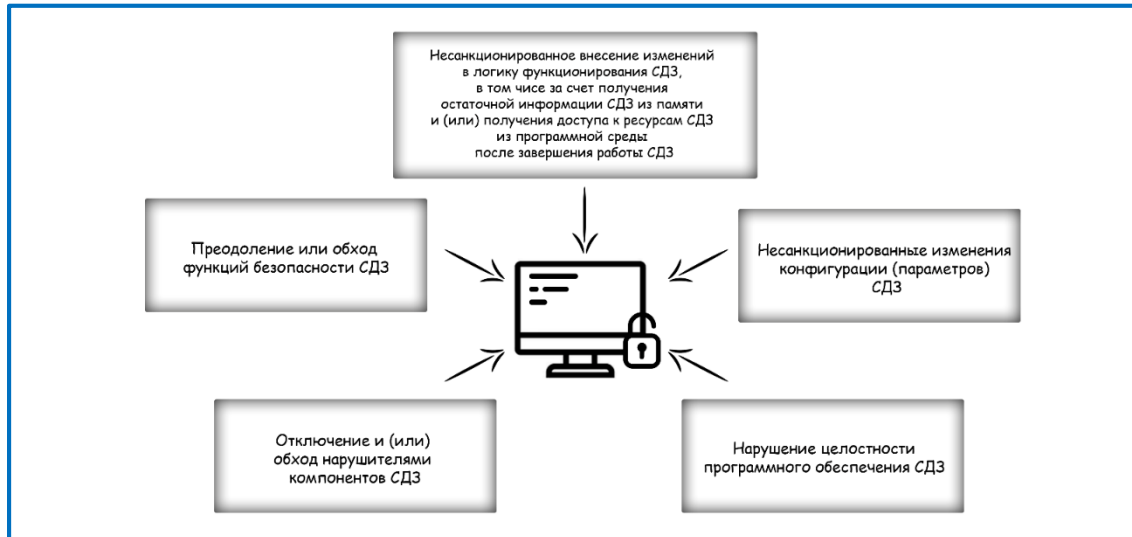
Дефекты

НДВ

Уязвимости

Негативное влияние на  
функции СДЗ

## Влияние



Вывод

**ТРЕБУЮТСЯ ИССЛЕДОВАНИЯ,  
НАПРАВЛЕННЫЕ НА ПОИСК И УСТРАНЕНИЕ ОФВ В БСВВ**

## Недостатки иностранной БСВВ

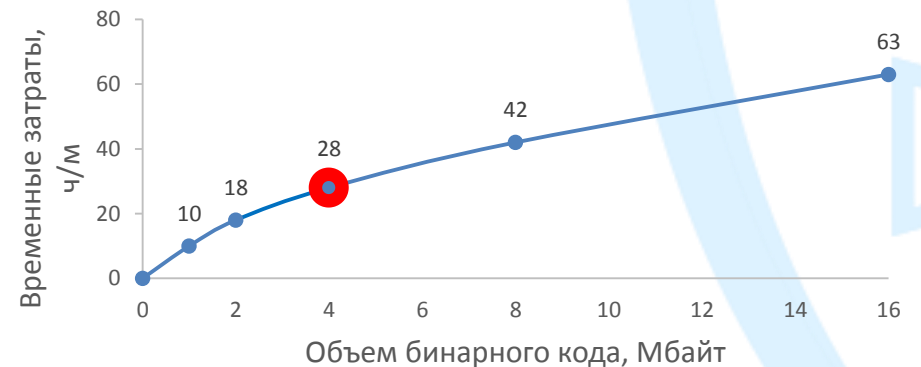
Отсутствие  
исходного кода и ПД

Отсутствие реализации  
требований по встраиванию СДЗ

Большой объем бинарного  
кода и сложность

Трудоемкие работы по  
реверс-инжинирингу

## Зависимость временных затрат от объема бинарного кода БСВВ



Вывод

**ИССЛЕДОВАНИЯ ТРУДОЕМКИЕ, ДОРОГОСТОЯЩИЕ,  
НЕВЫПОЛНИМЫЕ В ЗАДАННОЕ ВРЕМЯ**



# Распределенная архитектура программного средства доверенной загрузки уровня базовой систем ввода-вывода

## Перечень функций безопасности

- ✓ идентификация и аутентификация пользователей
- ✓ контроль целостности программной среды
- ✓ контроль состава аппаратных компонентов
- ✓ тестирование аппаратной среды и функций безопасности
- ✓ аудит
- ✓ управление функциями безопасности и настройка их параметров
- ✓ исполнение функций безопасности на основе их параметров

## Перечень функциональных требований

- ✓ пользовательский интерфейс взаимодействия с оператором
- ✓ локальное и удаленное управление функциями безопасности
- ✓ взаимодействие с USB-токенами
- ✓ взаимодействие с объектами контроля целостности
- ✓ взаимодействие с объектами контроля состава аппаратных компонентов
- ✓ взаимодействие с файлами конфигурации
- ✓ взаимодействие с журналом безопасности и объектами аудита
- ✓ реализация протоколов прикладного уровня и удаленного вызова процедур
- ✓ инициализация аппаратных компонент и взаимодействие с заимствованным бинарным кодом
- ✓ построение карты памяти и дерева ресурсов системы
- ✓ настройка параметров аппаратных компонентов
- ✓ поиск устройства загрузки и передача управления на загрузчик ОС

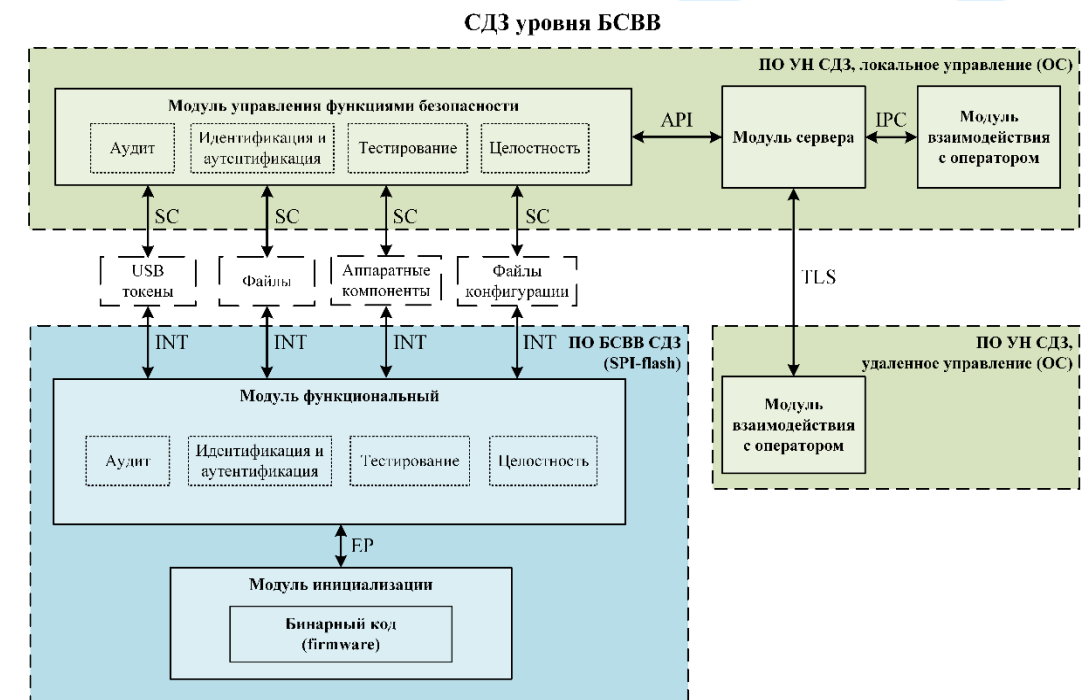
## Перечень нефункциональных требований

- ✓ надежность (способность безотказно выполнять определенные функции при заданных условиях в течение заданного периода времени)
- ✓ безопасность (отсутствие влияния стороннего ПО на управление и исполнение функций безопасности)
- ✓ кроссплатформенность (способность работать с несколькими аппаратными платформами или операционными системами)
- ✓ адаптивность (возможность оперативной модификации и устранения выявленных уязвимостей)
- ✓ эргономичность (удобство в использовании)

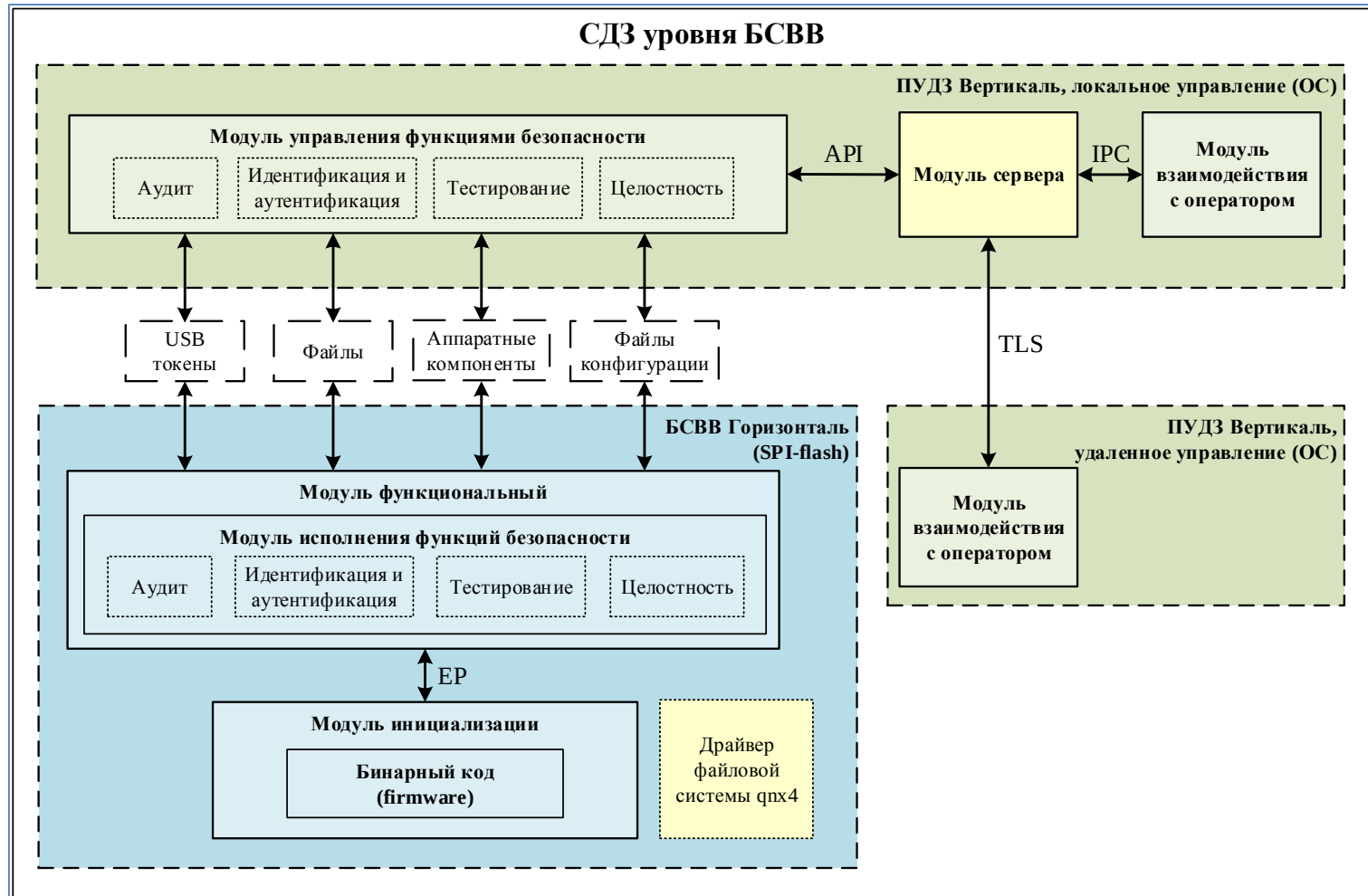
## Основные программные компоненты

- ✓ платформонезависимый модуль взаимодействия с оператором (ОС)
- ✓ платформонезависимый модуль сервера (ОС)
- ✓ платформонезависимый модуль управления функциями безопасности СДЗ (ОС)
- ✓ платформозависимый заимствованный бинарный код (БСВВ)
- ✓ платформозависимый модуль инициализации (БСВВ)
- ✓ платформонезависимый модуль функциональный с функциями СДЗ (БСВВ)
- ✓ драйверы токенов, файлов, аппаратных компонентов, сетевого взаимодействия

## Функциональная модель

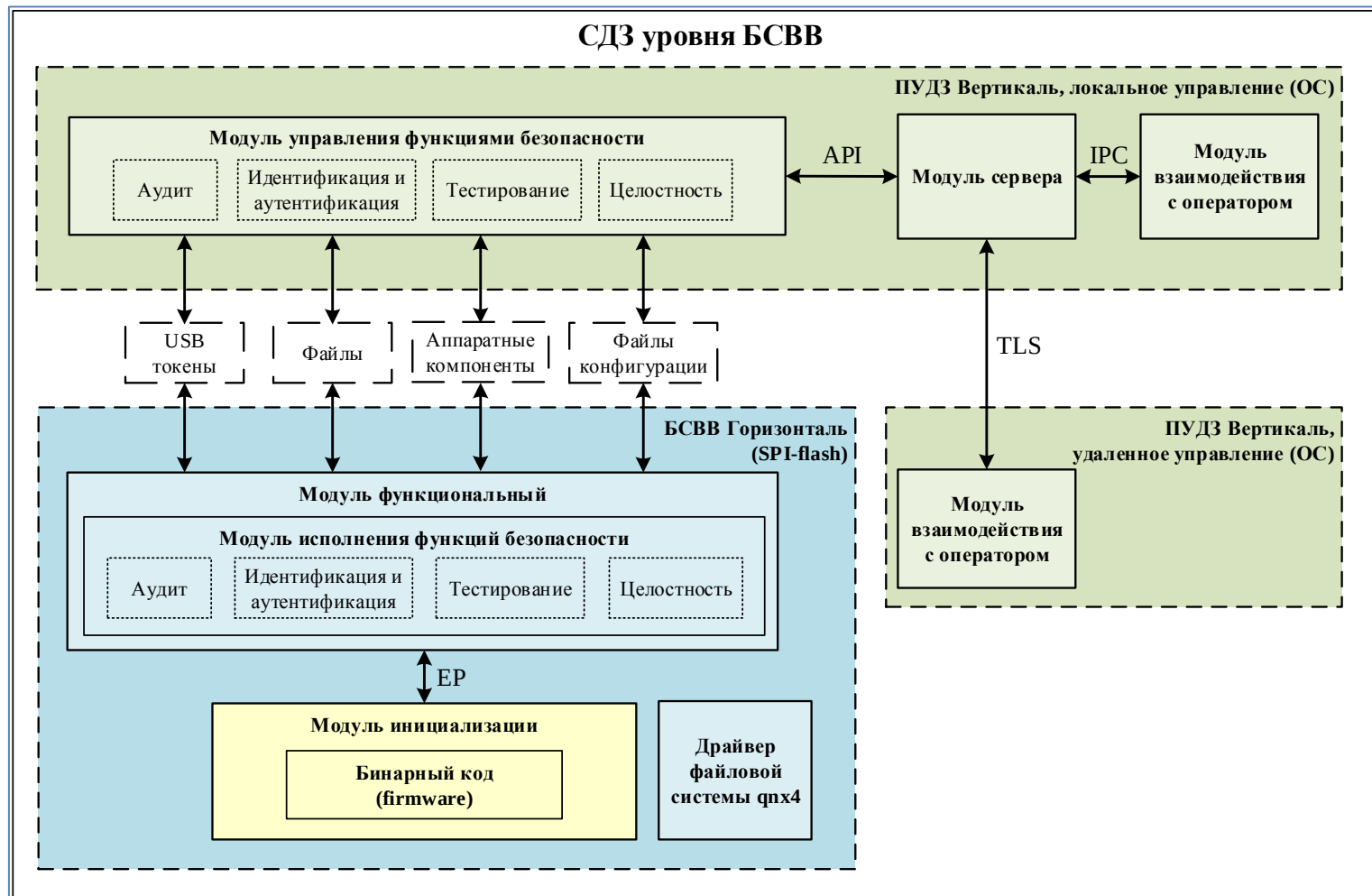


# Технические предложения по реализации средства доверенной загрузки для операционных систем семейства КПАД

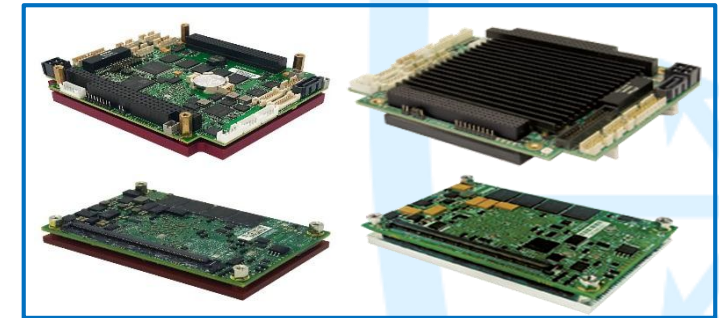


Для обеспечения возможности поддержки доверенной загрузки ОС семейства КПАД требуется только реализация в БСВВ Горизонталь драйвера для работы с файловой системой qnx4 и проведение адаптации (портирования) ПУДЗ Вертикаль под ОС семейства КПАД

# Перспективы развития средства доверенной загрузки уровня базовой систем ввода-вывода



Аппаратно-программные платформы  
Intel Atom Baytrail E38xx



Современные  
аппаратно-программные платформы



Для обеспечения возможности поддержки современных аппаратно-программных платформ требуется только реализация в БСВВ Горизонталь модуля инициализации аппаратного обеспечения целевой платформы

# Область применения продуктов семейства Горизонт

## Загрузчик операционных систем Горизонт ЦИАТ.00169-02

- ☐ Серийное изделие
- ☐ Реализованы некоторые функции средства доверенной загрузки
- ☐ Получен сертификат соответствия требованиям по безопасности информации Минобороны России

## Средство доверенной загрузки Горизонт ЦИАТ.00185-01

- ☐ Серийное изделие
- ☐ Реализованы все функции средства доверенной загрузки
- ☐ Проводятся сертификационные испытания в системе сертификации Минобороны России

## Блоки вычислительные БВ002-01 и БВ002-02



## Специализированные изделия и специальная техника





## Контактные данные

Ознакомиться с функциями ПУДЗ Вертикаль можно на любой аппаратной платформе с процессором архитектуры x86 и установленной ОС CN Astra Linux Special Edition РУСБ.10015-01 (версия 1.7.3 или 1.7.5) без установки БСВВ Горизонталь.

В случае заинтересованности в адаптации СДЗ Горизонт под другие аппаратные платформы ПФ АО «НТЦ «Атлас» готов рассмотреть возможность и предоставить информацию по стоимости и срокам выполнения работ.

☐ Ссылка для скачивания: [www.atlas-pf.ru/download/sdz\\_gorizont.zip](http://www.atlas-pf.ru/download/sdz_gorizont.zip)

☐ Контактные данные:

☐ Главный конструктор: [Боровиков Алексей Юрьевич](#)

☐ Телефон: [8\(8412\)47-77-05](#)

☐ Email: [atlaswest@mail.ru](mailto:atlaswest@mail.ru)

☐ Научный сотрудник ПФ АО «НТЦ «Атлас»: [Карпов Артем Павлович](#)

☐ Телефон: [8\(8412\)64-38-43](#)

☐ Email: [atlaswest@mail.ru](mailto:atlaswest@mail.ru)