

ПЛАТФОРМЕННЫЕ РЕШЕНИЯ ОКБ САПР



Содержание вебинара

1. Обзор платформенных решений ОКБ САПР

Докладчик: Каннер Татьяна Михайловна

руководитель учебного центра ОКБ САПР, преподаватель курсов переподготовки и пов. квалификации ЦДПО МФТИ

2. Особенности применения платформенных решений ОКБ САПР и опыт их внедрения в АС различной конфигурации

Докладчик: Мищенко Михаил Георгиевич

заместитель начальника отдела продаж ОКБ САПР

Специальный гость вебинара:

Батраков Антон Юрьевич

начальник отдела инновационных разработок ОКБ САПР

Обзор платформенных решений ОКБ САПР



Докладчик: Каннер Татьяна Михайловна

руководитель учебного центра ОКБ САПР,
преподаватель курсов переподготовки и пов.
квалификации ЦДПО МФТИ

СЗИ НСД «Аккорд-АМДЗ»: аппаратура

Накопленный опыт позволяет выполнять Аккорд-АМДЗ в любом необходимом форм-факторе для установки в любые средства вычислительной техники (СВТ): серверы, десктопы, ноутбуки, планшеты.

Работа по поддержке новых интерфейсов ведется постоянно.

Аккорды

Инафы

Аккорд-GX



PCI-express

Аккорд-GXMH



miniPCI-express
half size

Аккорд-GXM.2



m.2



USB



USB
стырьковый



USB стырьковый
с «коленом» под прямым углом

СЗИ НСД «Аккорд-АМДЗ»: средство доверенной загрузки

Высокая адаптивность и гибкость Аккорда-АМДЗ обусловлена несколькими факторами:

- большие аппаратные ресурсы;
- использование гибкой ОС;
- собственные системы прерываний и DMA.

Это позволяет реализовать на Аккорд-АМДЗ самые разные решения, используя его как источник

- доверенного BIOS;
- доверенной ОС;
- доверенного функционального программного обеспечения.

СЗИ НСД «Аккорд-АМДЗ»

Сертификат ФСТЭК России

Соответствует требованиям документов:

- ✓ «Требования к СДЗ» - по **2 уровню доверия**
- ✓ «Профиль защиты СДЗ уровня платы расширения **второго класса защиты**. ИТ.СДЗ.ПР2.ПЗ»

Сертификат ФСБ России

Соответствует требованиям к АПМДЗ ЭВМ **класса 1Б** и может использоваться для защиты от НСД к информации, содержащей/не содержащей сведений, составляющих государственную тайну.

**СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.018V00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4299

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 23 сентября 2020 г.

Выдан: 23 сентября 2020 г.
Действителен до: 23 сентября 2025 г.

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ», разработанный и произведенный ЗАО «ОКБ САПР» в соответствии с техническими условиями ТУ 26.20.40.140-079-3722406-2015, является средством доверительной загрузки, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия и средства технической защиты информации и средства обеспечения безопасности информационных технологий» (ФСТЭК России, 2016) - по 2 уровню доверия, «Требования к средствам доверительной загрузки» (ФСТЭК России, 2013), «Профиль защиты средств доверительной загрузки уровня платы расширения второго класса защиты. ИТ.СДЗ.ПР2.ПЗ» (ФСТЭК России, 2013) при выполнении указанных по записям в формуляре 37222406.26.20.40.140.079.30.

Сертификат выдан на основании технического заключения от 24.08.2020, оформленного по результатам сертификационных испытаний испытательной лабораторией ЗАО «НПТ «БИТ» (аттестат аккредитации от 22.05.2017 № СЗН RU.0001.018V00.0020), и испытательного заключения от 28.08.2020, оформленного органом по сертификации ФАУ «НИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗН RU.0001.018V00.A002).

Заявитель: ЗАО «ОКБ САПР»
Адрес: 115114, г. Москва, 2-й Кожовский переулок, д. 12, эт. 2, пом. I, ком. 21
Телефон: (495) 994-7262

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ


В. Любимов

Печать: Печать сертификата выдана, внесенной в государственный реестр системы сертификации в области (область) информационной безопасности при выполнении условий и в государственном реестре средств защиты информации по требованиям безопасности информации

**ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ 527-3214** от **10 октября** 2017 г.
Действителен до **30 апреля** 2022 г.

Выдан закрытому акционерному обществу «Особое конструкторское бюро систем автоматизированного проектирования».

Настоящий сертификат удостоверяет, что изделие «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ» (исполнение GX, GXM2, GXM1)

соответствует требованиям «ФСБ России к аппаратно-программным модулям доверительной загрузки ЭВМ класса 1Б и может использоваться для защиты от несанкционированного доступа к информации, содержащей/исключающей сведения, составляющих государственную тайну».

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «Центр сертификационных исследований» сертификационных испытаний образцов продукции №№ 935А-000501, 935В-000501, 935С-000501.

Безопасность информации обеспечивается при использовании изделия, изготовленного в соответствии с техническими условиями ТУ 012.054.1143105.2013, и выполнении требований дискуссионной документации согласно формуляру 11443195.4012.054.Ф0.

Временно исполняющий обязанности
начальника Центра защиты информации
и специальной связи ФСБ России


А.М. Шойков

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.
Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России


А.В. Парфенов

МДЗ «Аккорд-МКТ»

программный продукт (СПО), предназначенный для встраивания в BIOS МК Новой гарвардской архитектуры и ЭВМ на базе процессоров с архитектурой x86_64 и обеспечения выполнения основных функций его защиты от НСД, в том числе настройки, контроля функционирования и управления защитными механизмами.

Сертификат ФСТЭК России

Соответствует требованиям документов:

- ✓ «Требования к СДЗ» - по **2 уровню доверия**
- ✓ «Профиль защиты СДЗ уровня базовой системы ввода-вывода **второго класса защиты.** ИТ.СДЗ.УБ2.ПЗ»

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01Б1900

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4286

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации
13 августа 2020 г.

Выдан: 13 августа 2020 г.
Действителен до: 13 августа 2025 г.

Настоящий сертификат удостоверяет, что модуль доверенной загрузки «Аккорд-МКТ», разработанный и производимый ЗАО «ОКБ САПР» в соответствии с техническими условиями ТУ 26.20.40.140.082-37222406-2019, является средством доверенной загрузки, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - по 2 уровню доверия, «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указанных по эксплуатации, приведенных в формуляре 37222406.26.20.40.140.082 ФО.

Сертификат выдан на основании технического заключения от 19.05.2020, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «НИИ-СПЕКТЕСТ» (аттестат аккредитации от 22.12.2017 № СИИ RU.0001.01Б1900.0026), и экспертного заключения от 13.07.2020, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СИИ RU.0001.01Б1900.A001).

Заявитель: ЗАО «ОКБ САПР»
Адрес: 115114, г. Москва, 2-й Кожевинский переулок, д. 12, эт. 2, пом. I, ком. 21
Телефон: (495) 994-7262

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ


В.Лютиков

ПАК СЗИ НСД «Аккорд»

ПАК предназначены для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам:

- ✓ Аккорд-Win32 TSE (для 32-х битных ОС Windows)
- ✓ Аккорд-Win64 TSE (для 64-х битных ОС Windows)
- ✓ Аккорд-X (для 32-х битных ОС Linux)
- ✓ Аккорд-XL (для 32-х и 64-х битных ОС Linux)

СПО «Аккорд-Win64 К»

Для некоторых систем доверенная загрузка компьютера **не является необходимой для реализации**. В таких случаях использование ПАК СЗИ НСД «Аккорд» будет **избыточным**.

Следует использовать:

✓ Аккорд-Win64 К (для 32-х и 64-х битных ОС Windows), предназначенное для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам с ОС Windows.

Сертификат ФСТЭК России

Соответствует требованиям документов:

- ✓ «СВТ. Защита от НСД...» - по **5 классу** защищенности
- ✓ «Требования к средствам контроля съемных машинных носителей информации»
- ✓ «Профиль защиты средств контроля подключения съемных машинных носителей информации **четвертого класса** защиты»

и технических условий ТУ

СПО «Аккорд-Х К»

Для некоторых систем доверенная загрузка компьютера **не является необходимой для реализации**. В таких случаях использование ПАК СЗИ НСД «Аккорд» будет **избыточным**.

Следует использовать:

- ✓ Аккорд-Х К (для 32-х и 64-х битных ОС Linux), предназначенное для разграничения доступа к рабочим станциям с ОС семейства Linux.

Сертификат ФСТЭК России

Соответствует требованиям документов:

- ✓ «Классификация по уровню контроля отсутствия НДВ» - по **4 уровню контроля**,
- ✓ «СВТ. Защита от НСД...» - по **5 классу защищенности** и технических условий ТУ.

Новый взгляд на USB

USB-устройства кажутся очень простыми приборами и зарекомендовали себя как источник проблем в информационной безопасности. Наличие на рынке токенов и персональных идентификаторов в форм-факторе USB-устройств не влияет на это отношение, так как их защитный потенциал, увы, не велик. Мы изменили угол зрения и это позволило создать несколько разных линеек средств защиты с USB-интерфейсом.



Защищенный
служебный
носитель
СЕКРЕТ

Программно-
аппаратный
журнал (ПАЖ)



Идеальный
токен

Средство
обеспечения
доверенного
сеанса связи
«МАРШ!»

Мобильный
носитель
лицензий
(МНЛ)



В основе нашего подхода – оборудование USB-накопителя интеллектуальным управляющим компонентом и реализация управляемого доступа к памяти.

Защищенные флешки «Секрет»

Главная проблема защиты информации, связанная с USB-накопителями, состоит не в том, как контролировать использование флешки внутри информационной системы, и даже не в том, как защитить содержимое флешки от нелегального пользователя, а в том, как контролировать использование флешки за пределами информационной системы – именно туда утекают данные и именно оттуда приносятся вирусы.

Секрет Особого Назначения



Патент и сертификат на флешки «Секрет»



Быстрый секрет

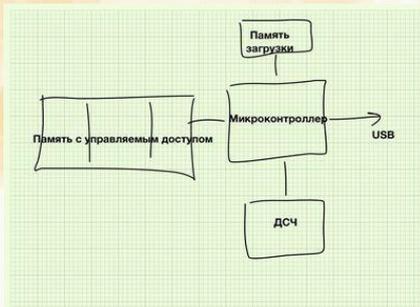
Семейство защищенных флешек «Секрет» – первое и пока единственное решение этой задачи.



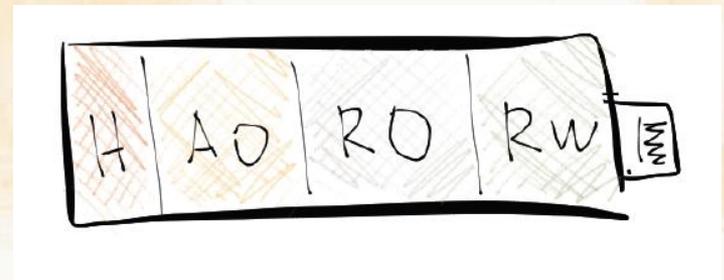
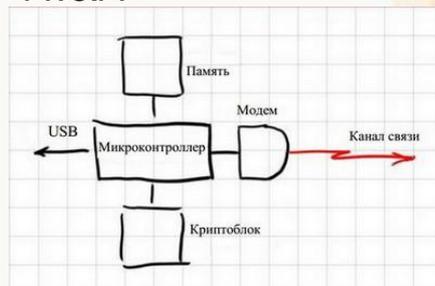
Средство обеспечения доверенного сеанса связи «МАРШ!»

МАРШ! – это флешка, диск которой разбит на разделы с разными атрибутами доступа, предназначенными для хранения разных типов данных. Доступ к памяти разграничивается процессором устройства. Главная функция – загрузка неизменной, эталонной ОС из защищенного от записи раздела: вирусный иммунитет.

СОДС«МАРШ!»



М!&М



- H – Hidden
- AO – AddOnly
- RO – ReadOnly
- RW – ReadWrite

М!&М: Это тот же МАРШ!, но в составе его аппаратной части – USB-носителя – есть модем.

Специальные USB-устройства

На основе описанных подходов по заказам различных предприятий и инициативно ОКБ САПР разрабатываются различные специальные устройства:

«Транзит» – это неперепрограммируемая флешка. То есть такая, которая может быть только USB-накопителем, и не может быть использована как канал скрытого управления компьютером или канал утечки данных, как обычные флешки, контроллер которых можно перепрограммировать.



«Мобильный носитель лицензий» (МНЛ) и **«KeyMaker»** – устройства, позволяющие генерировать данные (лицензии на ПО или криптографические ключи) в неконтролируемых владельцем условиях.

МНЛ



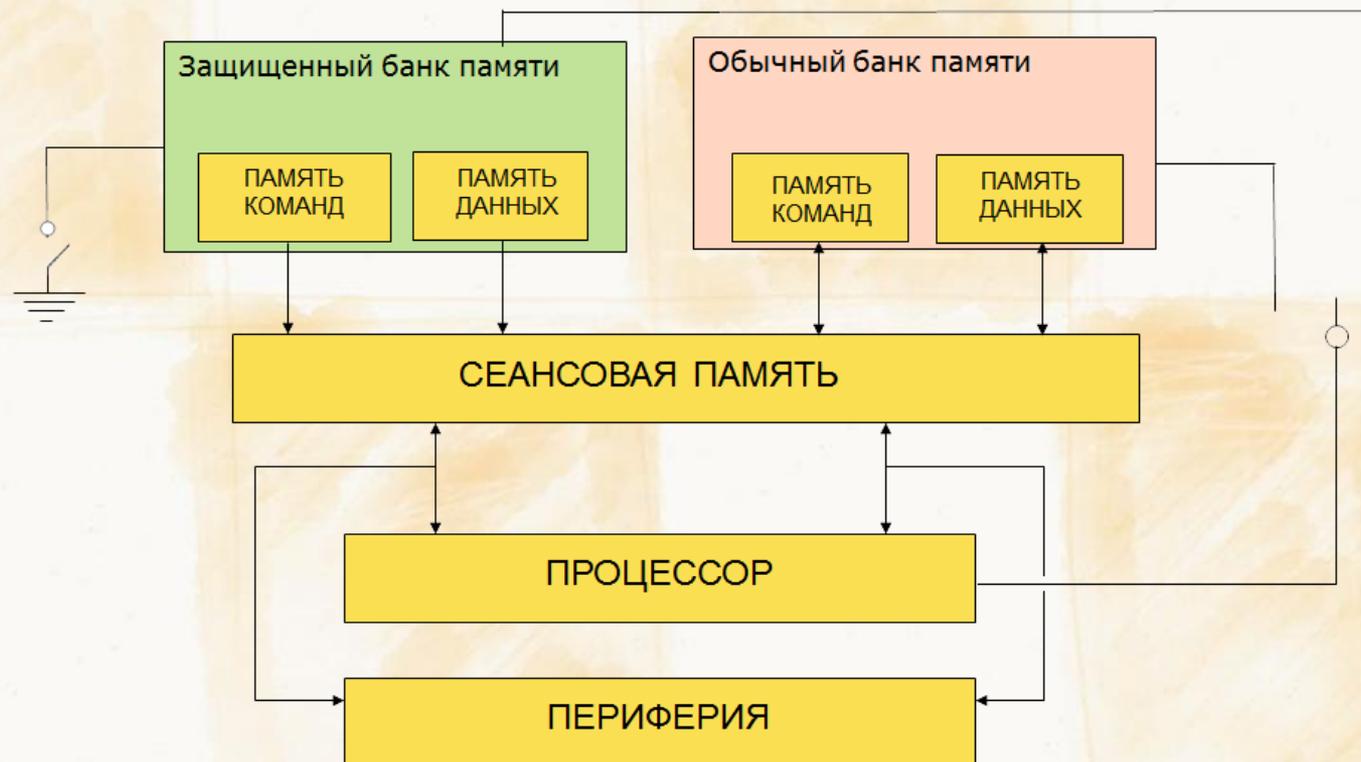
KeyMaker



Понимая возможности по управлению свойствами USB-устройств, мы можем использовать весь их потенциал для решения задач заказчика.

Новая гарвардская архитектура

Есть два пути устранения уязвимости, заложенной в архитектуру компьютера – установка в уязвимый компьютер специального устройства (такого, как Аккорд-АМД3) или изменение архитектуры и создание компьютера уже без уязвимости. Такая совершенная, не имеющая базовой уязвимости Машины Тьюринга архитектура существует – это разработанная в ОКБ САПР Новая гарвардская архитектура.



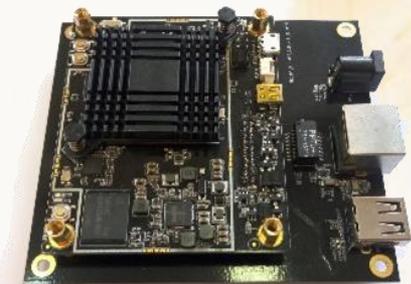
Новая гарвардская архитектура: плюсы

Новая гарвардская архитектура обеспечивает защищенность, надежность и экономичность компьютеров:

- вирусный иммунитет;
- доступная и контролируемая комплектация;
- доверенная среда для СКЗИ.

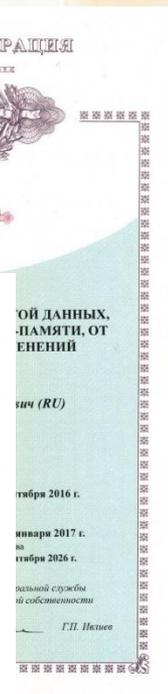


MKT-card long



m-TrusT

Небольшая часть патентов на Новую гарвардскую архитектуру



Защищенные микрокомпьютеры Новой гарвардской архитектуры: MKT-card long

MKT-card long – это микрокомпьютер, состоящий из универсальной док-станции с интерфейсами для подключения питания и периферии, а также отчуждаемого персонального микрокомпьютера.



MKT-card long

Док-станция не содержит никаких данных или средств обработки, а отчуждаемый микрокомпьютер может сдаваться на хранение, например, в пенале для ключей, а может оставаться под личную ответственность пользователя.

Защищенные микрокомпьютеры Новой гарвардской архитектуры: m-Trust

m-Trust – это промышленное решение, предназначенное для применения на объектах критических информационных инфраструктур.

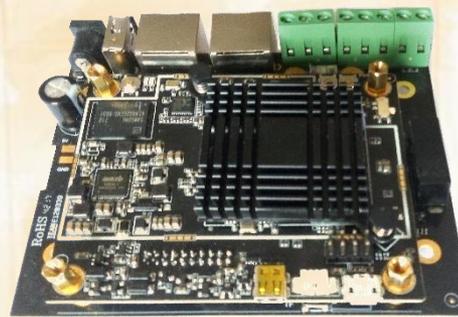


m-TrusT: универсальная платформа

Особенность аппаратного решения в том, что оно состоит из универсального ядра и интерфейсной платы, которая, без изменения ядра, изменяется под особенности оборудования на конкретном объекте КИИ.



Мезонин m-TrusT
(слева)



M-TrusT на
интерфейсных платах
(справа)



Интерфейсные платы



m-TrusT сервер

Для центральных узлов объекта выпускается исполнение в стойку. Таким образом исключаются проблемы интеграции – это одно и то же устройство в разных форм-факторах.

Специализированные компьютеры на базе решений ОКБ САПР

По мере того, как СВТ и средства защиты становятся сложнее, задача создания защищенного автоматизированного рабочего места (АРМ) из СВТ и средств защиты должна переходить от эксплуатирующей организации специалистам. ОКБ САПР выпускает защищенные АРМ на базе своих продуктов:

Двухконтурный моноблок



ПКЗ 2020



Планшет СКЗИ ready «ПКЗ 2020»

Для того чтобы на планшете можно было использовать криптографию **высокого класса (КС2 и выше)**, необходимы: и особенное СДЗ и особенный планшет.

Подобрать такую пару самостоятельно — **задача непростая и непрофильная** даже для системного интегратора.

«ПКЗ 2020» **решает данную проблему:**

реализована СФК на **класс СКЗИ КС3** (установлен «Аккорд-АМДЗ» на базе контроллера Аккорд-GXM.2, серт. ФСБ России)



Аналоги на сегодняшний день неизвестны – как целиком, так и АПМДЗ в формате М.2, соответствующего требованиям ФСБ России в части управления питанием для планшетов.

Инфраструктурные решения на базе продуктов ОКБ САПР

Задачи защиты информации уверенно смещаются от защиты отдельных рабочих мест к защите инфраструктур. На это направлены, в частности, все «двухконтурные» решения ОКБ САПР.

Однако есть и собственно инфраструктурные продукты, построенные на основе описанных технологий и подходов:

✓ **Центр-Т** – комплекс, обеспечивающий защищенное хранение и загрузку ОС на пользовательские СВТ системы удаленного доступа

✓ Комплексы средств для защиты виртуализации:

- **Аккорд-В.** и **Сегмент-В.** (для VMware),

- **Аккорд-KVM** (для KVM)

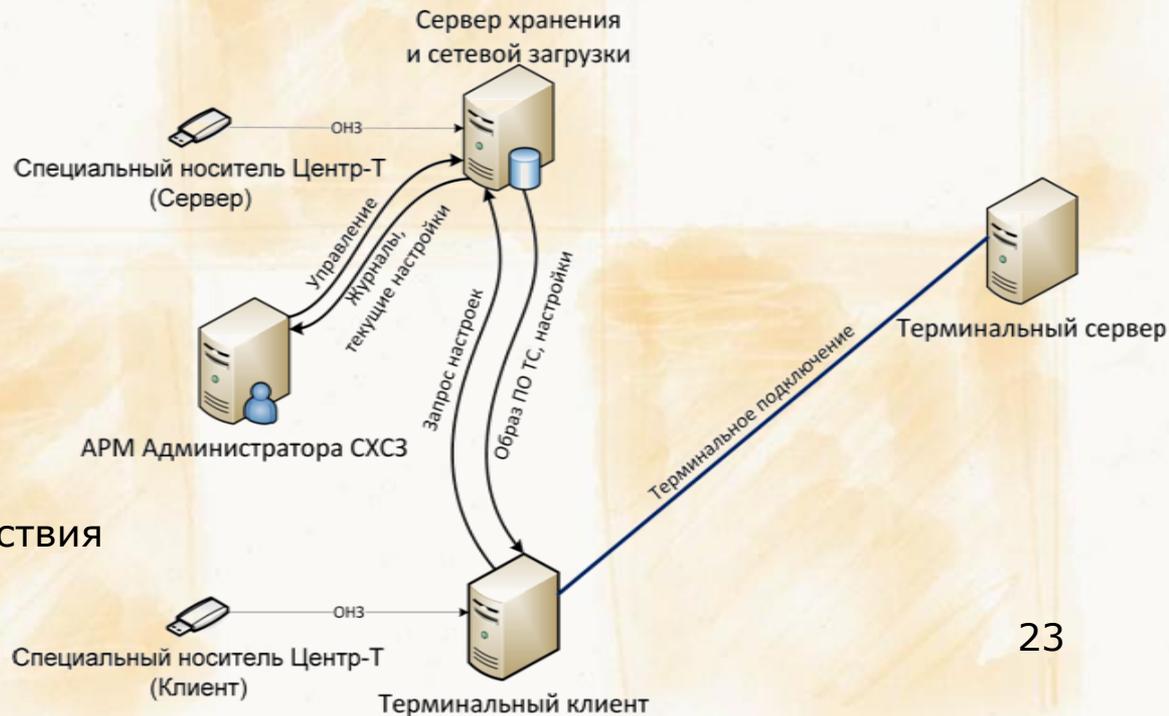
✓ **Система интеграции** СЗИ НСД со СКУД и видеонаблюдением «Рассвет»

Инфраструктурные решения

Центр-Т – комплекс, обеспечивающий защищенное хранение и загрузку ОС на пользовательские СВТ системы удаленного доступа



Структурная схема комплекса
Технических средств (сверху)
и
Схема информационного взаимодействия
(снизу)



Стажировки по продуктам

Варианты:

✓ по любым из рассмотренных продуктов или решений

✓ по существующим программам:

Раздел «Обучение – Учебный центр – Стажировки по продуктам»

<https://www.okbsapr.ru/education/education-centre/programs/>

✓ по индивидуальным программам

✓ длительность стажировки от 1 до 5 дней (при желании – дольше)

Цели стажировки:

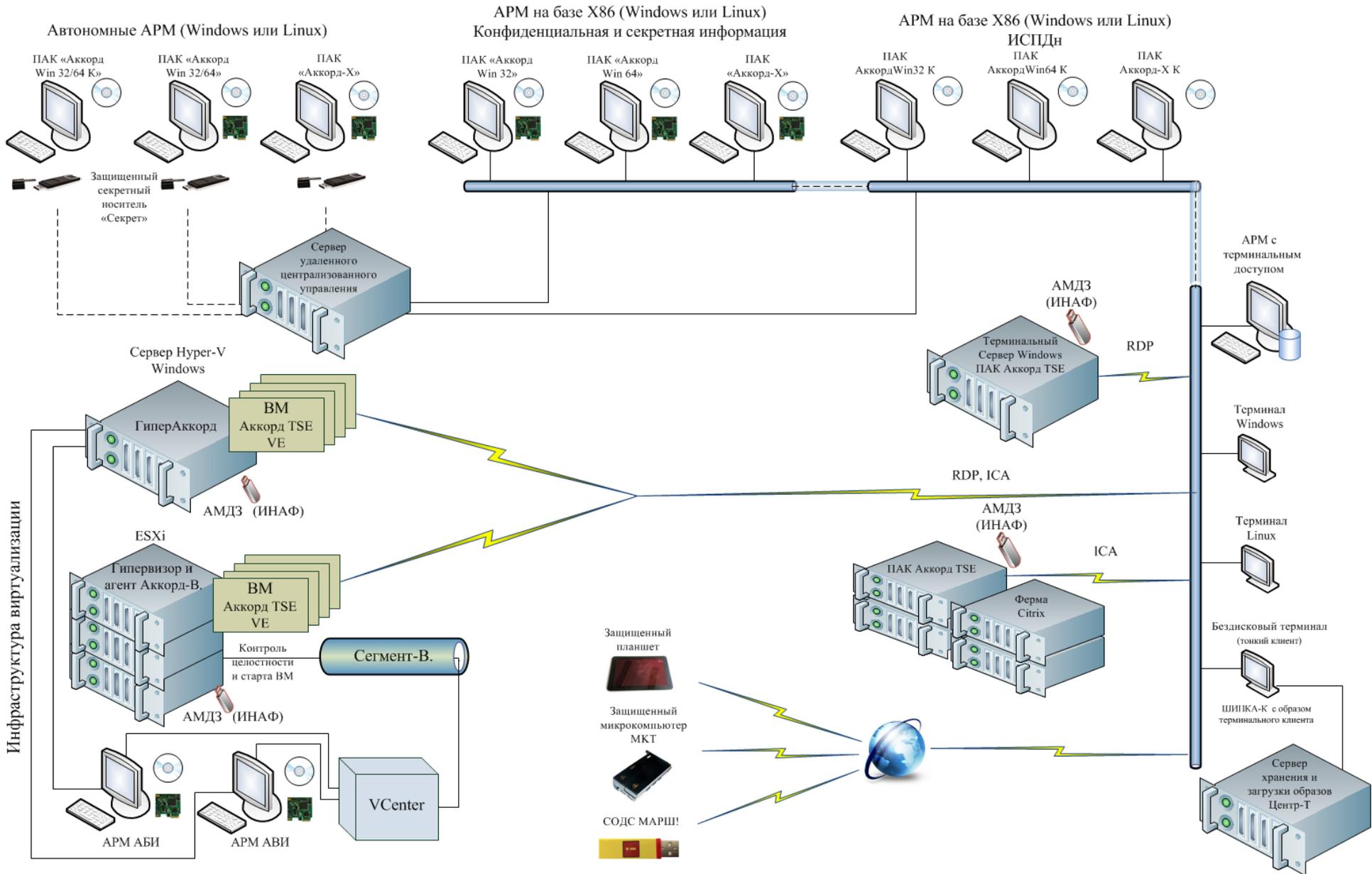
✓ углубленное изучение особенностей применения и администрирования программно-аппаратных комплексов СЗИ

✓ получение практических навыков настройки и применения СЗИ

Особенности применения платформенных решений ОКБ САПР и опыт их внедрения в АС различной конфигурации

Докладчик: Мищенко Михаил Георгиевич
заместитель начальника отдела продаж ОКБ САПР

Схема комплексной защиты информации на предприятии с использованием продуктов и решений компании «ОКБ САПР»



Вопросы?

Контакты

Отдел продаж:

Коковкин Алексей, ведущий менеджер по работе с ключевыми клиентами

е-mail: aak@okbsapr.ru

тел: 8(916)364-63-68, 8 (495)994-49-98 доб.1119

Тестенков Николай, менеджер по работе с ключевыми клиентами

е-mail: tnv@okbsapr.ru

тел: 8(915)098-07-14, 8 (495)994-49-98 доб. 1115

Учебный центр:

Каннер Татьяна, руководитель учебного центра

е-mail: tatianash@okbsapr.ru

тел: 8(926)235-14-67

СПАСИБО ЗА ВНИМАНИЕ!

