

ПЛАТФОРМЕННЫЕ РЕШЕНИЯ ОКБ САПР



Аккорд-АМДЗ и решения на его основе

Аппаратный модуль доверенной загрузки как концепцию и как вид средства защиты информации от НСД создал коллектив ОКБ САПР и уже 25 лет мы опережаем рынок в развитии продуктов этого класса на 2-3 года.

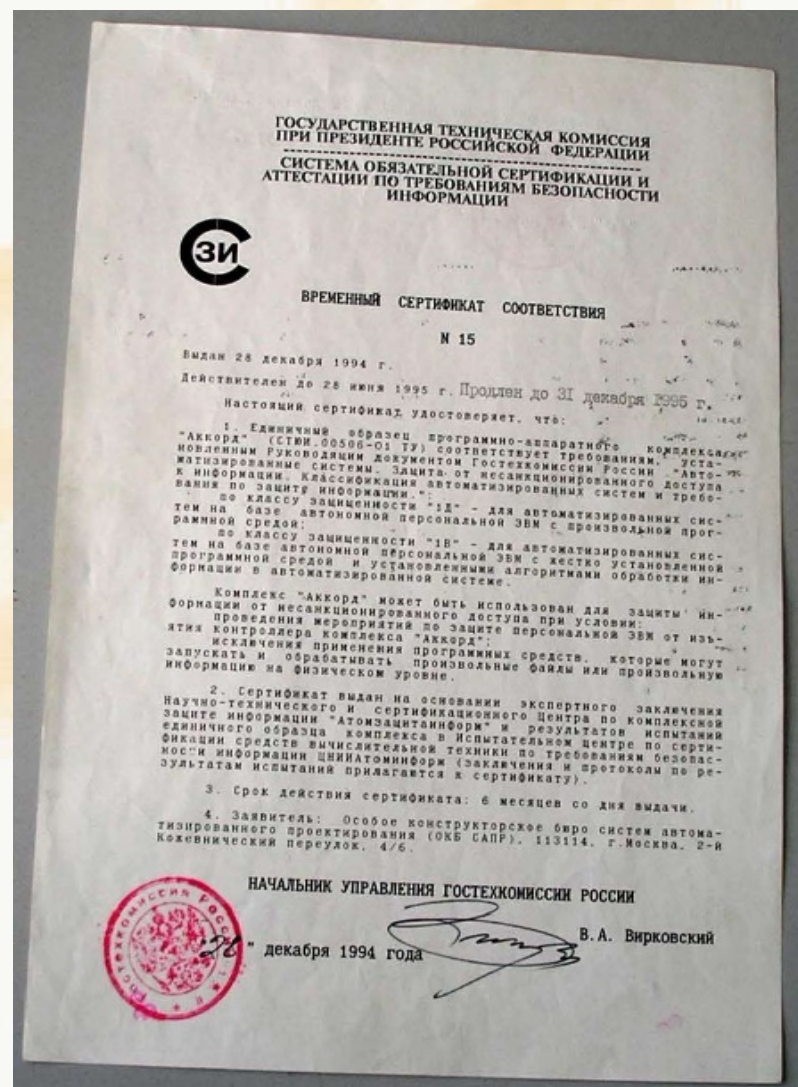


Аккорд-1



Аккорд-GXm.2

Аккорд-АМДЗ тогда (слева) и сейчас (справа), первый сертификат ФСТЭК (Гостехкомиссии) России на коммерческий продукт №15



Аккорд-АМДЗ: аппаратура

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

Работа по поддержке новых интерфейсов ведется постоянно.

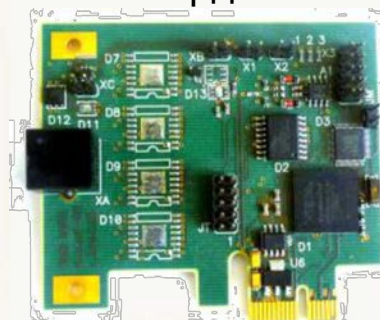
Аккорд-PC104



Слева примеры изделий с экзотическими интерфейсами – Аккорд с шиной PC104 и двухшинный Аккорд-КПД (ISA и PCI).

Справа – современные Аккорды – для шин PCI-express, miniPCI-express half size, m.2, USB штырьковый и с внешним разъемом.

Аккорд-GX

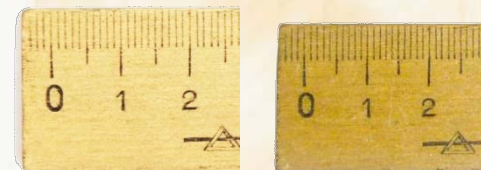


Аккорд-КПД



Инафы

Аккорд-GXMН



Аккорд-GXm.2

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 Аккорде-АМДЗ самые разные решения, используя его как источник

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

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.



Мобильный
носитель
лицензий

Защищенный
служебный
носитель
СЕКРЕТ



Средство
обеспечения
доверенного
сеанса связи
«МАРШ!»



Программно-аппаратный
журнал

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



Быстрый секрет

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



ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 4 февраля 2015 г.

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.



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

Специальные USB-устройства

На основе описанных подходов по заказам различных предприятий и инициативно ОКБ САПР разрабатываются различные специальные устройства, например, флешка «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.

Другой пример – мобильный носитель лицензий и KeyMaker – устройства, позволяющие генерировать данные (лицензии на ПО или криптографические ключи) в неконтролируемых владельцем условиях.

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



МНЛ



Идеальный токен



ПАЖ



Новая гарвардская архитектура

Есть два пути устранения уязвимости, заложенной в архитектуру компьютера – установка в уязвимый компьютер специального устройства (такого, как Аккорд-АМДЗ) 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.



TrusTPad



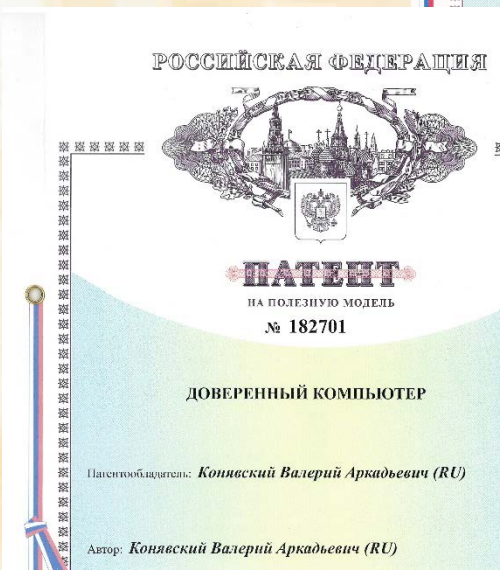
MKT-card long

Небольшая часть патентов на Новую гарвардскую архитектуру

MKT



m-TrusT



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: TrusTPad

Планшет TrusTPad позволяет совмещать на одном планшете работу в защищенной системе и использование планшета в привычных личных целях – интернет-серфинг, просмотр видео и прочее.

Смена среды – доверенной и обычной – происходит путем физического переключения переключателя на корпусе планшета, который управляет тем, на какой банк памяти подается питание.

Это невозможно сделать с помощью хакерской атаки или вируса.



TrusTPad

Защищенные микрокомпьютеры Новой гарвардской архитектуры: m-Trust

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

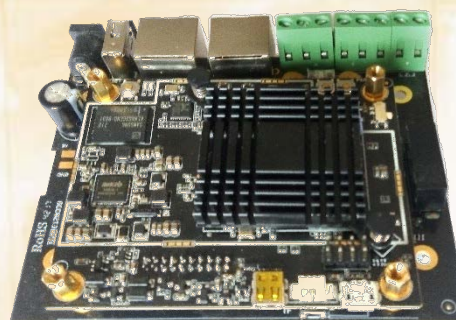


m-Trust: универсальная платформа

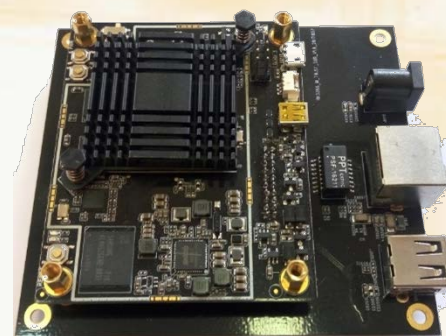
Особенность аппаратного решения в том, что оно состоит из универсального ядра и интерфейсной платы, которая, без изменения ядра, изменяется под особенности оборудования на конкретном объекте КИИ.



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:



Слева направо:
двухконтурный моноблок,
Ноутбук Руководителя,
планшет с СДЗ уровня платы расширения,
Компьютер с защитой от Intel Management Engine (IntelME, IME);



Инфраструктурные решения на базе продуктов ОКБ САПР

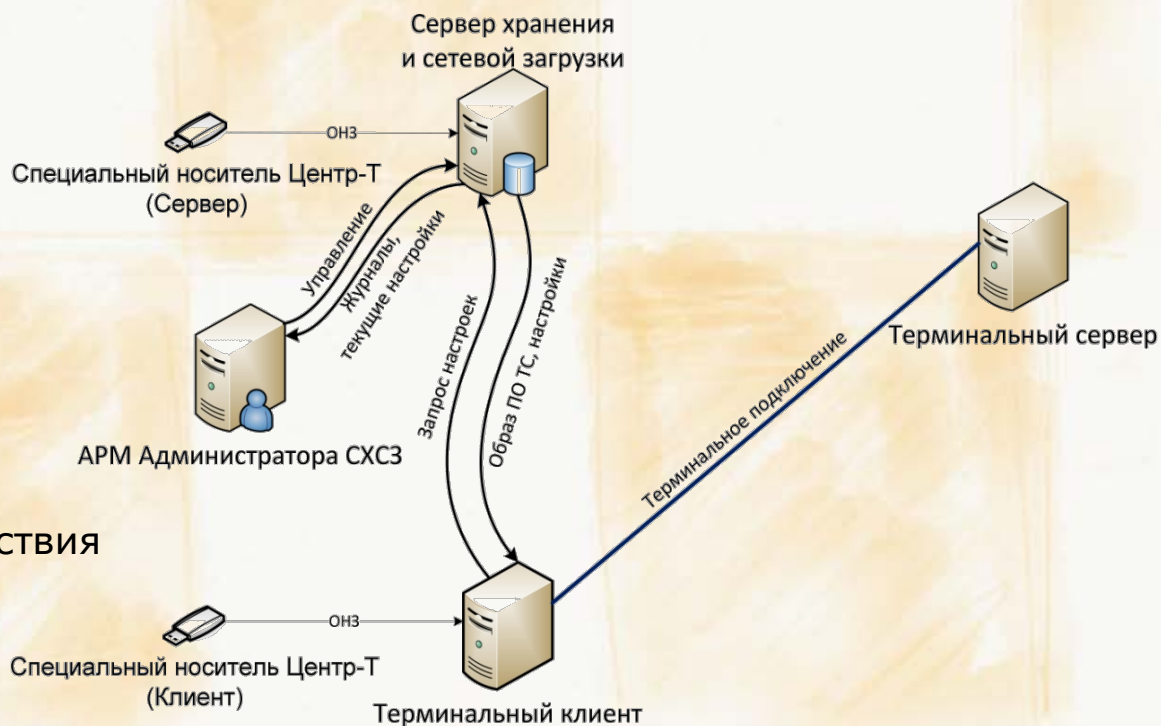
Задачи защиты информации уверенно смещаются от защиты отдельных рабочих мест к защите инфраструктур. На это направлены, в частности, все «двухконтурные» решения ОКБ САПР.

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), ГиперАккорд (для Hyper-V)
- 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



Инфраструктурные решения

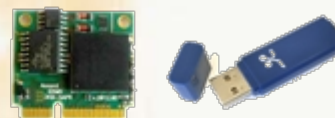
Комплексы средств для защиты виртуализации – Аккорд-В. и Сегмент-В. (для VMware), Аккорд-KVM (для KVM), ГиперАккорд (для Hyper-V)

Этапы работы виртуальной инфраструктуры



Работа СЗИ

Аккорд-АМД3
ИНАФ



Windows: Аккорд-Win32/64 (TSE)
Linux: Аккорд-X/XL



VMware vSphere: Сегмент-В.



ESXi: Аккорд-В.
KVM: Аккорд-KVM
Hyper-V: Гипер-Аккорд

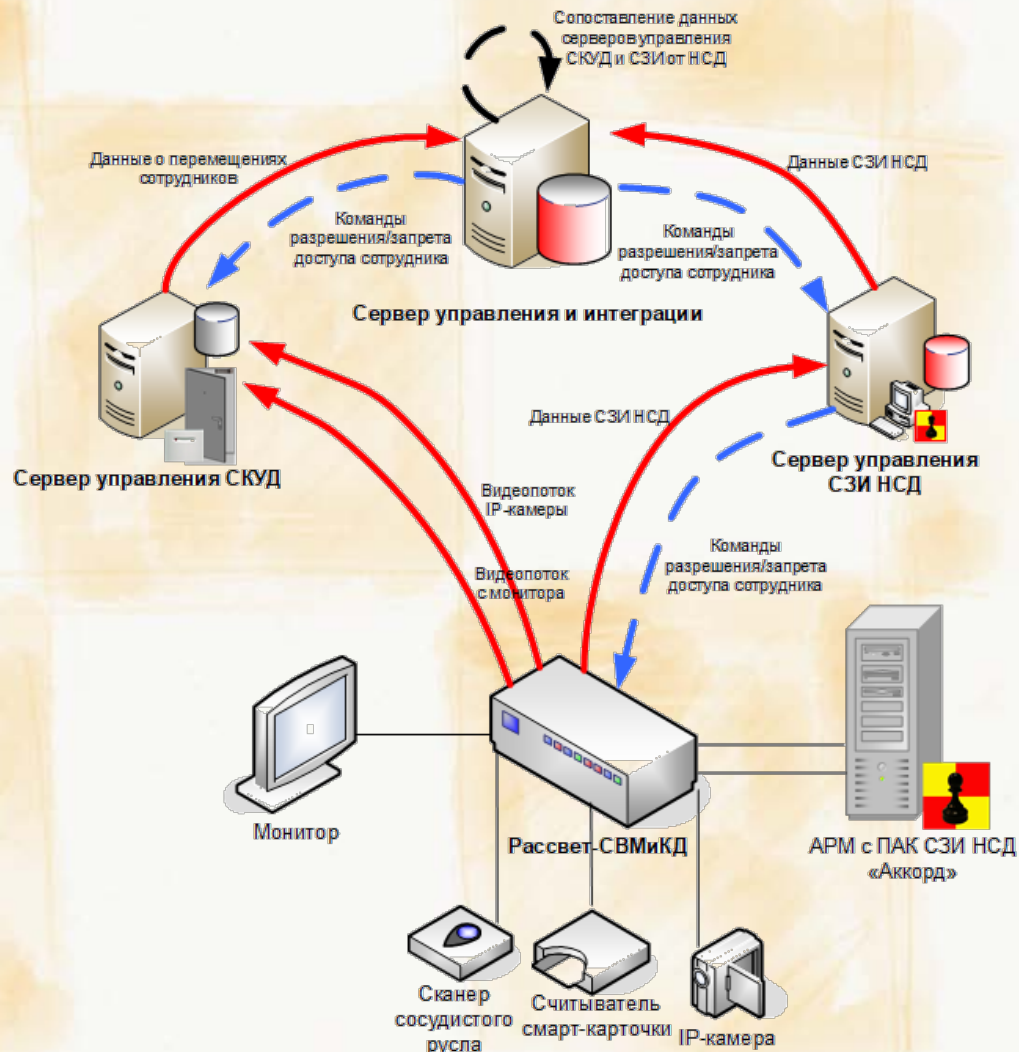
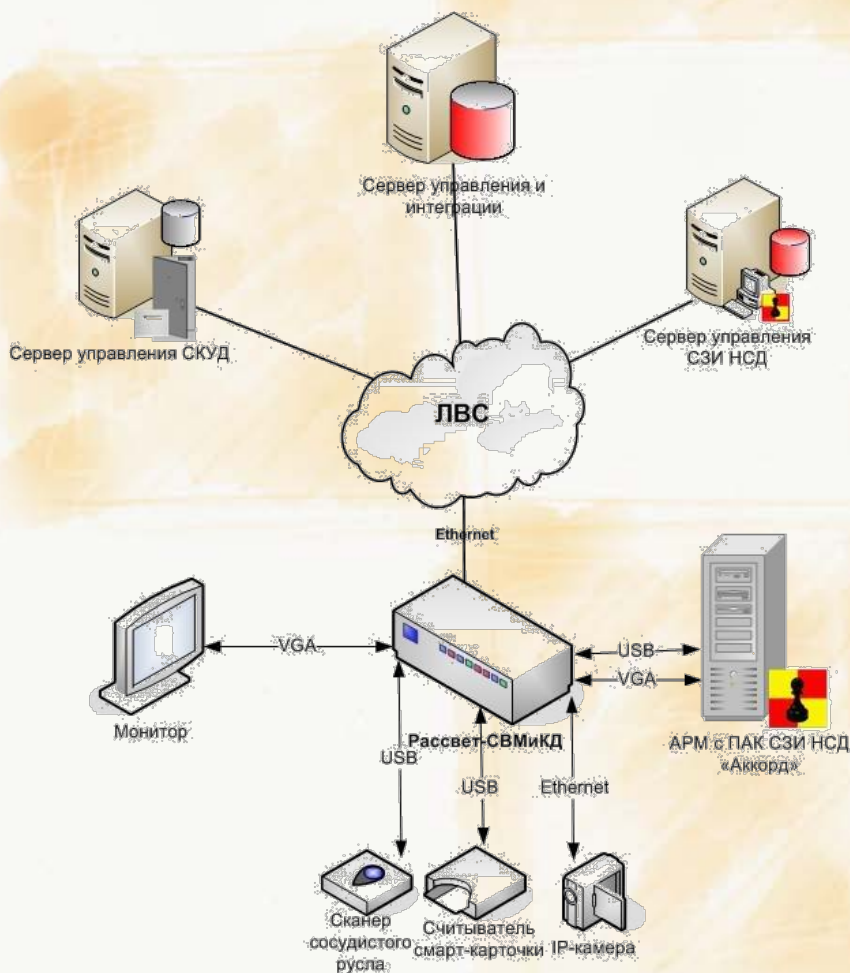


Windows: Аккорд-Win32/64 VE (TSE)
Linux: Аккорд-X/XL VE



Инфраструктурные решения

Система интеграции СЗИ НСД со СКУД и видеонаблюдением «Рассвет» (структурная схема (слева) и схема информационных потоков (справа)).



СПАСИБО ЗА ВНИМАНИЕ!

