ОКБ САПР

www.okbsapr.ru
okbsapr@okbsapr.ru

Почему защита должна быть аппаратной?

Как обеспечить целостность программы, обеспечивающей целостность?

Еще одной программой?

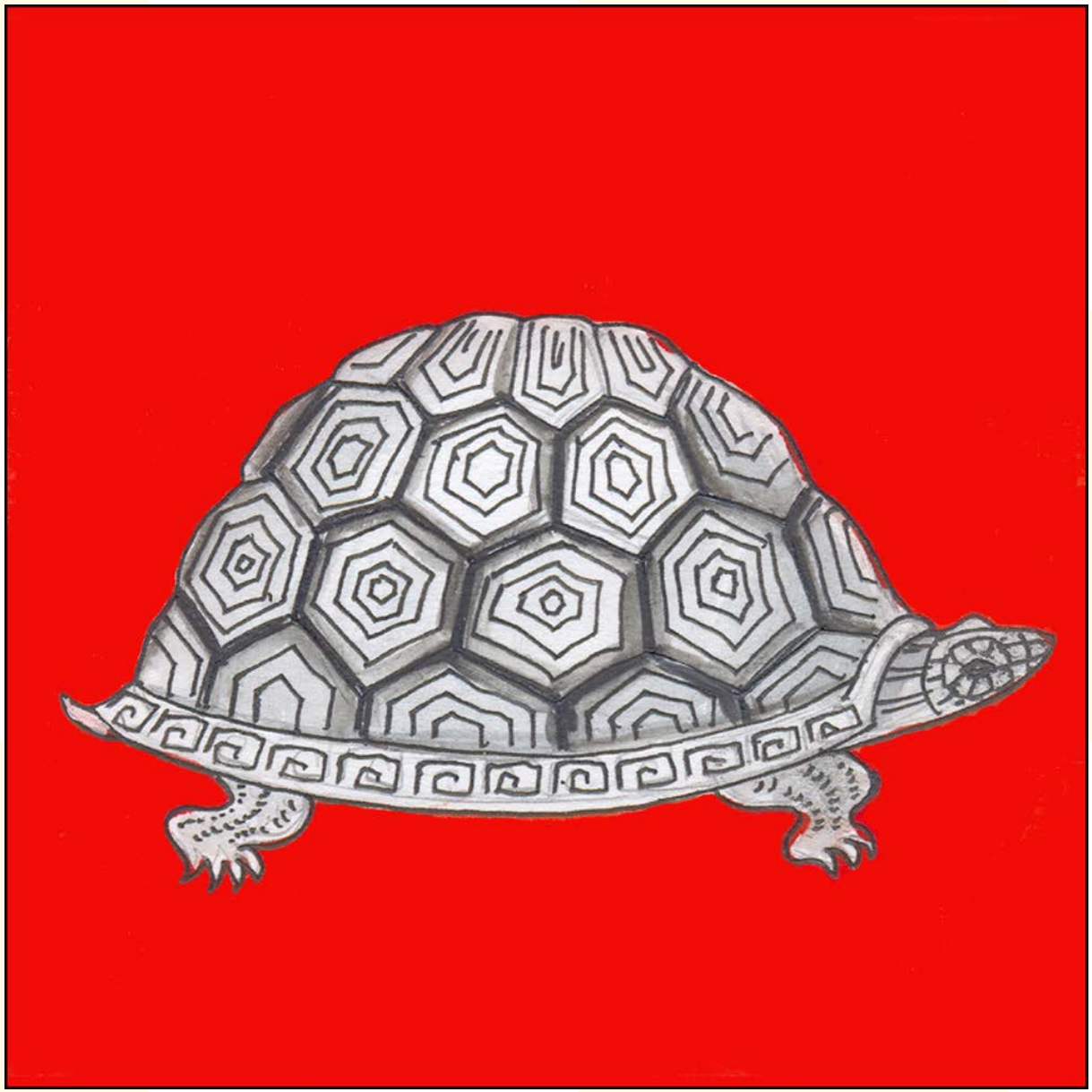
А ее целостность?

Еще…

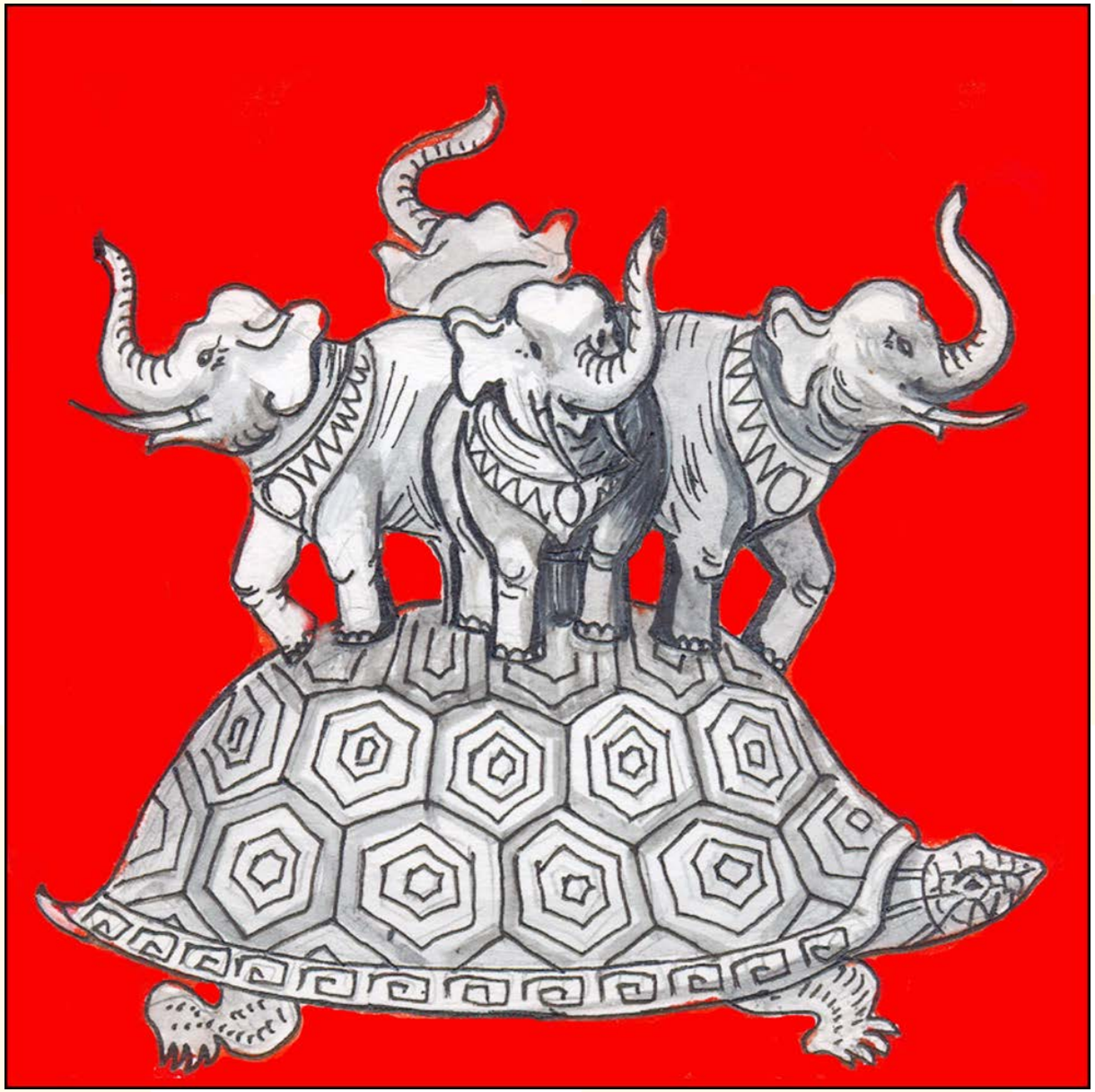
Каким должно быть средство защиты от НСД?

- ✓ **независимым** от операционной и файловой системы ПК
- ✓ **недоступным** для внесения изменений
- ✓ **аппаратным.**

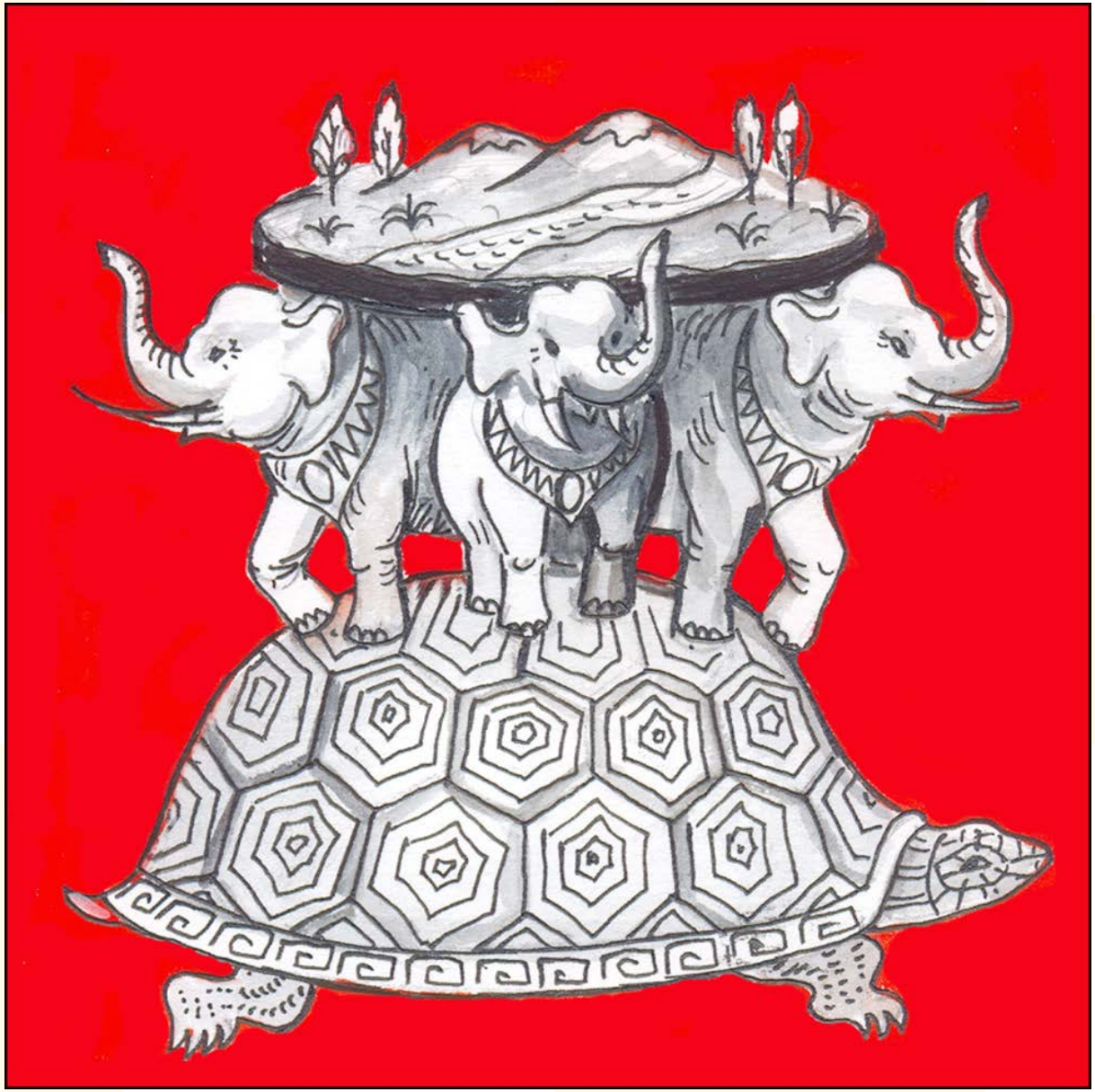
Базис: доверенная загрузка



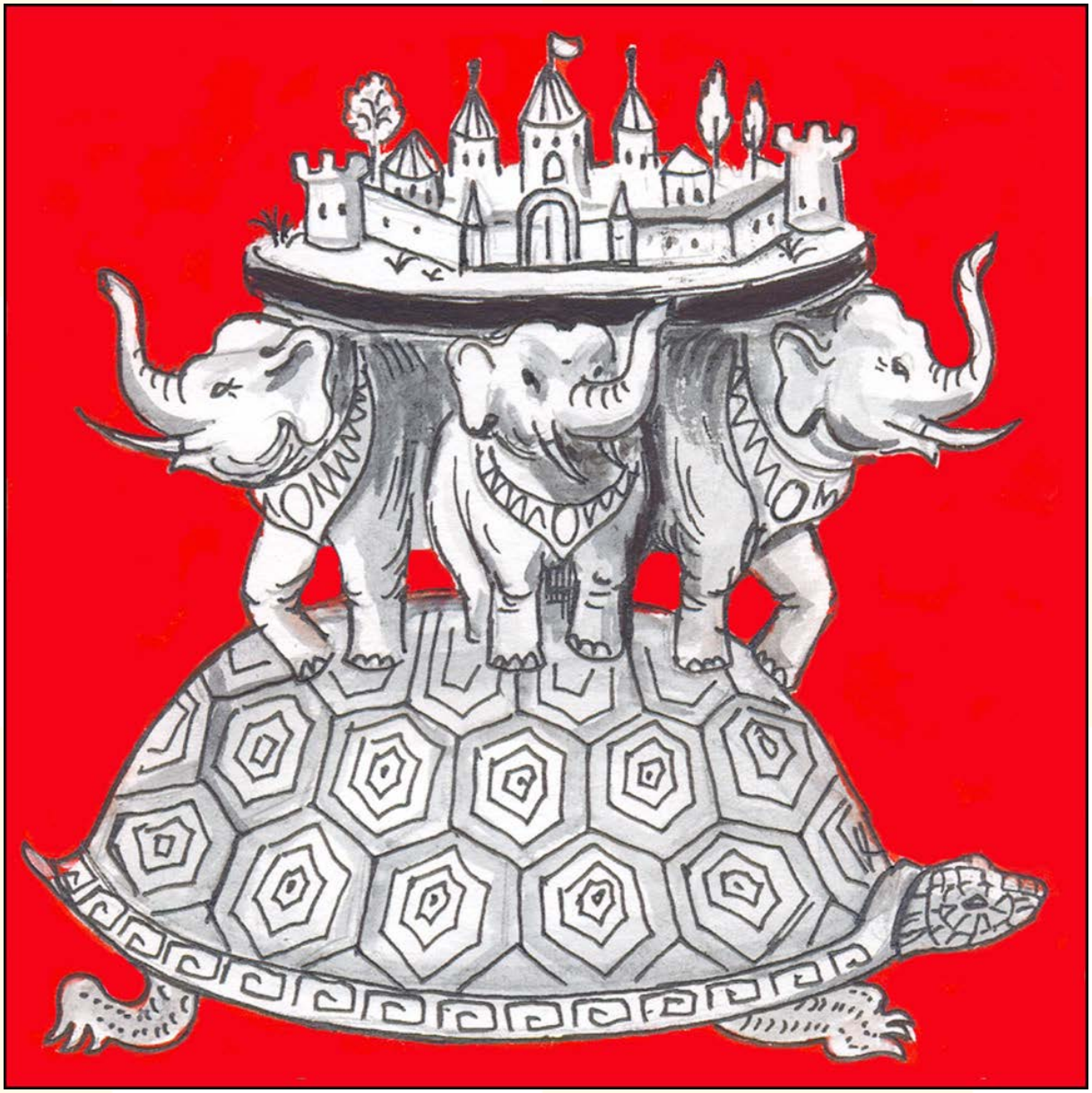
Надстройка: доверенная среда



Надстройка: доверенная система



Надстройка: доверенная инфраструктура



Надстройка: доверенная инфраструктура виртуализации

СЗИ от НСД

Стационарные

На базе контроллеров АМДЗ семейства Аккорд

Мобильные

На базе контроллеров АМДЗ семейства Инаф

СКЗИ

Стационарные

Аккорд-У КВ2, Аккорд-У КС3

Мобильные

ПСКЗИ ШИПКА, ПАК Privacy

Инфраструктурные решения

Стационарные

Аккорд-В., Аккорд-РАУ, СУЦУ

Мобильные

ПАК «Центр-Т», СОДС «МАРШ!»

Защищенные служебные носители

СЕКРЕТ

Для применения на автономных ПК и в ЛВС

АККОРД

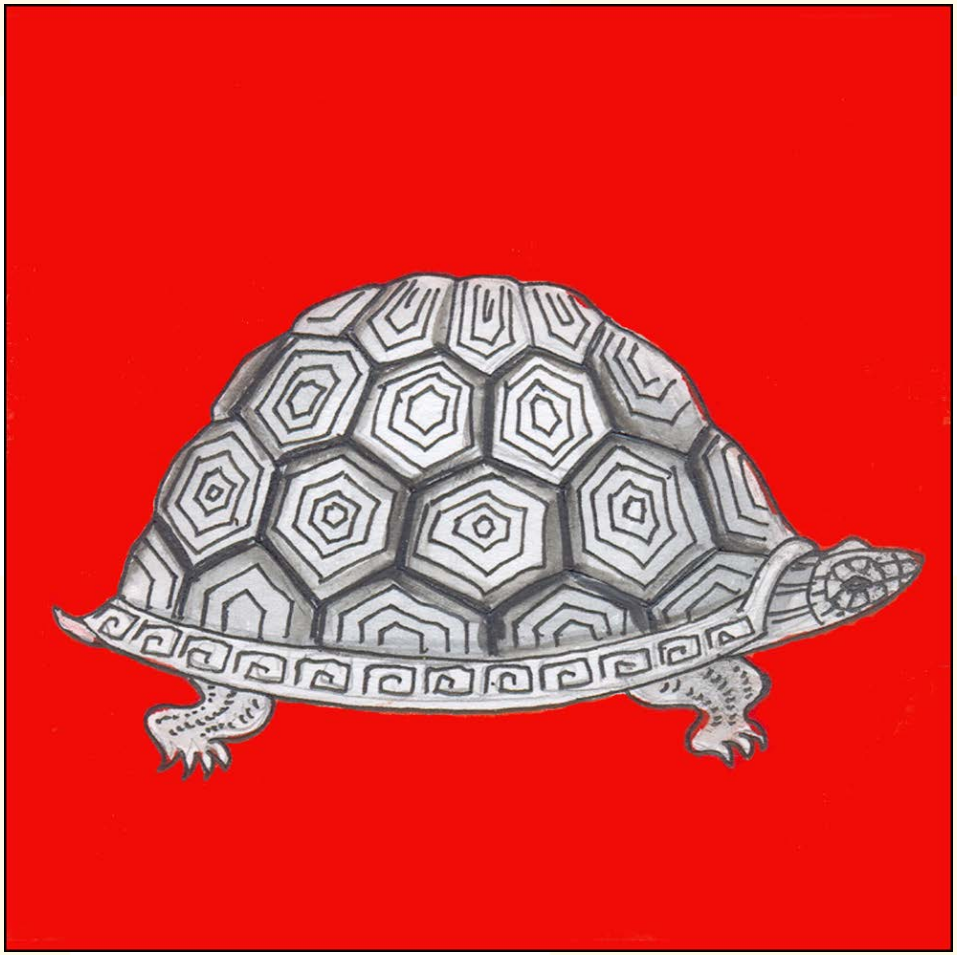
Защищенность компьютера от НСД

достигается обеспечением режима доверенной загрузки ОС, при котором подтверждено, что:

пользователь **именно тот**, который имеет право работать на данном компьютере;

компьютер **именно тот**, на котором имеет право работать данный пользователь.

Аккорд-АМДЗ. Доверенная загрузка



Доверенная загрузка

Загрузка ОС производится только **после** успешного завершения процедур:

- ✓ блокировка загрузки ОС с внешних носителей информации;
- ✓ проверка целостности технических и программных средств ПК с использованием алгоритма пошагового контроля целостности;
- ✓ идентификация/аутентификация пользователя.

Надежность в ненадежном мире:

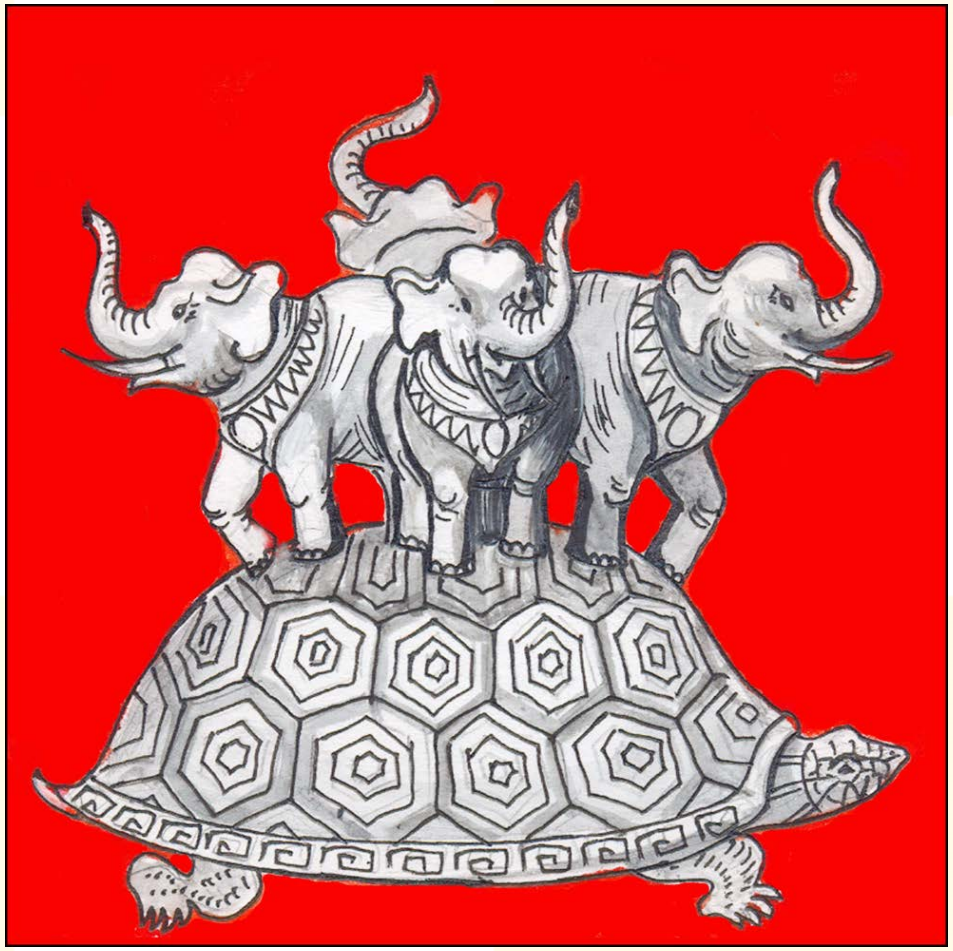
Архитектура Аккорд-АМДЗ обеспечивает

невозможность внесения изменений в firmware;

невозможность сокрытия попытки НСД от администратора безопасности информации;

возможность построения систем защиты информации на базе Аккорд-АМДЗ.

Разграничение доступа к данным



Разграничение доступа к данным

обеспечивают программно-аппаратные комплексы на базе Аккорд-АМДЗ и специального ПО

Аккорд-Win32, Аккорд-Win64 – для операционных систем семейства Windows;

Аккорд-X – для операционных систем **Linux**

ПАК Аккорд

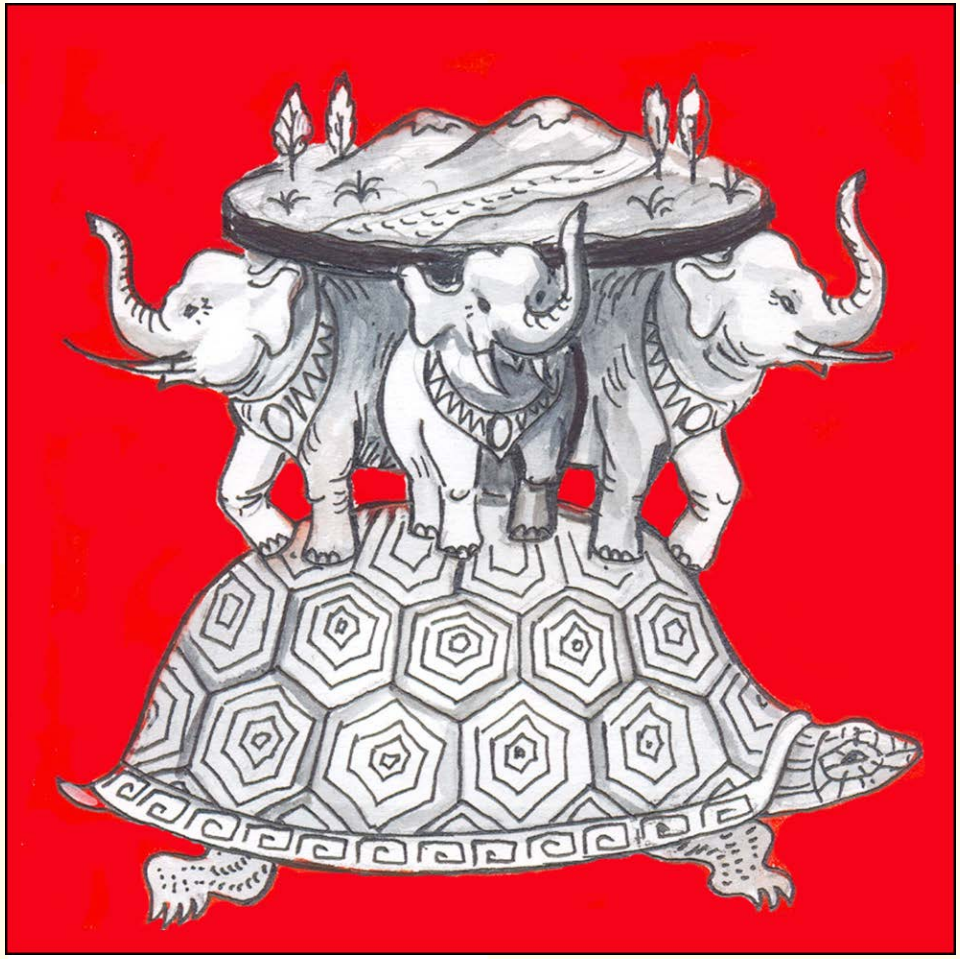
проводит процедуры идентификации/аутентификации пользователей (как локальных, так и удаленных);

обеспечивает изолированную программную среду;

проводит взаимную проверку подлинности взаимодействующих технических средств;

содержит собственный монитор разграничения доступа (мандатный и дискреционный механизмы).

Защищенность терминальных решений



Защищенность терминальных решений

достигается обеспечением режима взаимодействия, при котором подтверждено, что

пользователь работает **только с защищенным** терминальным сервером;

с терминальным сервером работает пользователь **только с защищенного** «тонкого клиента».

Компоненты ПАК Аккорд TSE

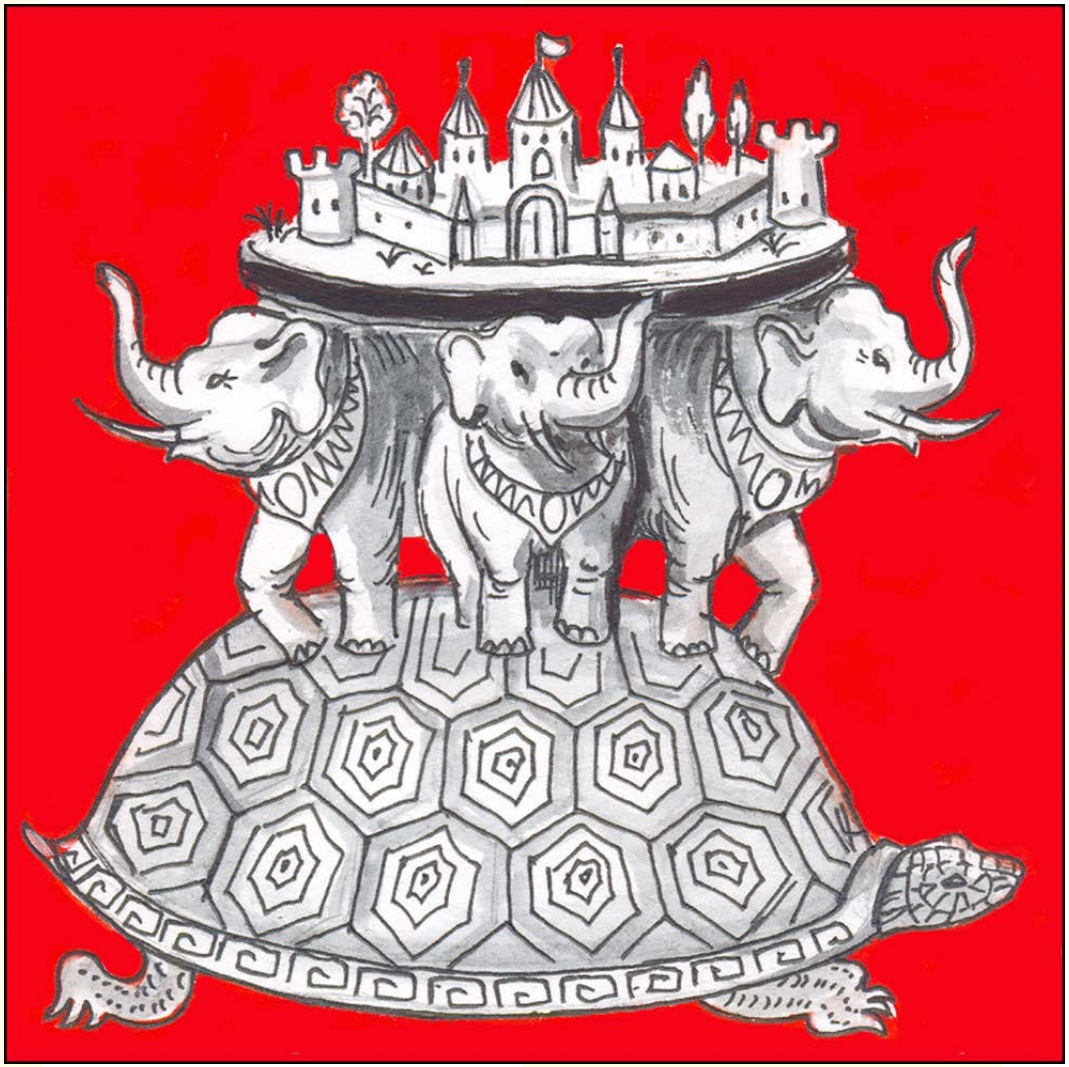
установленные на терминальных серверах и пользовательских терминалах взаимодействуют в рамках виртуальных каналов, построенных на протоколах:

RDP и

ICA,

что позволяет использовать для взаимодействия СЗИ **уже установленный канал**, а не организовывать новый.

Защищенная инфраструктура

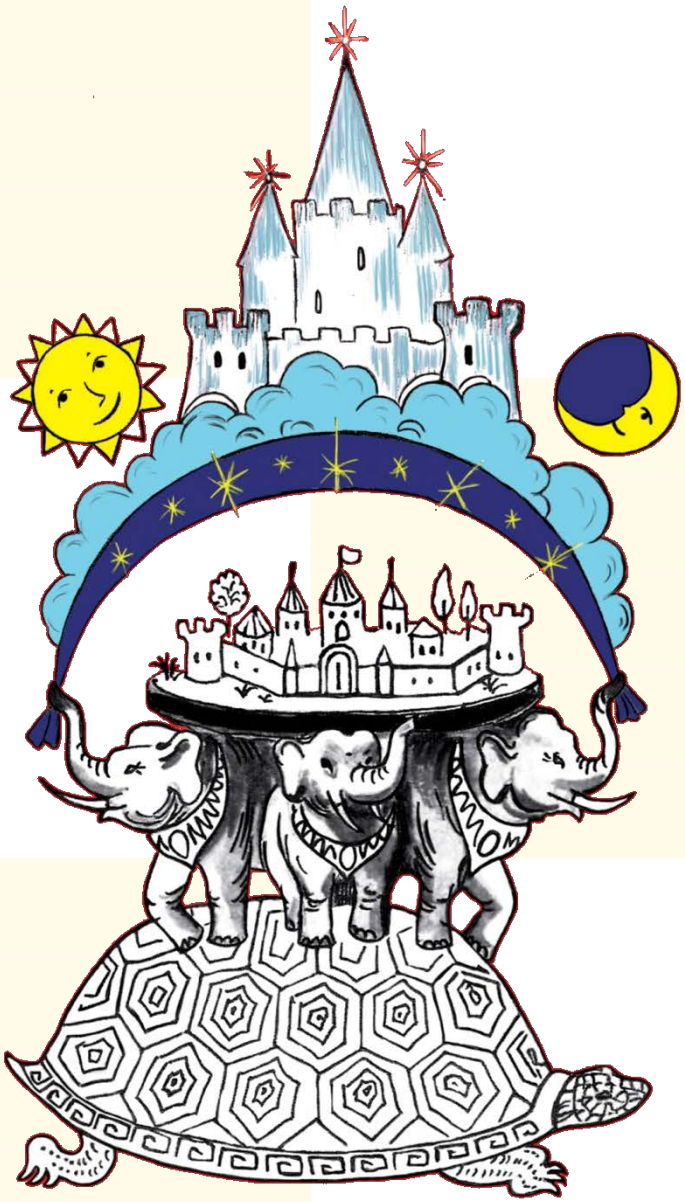


Защищенная инфраструктура

удаленного доступа предполагает защищенность терминального клиента – доверенную загрузку его ОС.

Доверенная загрузка ОС на терминальном клиенте может обеспечиваться установкой на ТК Аккорд-АМДЗ или применением полностью интегрированных с СЗИ НСД Аккорд системами «Центр-Т» и СОДС «МАРШ!»

Защищенная инфраструктура виртуализации



Аккорд-В.

Система защиты

- ✓ полностью интегрируется в инфраструктуру виртуализации, поэтому для ее функционирования не требуются дополнительные серверы;
- ✓ Реализует концепцию корректного старта на всех этапах запуска системы;
- ✓ не ограничивает в целях безопасности возможностей инфраструктуры виртуализации, оставляя доступными все ее преимущества.

Удаленный доступ

Удаленный доступ

системы удаленного доступа могут строиться несколькими способами

- ✓ Терминальный доступ (работа с терминальным сервером в терминальной сессии)
- ✓ Web-доступ (работа через web-интерфейс с web-ресурсом)
- ✓ Смешанная система, сочетающая возможность работы в одном и во втором режиме

Удаленный доступ

целесообразен во многом потому, что он делает систему экономически выгоднее

- ✓ Тонкие клиенты дешевле ПК
- ✓ Существенно меньше затрат на СЗИ при том же уровне защищенности
- ✓ В качестве клиентских рабочих мест могут использоваться самые разные СВТ

Удаленный доступ

целесообразен, если эти принципы при построении системы НЕ НАРУШАЮТСЯ

- ✓ Тонкие клиенты дешевле ПК
- ✓ Существенно меньше затрат на СЗИ при том же уровне защищенности
- ✓ В качестве клиентских рабочих мест могут использоваться самые разные СВТ

Удаленный доступ

безопасен, если защищены

- ✓ сам удаленный ресурс,
- ✓ клиентские рабочие места и
- ✓ их взаимодействие

причем компоненты СЗИ – части единой системы, а не разрозненные не связанные между собой средства

Тонкое место

системы удаленного доступа – это доверенная среда на клиентском рабочем месте

- ✓ ПАК «Центр-Т»(работа с терминальным сервером в терминальной сессии)
- ✓ СОДС «МАРШ!»(работа через web-интерфейс с web-ресурсом и системы смешанного типа)

ПАК «Центр-Т» и СОДС «МАРШ!» не конфликтуют между собой и могут использоваться в одной системе или в разных, доступ к которым осуществляется с одних и тех же клиентских мест.

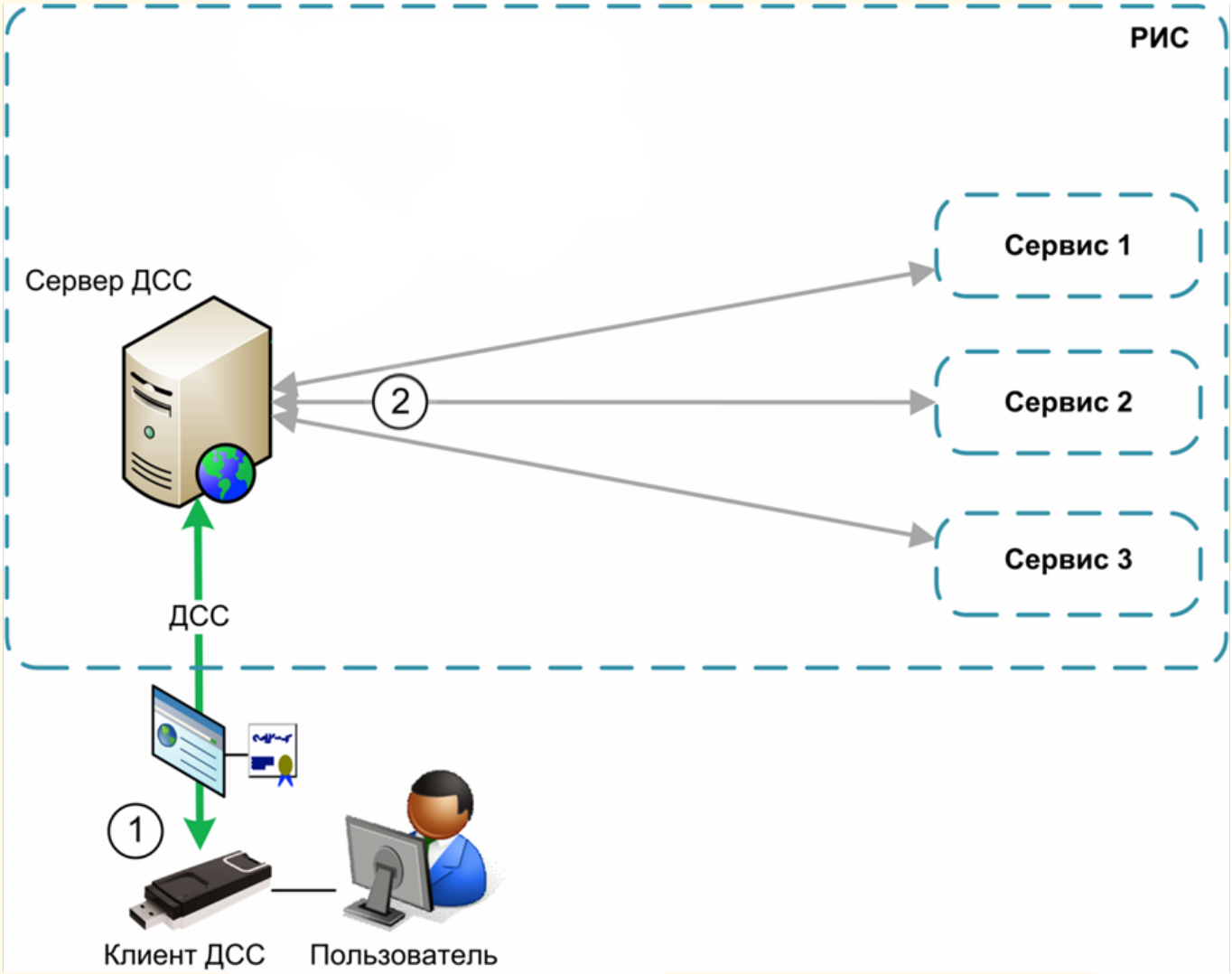
СОДС «МАРШ!»

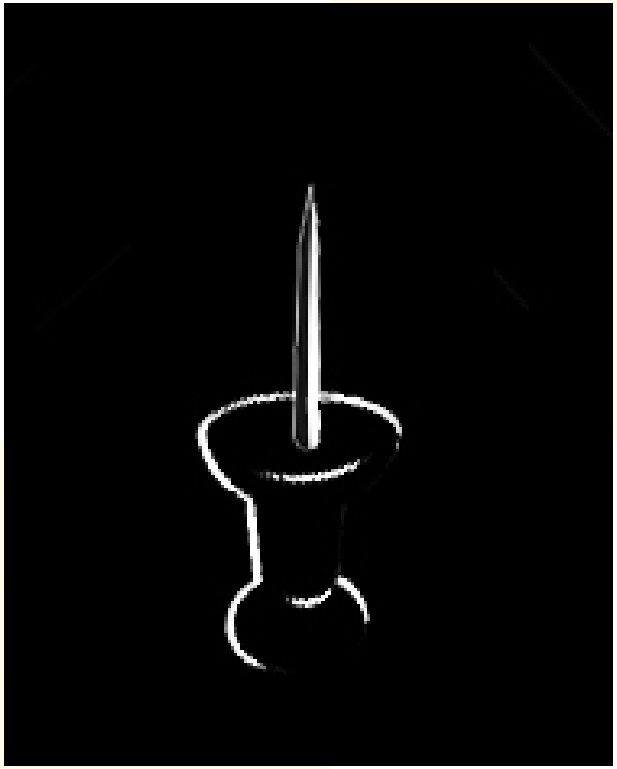
Определение ДСС

Доверенный сеанс связи (ДСС) – период работы компьютера, в рамках которого:

- ✓обеспечивается доверенная загрузка ОС
- ✓организуется защищенное соединение
- ✓поддерживаются достаточные условия для работы с ЭЦП

Схема работы «МАРШ!»





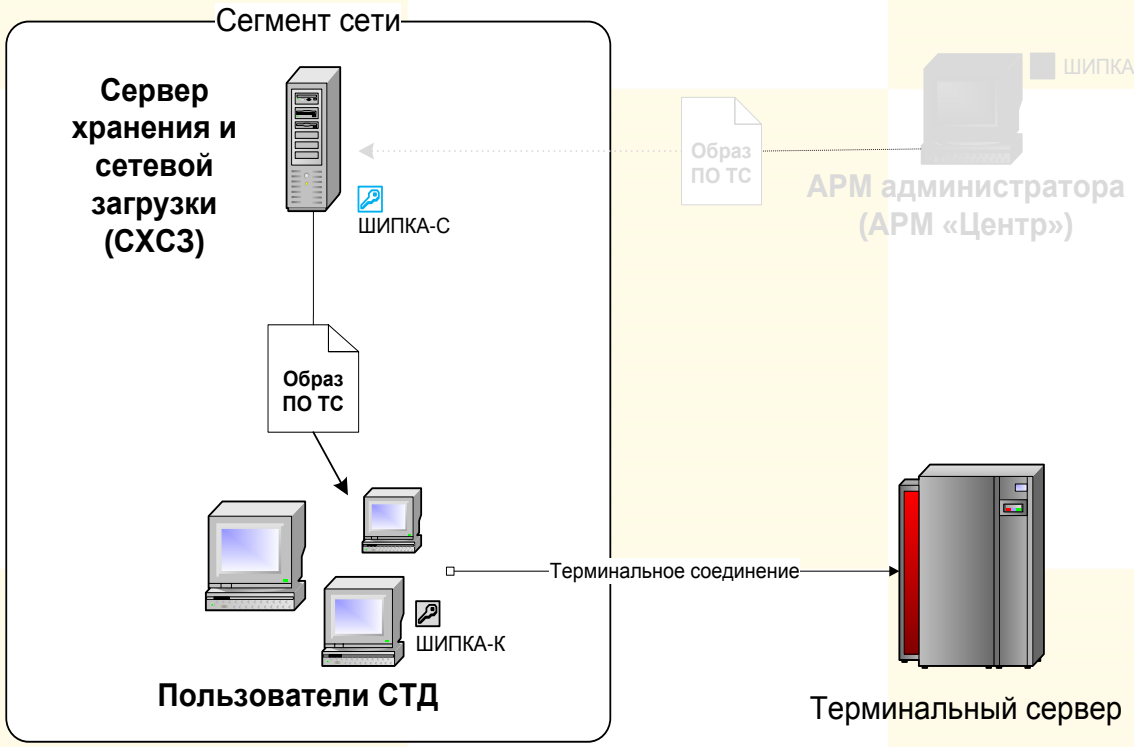
Центр-Т

Система защищенной сетевой загрузки программного обеспечения на терминальные станции

Назначение системы

1. Организация терминального доступа с бездисковых рабочих станций путем загрузки образов ПО терминальных станций (ПО ТС) по сети;
2. Обеспечение централизованного управления и аудита процесса загрузки образов;
3. Контроль целостности загружаемых образов;
4. Осуществление входа пользователя на терминальный сервер, защищенный ПАК СЗИ НСД Аккорд TSE, с использованием аппаратного идентификатора, в роли которого выступает ПСКЗИ ШИПКА.

Порядок работы пользователей СТД



1. Пользователь запускает ТС с подключенной ШИПКА-К;
2. С ШИПКА-К загружается ОНЗ, запрашивается PIN-код;
3. После ввода PIN-кода с СХСЗ загружается образ ПО ТС, проверяется его целостность;
4. После успешной проверки целостности управление передается образу ПО ТС;
5. Запускается терминальная сессия.

Удаленный доступ

при использовании СОДС «МАРШ!» и/или ПАК «Центр-Т» не теряет своих преимуществ

- ✓ Не требует существенного переоборудования самой АС или изменения регламента ее работы
- ✓ Затраты на защиту информации в разы меньше, чем при традиционных подходах
- ✓ Не влечет потерю инвестиций, так как в качестве клиентских рабочих мест могут использоваться самые разные СВТ

ПЕРСОНАЛЬНОЕ СКЗИ

ШИПКА

Функциональность ПСКЗИ ШИПКА

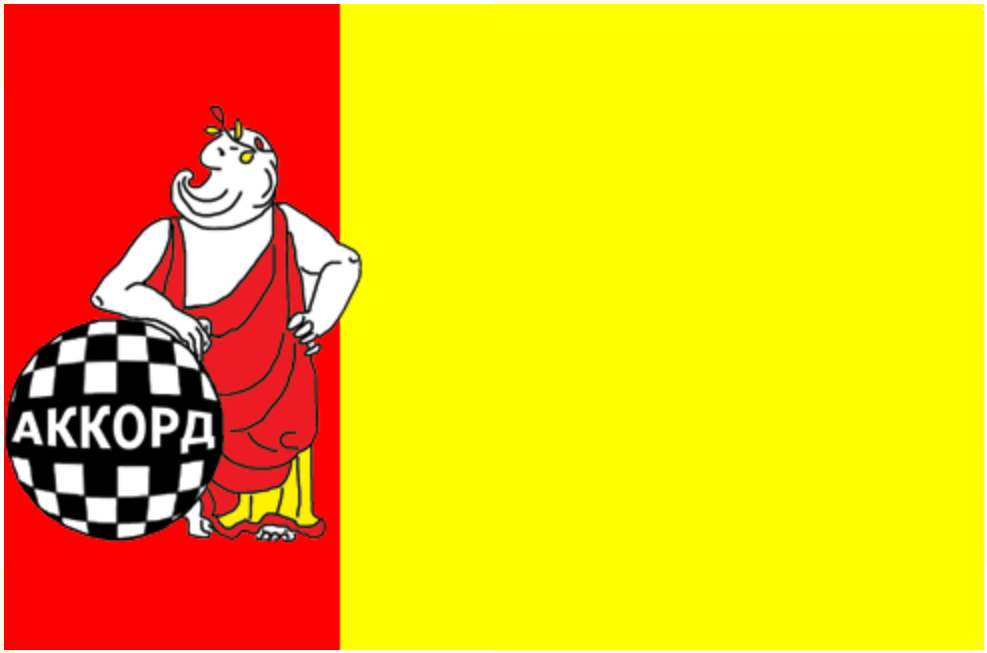
- ✓ Аппаратное СКЗИ
- ✓ Идентификация/аутентификация пользователя в ПАК Аккорд (локально и на терминальных серверах)
- ✓ Идентификация/аутентификация пользователя в ОС Windows
- ✓ Идентификация/аутентификация пользователя в Домене
- ✓ Хранение ключей программных СКЗИ, в том числе VPN
- ✓ Хранение паролей и автозаполнение форм авторизации

ПСКЗИ ШИПКА является базой ПАК «Центр-Т» и Privacy

Криптографическая функциональность

- ✓ Шифрование и подпись данных
- ✓ Шифрование и подпись сообщений электронной почты
- ✓ Генерация самоподписанных цифровых сертификатов, получение сертификатов УЦ, хранение и применение сертификатов
- ✓ Выработка ключей и управление ими в трех парадигмах:
  - прямой обмен ключами и их использование
  - использование ключей в составе сертификатов
  - использование ключей в формате «сети доверия»

«Аккорд-У»



«Аккорд-У» <–> ШИПКА

полностью совместимы с точки зрения работы навстречу:

- ✓могут обмениваться ключами;
- ✓могут производить все встречные криптографические операции;
- ✓пользовательские программы полностью аналогичны.

Целесообразно построение систем, сочетающих эти два типа устройств. Это позволит получить достаточно гибкое в смысле стоимости и дружественности решение.

Сертификат соотвествия требованиям ФСБ России

варианты исполнения «Аккорд-У» сертифицированы в качестве СКЗИ и в качестве СЭП по требованиям классов:

КС3

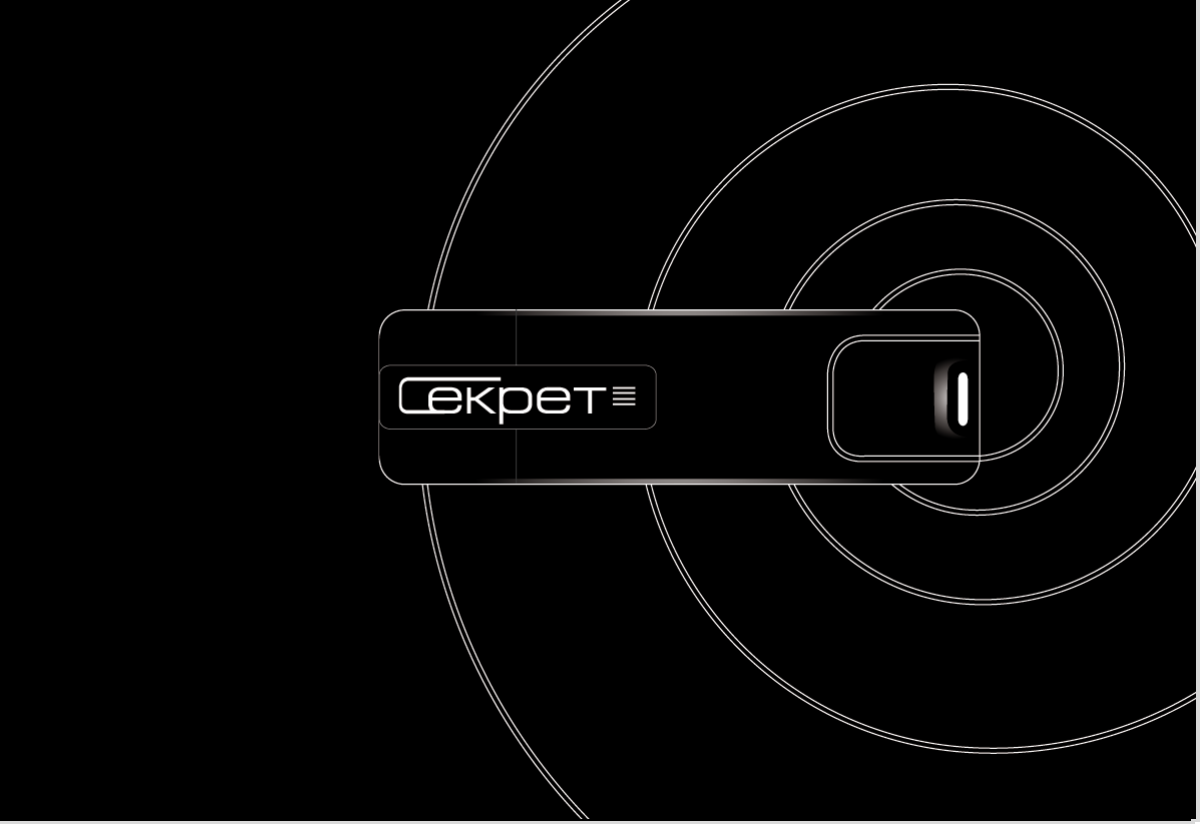
и

КВ2

«Автограф»

удостверяющий центр, построенный на базе разработок ОКБ САПР:

- ✓ ПСКЗИ ШИПКА
- ✓ АККОРД-У
- ✓ ПАК Аккорд



СЛУЖЕБНЫЙ НОСИТЕЛЬ СЕКРЕТ

Угрозы при использовании внешних носителей данных

- ✓ Возможность потери и, соответственно, находки.
- ✓ Реализация внутренних угроз ИБ (нерегламентированное использование служебной информации).
- ✓ Заражение вредоносным ПО компьютеров корпоративной сети.

Традиционные способы защиты информации

при работе со съемными носителями

- ✓ аутентификация по PIN-коду или биометрическим данным;
- ✓ «прозрачное» (то есть в фоновом режиме на основании ввода пароля) шифрование содержимого носителя информации;
- ✓ использование USB-фильтров (запрет работы с «неразрешенными» носителями);
- ✓ полный запрет применения.

Служебный носитель «Секрет»

специальный USB-носитель (mass storage), который можно использовать только на разрешенных администратором АРМ:

- ✓ Личный Секрет;
- ✓ Секрет Фирмы;
- ✓ Секрет Особого Назначения.

ОКБ САПР

Предложения?