Аттестация ИСПДн – собственный успешный опыт:

Опыт аттестации АС с «зоопарком» СВТ и различными типами доступа

Рябов Андрей

ЗАО «ОКБ САПР»

О чем сегодня пойдет речь?

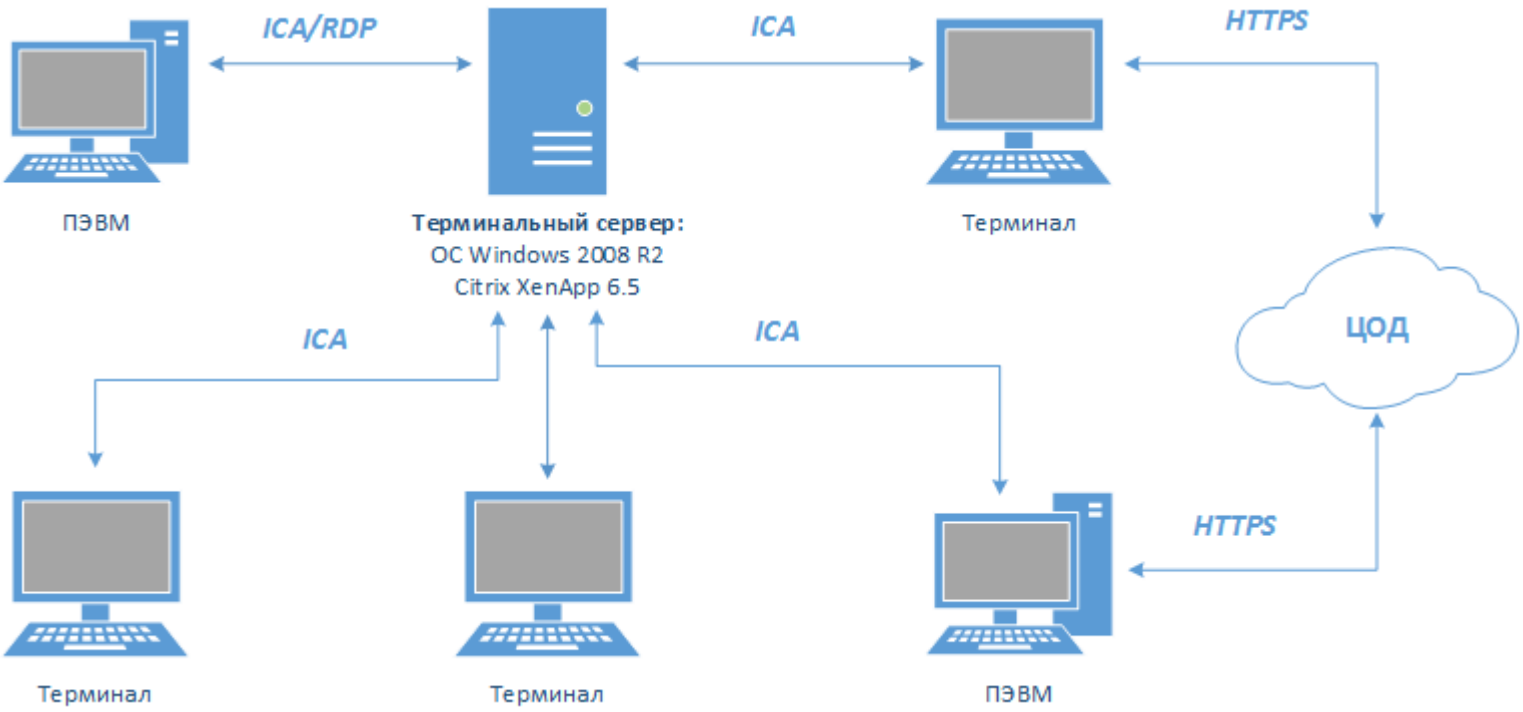
Рассмотрим вопросы защиты ИСПДн с высоким уровнем защиты **(УЗ-2)** на примере типовой терминальной системы с «зоопарком» СВТ (ПК, терминальные станции, бездисковые ПЭВМ) и различными типами удаленного доступа (Web, терминальный ICA/RDP)

Краткое описание типовой терминальной системы

- ИС включает в себя два логических сегмента: пользовательский и серверный;
- В качестве платформы, реализующей технологии терминального доступа, применяется решение Citrix XenApp 6.5;
- У пользователей ИС различаются технологические процессы:
  - некоторые пользователи ИС осуществляют обработку ПДн и локально и на сервере,
  - некоторые пользователи ИС осуществляют ПДн только на сервере,
  - некоторым пользователям необходим периодический доступ к Web-ресурсам внешних ИС;
- Различные протоколы взаимодействия (RDP, ICA, HTTP(S));
- Сегмент АРМ состоит из различных видов и типов СВТ - от высокопроизводительных полнофункциональных вычислительных машин до бездисковых терминальных станций.
- Уровень защищенности ИСПДн УЗ-2.

Краткое описание типовой терминальной системы

- Схема взаимодействия:



Требования регуляторов по защите персональных данных

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ФСТЭК России:

Приказ № 21 ФСТЭК России от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Требования к ИСПДн УЗ-2

Адаптированный набор мер для ИСПДн УЗ-2, с учетом особенностей применяемых технологий и архитектуры ИС:

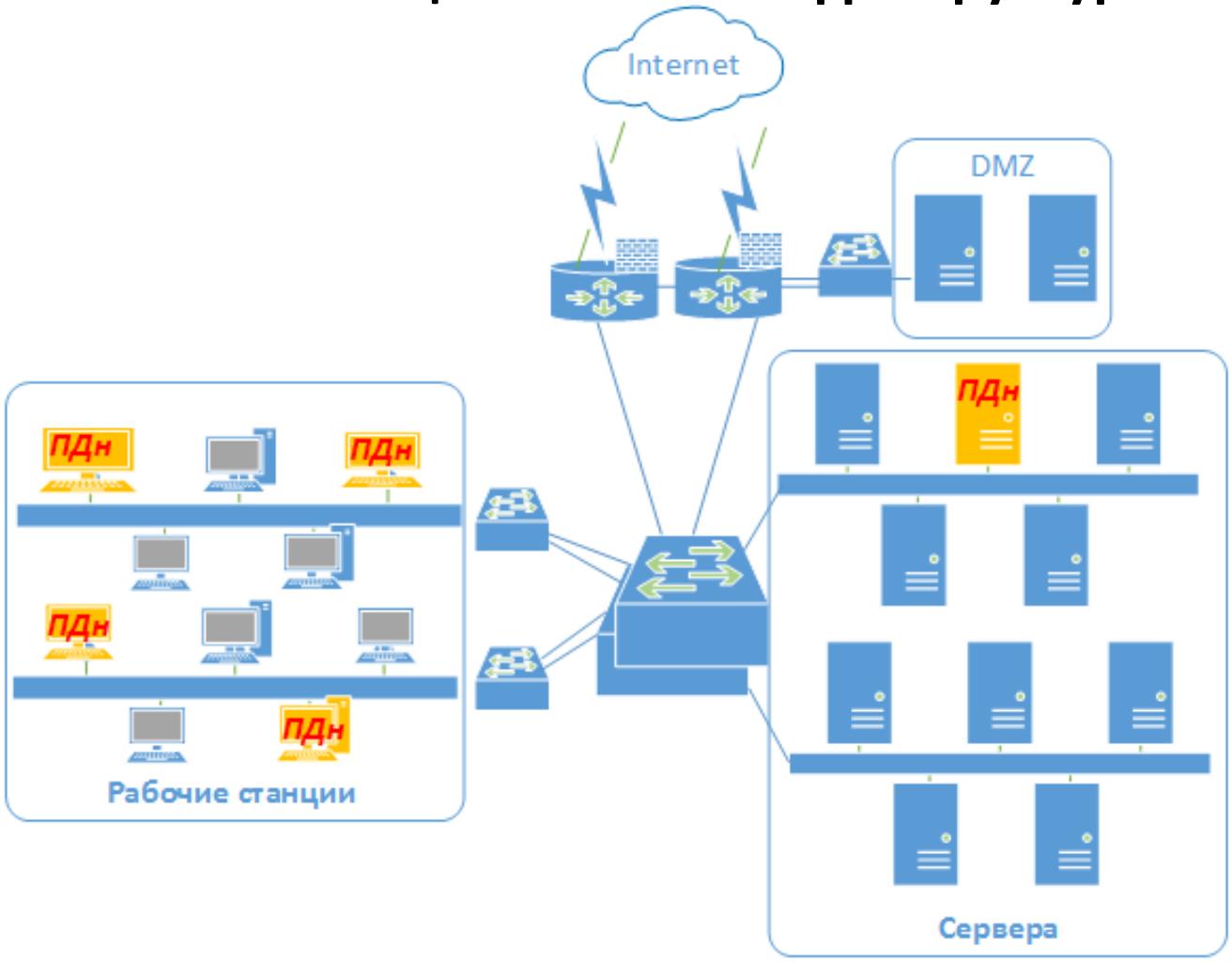
- идентификация и аутентификация субъектов доступа и объектов доступа **(ИАФ.1-6)**;
- управление доступом субъектов доступа к объектам доступа **(УПД.1-6, 10, 11, 17)**;
- ограничение программной среды **(ОПС.2)**;
- защита машинных носителей информации **(ЗНИ.1, 2, 8)**;
- регистрация событий безопасности **(РСБ.1-3, 5, 7);**
- антивирусная защита **(АВЗ.1, 2)**;
- контроль (анализ) защищенности информации **(АНЗ.1-5)**;
- обеспечение целостности ИС и информации **(ОЦЛ.1, 4);**
- обеспечение доступности информации **(ОДТ.4, 5)**;
- защита технических средств **(ЗТС.3, 4)**;
- защита ИС, ее средств и систем связи и передачи данных **(ЗИС.15, 17, 23)**,
- выявление инцидентов и реагирование на них **(ИНЦ.1-6)**;
- управление конфигурацией ИС и СЗПДн **(УКФ.1-4).**

Требования к ИСПДн УЗ-2

Должны применяться сертифицированные средства защиты:

- СВТ не ниже 5 класса;
- САВЗ не ниже 4 класса;
- МЭ не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия ИС с Интернет и МЭ не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия ИС с Интернет;
- ПО СЗИ должно пройти проверку по 4 уроню контроля НДВ.

Оптимизация сетевой инфраструктуры

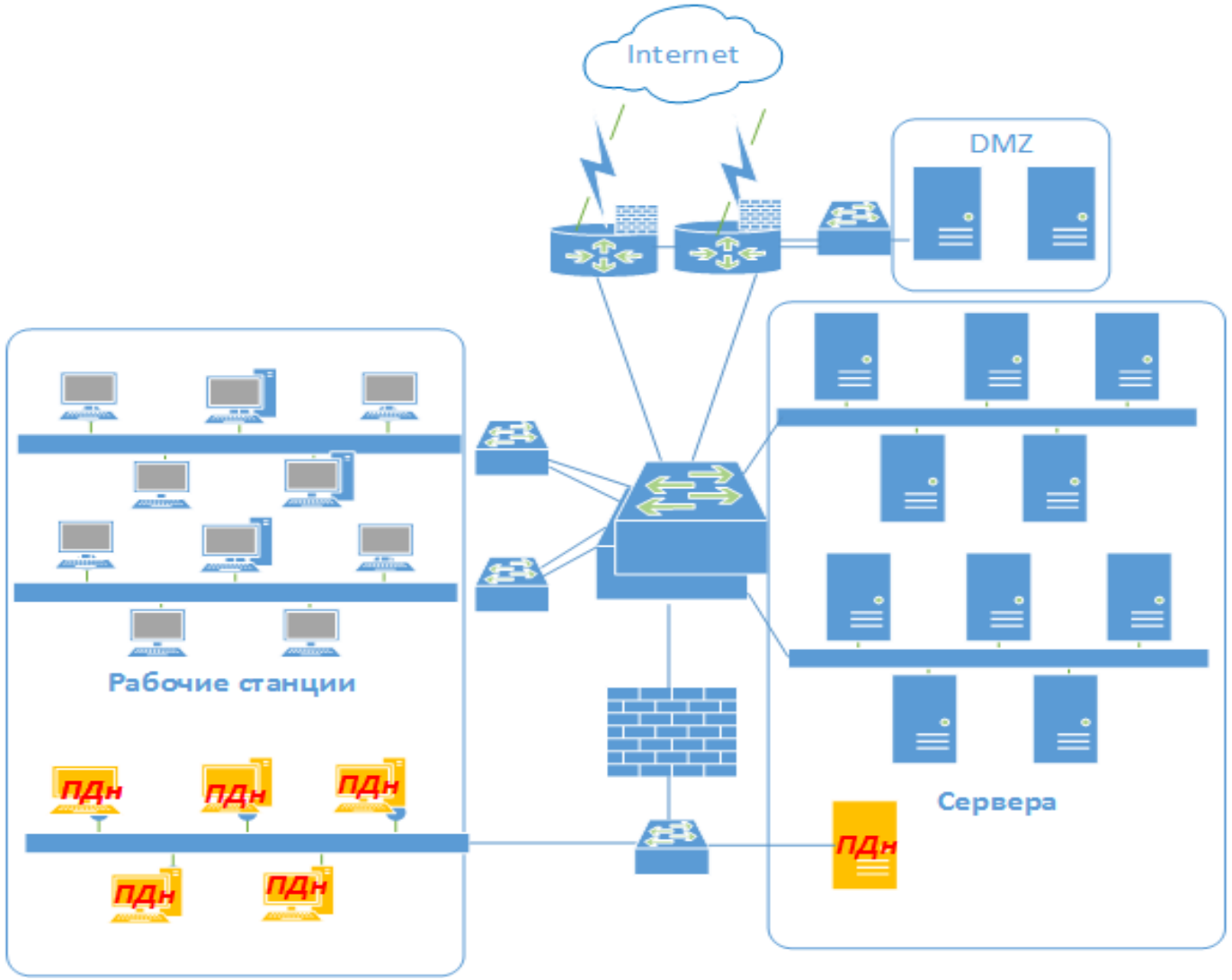


Оптимизация сетевой инфраструктуры

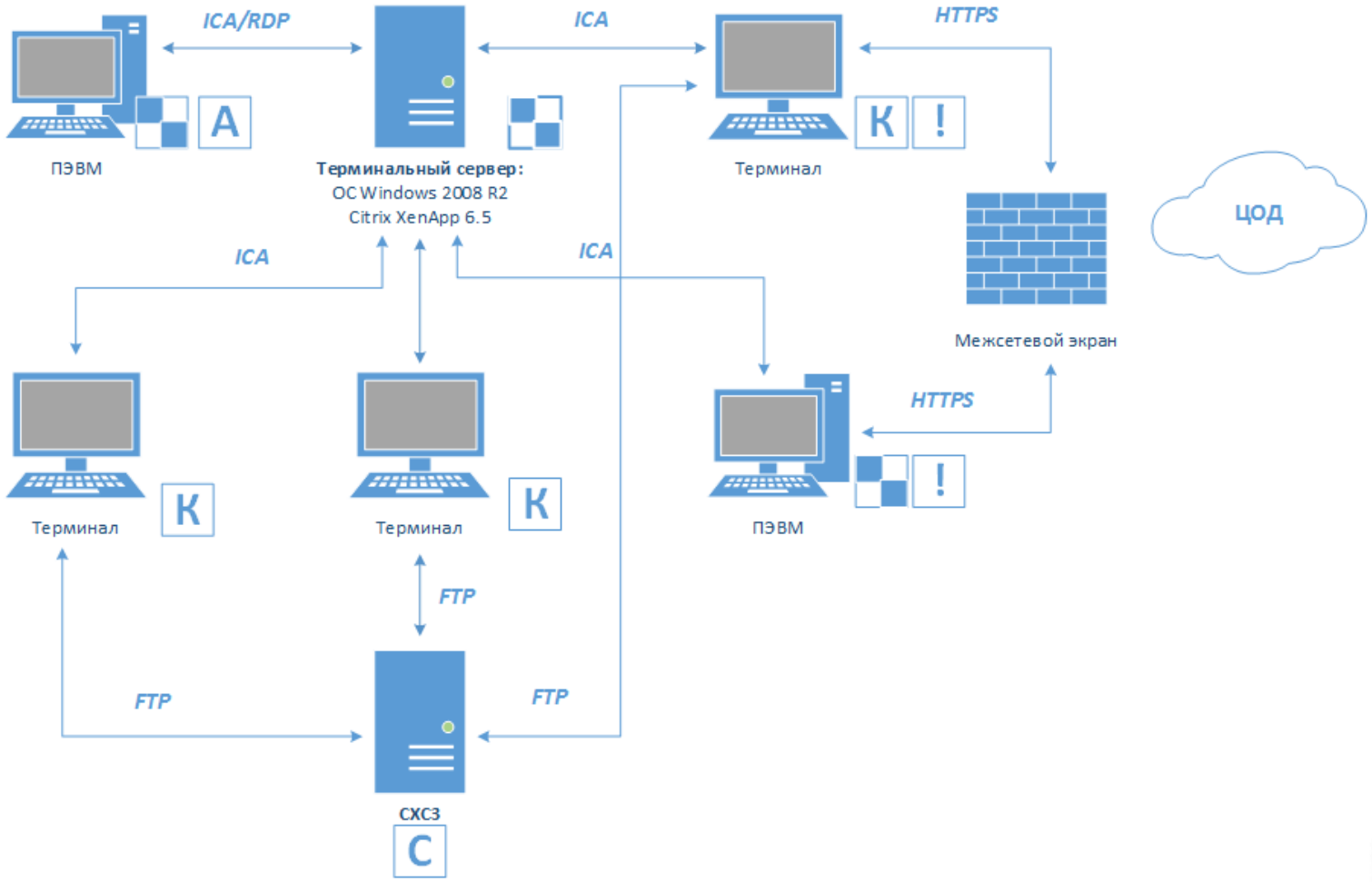
Меры защиты:

- Сегментация ИС **(ЗИС.17)**:
  - Сегментирование ИС проводиться с целью разделения ИС на сегменты, имеющие различные классы защищенности.
- Защита периметра ИС **(ЗИС.23):**
  - управление (контроль) входящими в ИС и исходящими из ИС информационными потоками;
  - обеспечение взаимодействия ИС с другими ИС и сетями только через управляемые (контролируемые) сетевые интерфейсы;
  - ограничение количества точек доступа в ИС из внешних ИС и сетей;
  - реализация правил управления информационными потоками;
  - реализация принципа «запрещено все, что не разрешено»;
- Управление доступом в ИС (фильтрация, маршрутизация, контроль соединений) **(УПД.3)**.

Оптимизация сетевой инфраструктуры



Состав и схема взаимодействия технических средств ИСПДн



Защита терминального сервера

Угрозы ИБ терминального сервера:

- Угрозы, реализуемые до загрузки ОС сервера;
- Угрозы, реализуемые после загрузки ОС севера;
- Угрозы внедрения вредоносного ПО.

Защита терминального сервера

На терминальном сервере необходимо обеспечить:

- доверенную загрузку операционной системы (УПД.17),
- идентификацию/аутентификацию пользователей/стационарных и моб. устройств (ИАФ.1-5);
- разграничение доступа пользователей к ресурсам сервера(УПД.1, 2, 4-6, 10-11)
- регистрацию событий безопасности(РСБ.1-3, 5);
- контроль целостности ПО (в т.ч. ПО СЗИ) (ОЦЛ.1);
- антивирусную защиту системы (АВЗ.1).

Защита терминального сервера

ПАК «Аккорд-Win64» (TSE):

- доверенная загрузка ОС (Аккорд-АМДЗ);
- аппаратная И/А пользователей ;
- контроль целостности ПО и данных, их защита от несанкционированных модификаций;
- разграничение доступа пользователей к ресурсам сервера (дискреционный и мандатный контроль доступа);
- усиленная аутентификация терминальных станций с помощью контроллера Аккорд или ШИПКА;
- управление терминальными сессиями;
- контроль печати на принтерах;
- контроль доступа к устройствам.

Защита полнофункциональных ПЭВМ

Угрозы ИБ полнофункциональных ПЭВМ:

- Угрозы, реализуемые до загрузки ОС;
- Угрозы, реализуемые после загрузки ОС;
- Угрозы внедрения вредоносного ПО.

Защита полнофункциональных ПЭВМ

на ПЭВМ необходимо обеспечить:

- доверенную загрузку операционной системы (УПД.17),
- идентификацию/аутентификацию пользователей/стационарных и моб. устройств (ИАФ.1-5);
- разграничение доступа пользователей к ресурсам сервера(УПД.1, 2, 4-6, 10-11);
- регистрацию событий безопасности (РСБ.1-3, 5);
- контроль целостности ПО (в т.ч. ПО СЗИ) (ОЦЛ.1);
- антивирусную защиту системы (АВЗ.1).

Защита полнофункциональных ПЭВМ

ПАК «Аккорд-Win32» («Аккорд-Win64»):

- доверенная загрузка ОС (Аккорд-АМДЗ);
- аппаратная И/А пользователей ;
- контроль целостности ПО и данных, их защита от несанкционированных модификаций;
- разграничение доступа пользователей к ресурсам ПЭВМ (дискреционный и мандатный контроль доступа);
- контроль печати на принтерах;
- контроль доступа к устройствам.

Сертифицировано ФСТЭК

ПАК «Аккорд-Win32»

Сертификат ФСТЭК России №2398

- СВТ 3, НДВ 2.
- ИСПДн УЗ-1;
- ГИС К1;
- АС 1Б.

ПАК Аккорд-Win64

Сертификат ФСТЭК России №2400

- СВТ 3, НДВ 2.
- ИСПДн УЗ-1;
- ГИС К1;
- АС 1Б.

Защита тонких клиентов

- Тонкие клиенты не содержат данных, но реализуют технологии, которые нуждаются в защите.
- ОС терминального клиента поддерживает работу оборудования терминала (сетевая карта, видеокарта и так далее), именно в ней исполняется (как приложение) само ПО терминального клиента ICA или RDP, поддерживается работа протокола.
- Часто используются дистрибутивы Linux.

Защита тонких клиентов

- **Тонкие клиенты** информационной системы являются ее такой же неотъемлемой частью;
- Для построения информационной системы **с равным уровнем защищенности**, необходимо обеспечивать и их защиту в том числе.
- **Тонкие клиенты** имеют ряд особенностей как архитектурных, так и функциональных;
- Все это оказывает **влияние** на весь технологический процесс и, как следствие, на **технологию защиты** процесса загрузки.

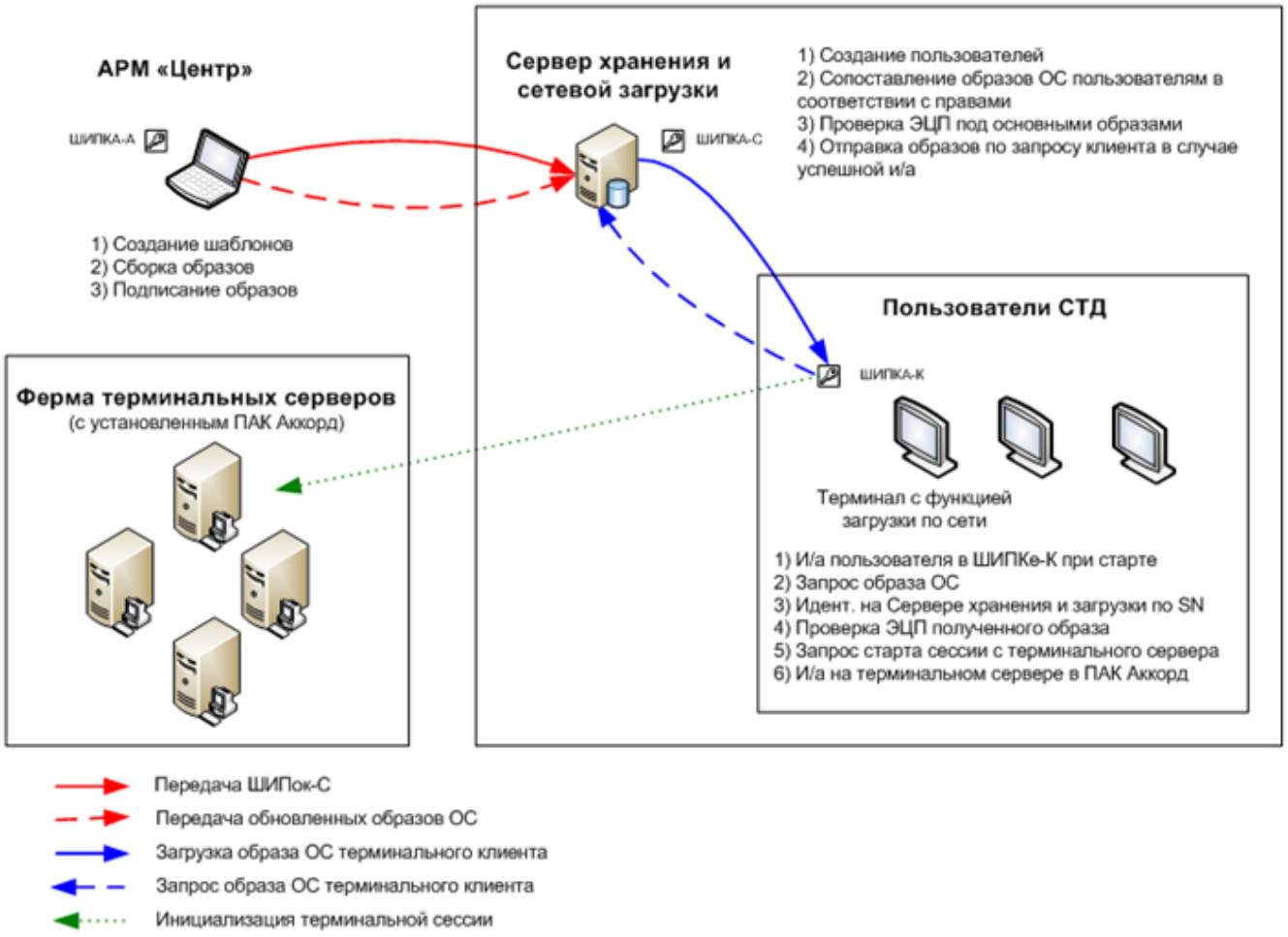
ПАК Центр-Т

- реализует технологию защищенной загрузки по сети ОС терминальной станции, хранящейся на мобильном устройстве.
- аппаратно независим - он полностью реализован на ШИПКА (и клиентские, и серверные компоненты размещаются на дисках, встроенных в эти устройства и могут исполняться на любом ПК).
- позволяет гарантировать контролируемую целостность и подлинность образов ПО терминальных станций, загружаемых по сети, криптографическими методами, реализованными полностью аппаратно.

ПАК Центр-Т

- Автоматизированное рабочее место «Центр» (АРМ «Центр»):
  - создание шаблонов;
  - Сборка образов терминальной станции;
  - подпись образов;
- Сервер хранения и сетевой загрузки (СХСЗ):
  - Управление пользователями и образами;
  - Проверка ЭЦП;
  - Отправка образа на клиентское устройство при успешных И/А;
- Клиентские ШИПКА для терминальных станций в составе СТД (ШИПКА-К):
  - Аутентификация пользователя до загрузки терминальной станции;
  - Загрузка образа;
  - Автоматическое подключение к терминальному серверу по протоколу Citrix ICA или RDP;
  - Использование ШИПКА-К в качестве аппаратного идентификатора при входе на терминальный сервер, защищенный ПАК «Аккорд-Win64» (TSE);
  - «Проброс» USB-принтеров и flash-носителей, подключенных к терминальной станции в рамках терминальной сессии

ПАК Центр-Т


АРМ «Центр»
ШИПКА-А
1) Создание шаблонов
2) Сборка образов
3) Подписание образов
Сервер хранения и сетевой загрузки
ШИПКА-С
1) Создание пользователей
2) Сопоставление образов ОС пользователям в соответствии с правами
3) Проверка ЭЦП под основными образами
4) Отправка образов по запросу клиента в случае успешной и/а
Ферма терминальных серверов
(с установленным ПАК Аккорд)
Пользователи СТД
ШИПКА-К
Терминал с функцией загрузки по сети
1) И/а пользователя в ШИПКе-К при старте
2) Запрос образа ОС
3) Идент. на Сервере хранения и загрузки по SN
4) Проверка ЭЦП полученного образа
5) Запрос старта сессии с терминального сервера
6) И/а на терминальном сервере в ПАК Аккорд
Передача ШИПок-С
Передача обновленных образов ОС
Загрузка образа ОС терминального клиента
Запрос образа ОС терминального клиента
Инициализация терминальной сессии

ПАК Центр-Т

Сертифицировано ФСТЭК

На сертификации:

- ТУ;
- НДВ 4;
- ИСПДн УЗ-1;
- ГИС К1;
- АС 1Г.

Периодическая работа с Web-ресурсами сторонних ИС

СОДС «МАРШ!»:

- реализует концепцию ДСС.
- является мобильным загрузочным устройством, готовым к работе на любом «недоверенном» компьютере;

«МАРШ!» предназначен для:

- обеспечения доверенной загрузки ОС (ОС загружается из защищённой от записи памяти устройства, жёсткий диск компьютера не используется);
- средства обеспечения защищённого соединения (VPN);
- средства идентификации-аутентификации пользователя;
- средства выработки и проверки ЭЦП;

Периодическая работа с Web-ресурсами сторонних ИС

- **Образ ОС СОДС «МАРШ!»** формируется по заказу для каждой конкретной системы и включает только необходимые и достаточные для этой системы компоненты.
- В рассматриваемой ИС в образ ОС включен браузер для работы с Web-ресурсами сторонних ИС и клиентское ПО Citrix Receiver для работы с ресурсами терминального сервера.
- С помощью «МАРШ!» пользователь идентифицируется на терминальном сервере в подсистеме И/А «Аккорд-Win64» (TSE).

СОДС МАРШ!

Сертифицировано ФСТЭК

Сертификат ФСТЭК России № 2797.

- НДВ 4 и ТУ;
- ИСПДн УЗ-1;
- ГИС К1.

Вопросы???

Спасибо за внимание!

С уважением,
Рябов Андрей
ЗАО «ОКБ САПР»
www: www.okbsapr.ru
email: asr@okbsapr.ru