

**Защищенная система
терминального доступа
как средство выполнения
требований
№152-ФЗ «О персональных данных»**

ОКБ САПР
<http://www.accord.ru>
<http://www.shipka.ru>
okbsapr@okbsapr.ru



**Аккорд.
Надежность в ненадежном мире.**

2010

Особенности требований №152-ФЗ к ИСПДн

- ✓ требования могут выполняться различными способами (неоднозначность);
- ✓ способы выполнения требований сильно привязаны к функциональным особенностям конкретной АС (нетипичность).

К соответствию требованиям №152-ФЗ необходимо приводить в том числе уже существующие и функционирующие АС.

В итоге разработчиками предлагаются ***различные по архитектуре и стоимости средства защиты.***



Основные цели внедрения средств защиты

- ✓ достижение максимального эффекта с минимальными изменениями:
 - **приведение АС к соответствию требованиям №152-ФЗ;**
 - минимизация затрат на переоборудование и потерь от списания технических компонент АС (в т.ч. использовавшихся ранее СЗИ);
 - недопущение возможности остановки работы АС и потери данных.
- ✓ переход к более выгодным решениям – например к **терминальным решениям.**



Еще не забытое старое становится новым:

терминальные решения **снова
востребованы**, поскольку они:

- ✓ **дешевле** – как установка, так и дальнейшее обслуживание;
- ✓ **удобнее** – проще администрирование, ниже требования к производительности оборудования;
- ✓ **надежнее** – выгода с точки зрения информационной безопасности, при инциденте с терминалом данные сохраняются на сервере.



Старое или новое?

Суть терминальной сессии осталась прежней:

- ✓ на **сервере** хранятся и обрабатываются ПД;
- ✓ рабочие места пользователей, на которых обрабатываются ПД, объединяются в терминальную систему;
- ✓ на **сервер** от пользователя передаются только нажатия клавиш и манипуляции с мышью;
- ✓ на **терминал** к пользователю передаются изменения изображения на экране.



Безопасность терминальных решений

✓ Данные обрабатываются в одном месте – на сервере. Значит, **в защите нуждается сервер**. Но необходимо позаботиться и о **защите «тонких клиентов»**.

✓ Методы защиты:

- двухфакторная идентификация;
- защищенное хранение аутентификационных данных;
- доверенная среда и механизм проверки аутентификационных данных на сервере.



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».



Защищенность терминальных решений

достигается, если

- ✓ **со стороны сервера** в момент создания терминальной сессии проверяется не только **пользователь**, но и «**тонкий клиент**»;
- ✓ **со стороны «тонкого клиента»** проверяется, что **сервер** именно тот, с которым должен работать данный пользователь.



Защищенность терминальных решений

достигается

применением ПАК СЗИ НСД

Аккорд-НТ/2000 V3.0,

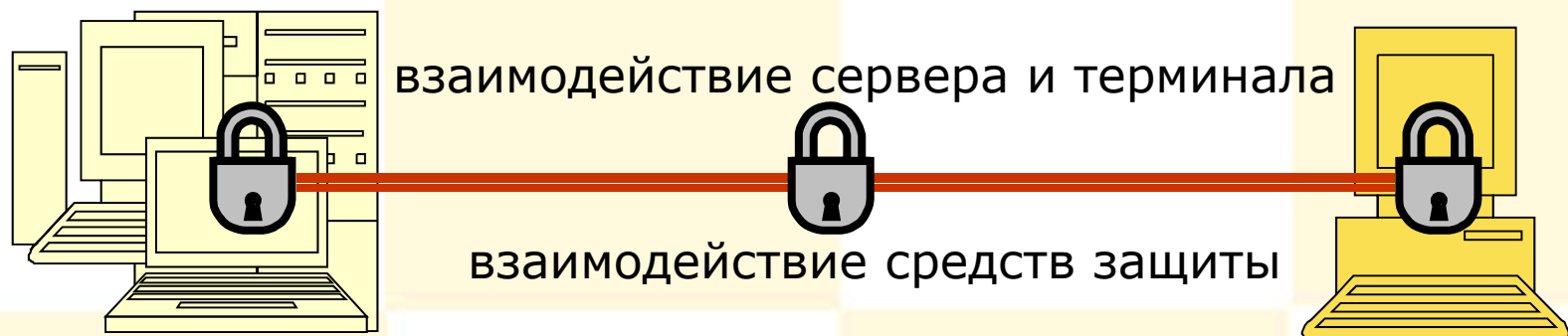
**сертифицированного ФСТЭК России
(сертификат № 1161)**



Защищенность терминальных решений

достигается применением ПАК СЗИ НСД Аккорд-NT/2000 V3.0, обеспечивающим

- ✓ защищенность терминальных серверов;
- ✓ защищенность «тонких клиентов»;
- ✓ взаимодействие этих защитных механизмов.



ПАК Аккорд-NT/2000 V3.0

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.



Соответствие требованиям к 1 классу ИСПДн (управление доступом)

- ✓ обеспечение идентификации/аутентификации пользователей при входе в ОС, при входе в СЗИ, при управлении функциями СЗИ;
- ✓ обеспечение защиты аутентификационной информации субъекта доступа;
- ✓ наличие механизмов блокирования терминала доступа;
- ✓ обеспечение идентификации терминалов, средств обработки ПДн, узлов ИСПДн, каналов связи, носителей ПДн;
- ✓ наличие механизмов ролевого разграничения доступа и контроля информационных потоков ко всем модулям СЗИ;
- ✓ управление потоками информации с помощью меток конфиденциальности.



Соответствие требованиям к 1 классу ИСПДн (регистрация и учет)

- ✓ регистрация входа/выхода, загрузки, инициализации и программного останова ОС;
- ✓ регистрация обращений субъекта доступа к СЗИ;
- ✓ регистрация попыток НСД;
- ✓ регистрация обновлений СЗИ;
- ✓ регистрация событий запуска/завершения модулей СЗИ;
- ✓ регистрация событий отката для СЗИ;
- ✓ регистрация запуска процессов, предназначенных для обработки защищаемых данных. Регистрация попыток доступа к данным;
- ✓ регистрация выдачи печатных документов на «твердую» копию;
- ✓ регистрация попыток доступа программных средств к терминалам, узлам ИСПДн, устройствам, ➡

Соответствие требованиям к 1 классу ИСПДн (регистрация и учет)

- ✓ автоматический учет создаваемых защищаемых файлов;
- ✓ сигнализация попыток нарушения защиты;
- ✓ защита данных регистрации от уничтожения/модификации нарушителем;
- ✓ наличие механизмов просмотра и анализа данных регистрации с фильтрацией по параметрам;
- ✓ очистка освобождаемых областей оперативной памяти (обнуление, обезличивание);
- ✓ автоматический непрерывный мониторинг событий, являющихся причиной реализации ПМВ;
- ✓ механизм автоматического анализа по шаблонам типовых ПМВ с автоматическим блокированием и уведомлением администратора безопасности.



Соответствие требованиям к 1 классу ИСПДн (обеспечение целостности)

- ✓ обеспечение целостности программных СЗ в составе СЗПДн и неизменности программной среды;
- ✓ проведение проверки целостности модулей СЗ от ПМВ при его загрузке с использованием контрольных сумм;
- ✓ проведение автоматического контроля корректности функционирования аппаратного обеспечения ИСПДн, необходимого для функционирования средства защиты от ПМВ;
- ✓ использование сертифицированных средства защиты информации.



**Защищенная система
терминального доступа
как средство выполнения
требований
№152-ФЗ «О персональных данных»**

ОКБ САПР
<http://www.accord.ru>
<http://www.shipka.ru>
okbsapr@okbsapr.ru



**Аккорд.
Надежность в ненадежном мире.**

2010