Аттестация ИСПДн – собственный успешный опыт

Задача аттестации ИСПДн не является профильной для разработчиков средств защиты информации, однако, чтобы лучше понимать вопросы, с которыми сталкиваются наши Заказчики при внедрении наших продуктов, а в идеале – быть способными оказать им необходимую помощь в практическом решении этих вопросов, мы решили самостоятельно пройти этот путь и аттестовать собственную систему защищенного терминального доступа в ИСПДн по второму уровню защищенности[1] персональных данных.

Естественно, наша информационная система (ИС) включает в себя два логических сегмента: пользовательский и серверный. В качестве платформы, реализующей технологии терминального доступа, применяется флагманское решение Citrix XenApp компании «Citrix». Сервера и рабочие места пользователей, входящие в состав информационной системы, как это зачастую и бывает, находились в тех же сегментах сети, где находились сервера и рабочие станции, выполняющие другие системные и прикладные задачи. Сегмент рабочих мест состоял из различных видов и типов средств вычислительной техники – от высокопроизводительных полнофункциональных вычислительных машин до бездисковых терминальных станций.

Чтобы опыт был максимально интересным и показательным, пользовательский сегмент мы предельно усложнили. Во-первых, у некоторых пользователей информационной системы различались технологические процессы – кто-то осуществлял обработку данных как на сервере, так и локально, кто-то осуществлял обработку только на сервере, кому-то был необходим периодический доступ к Web-ресурсам внешних информационных систем. Во-вторых, парк вычислительной техники был разнообразен – арсенал включал как различные тонкие клиенты, так и полнофункциональные рабочие места, а некоторые персональные компьютеры были технически устарелыми и уже не могли вытянуть системные потребности современных операционных систем и программного обеспечения. При этом на одном и том же СВТ, в зависимости от рабочей смены, могут работать разные пользователи.

Ну и наконец, СВТ находятся не в отдельном изолированном помещении, а разбросаны по территории предприятия.

Оптимизация сетевой инфраструктуры

В первую очередь с целью оптимизации затрат на систему защиты, было выполнено сегментирование локальной вычислительной сети компании, т.к., как уже было упомянуто, сервера и рабочие станции ИСПДн находились в одном сетевом сегменте с другими АРМ и серверами (см. рисунок 1).

[1] URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21.

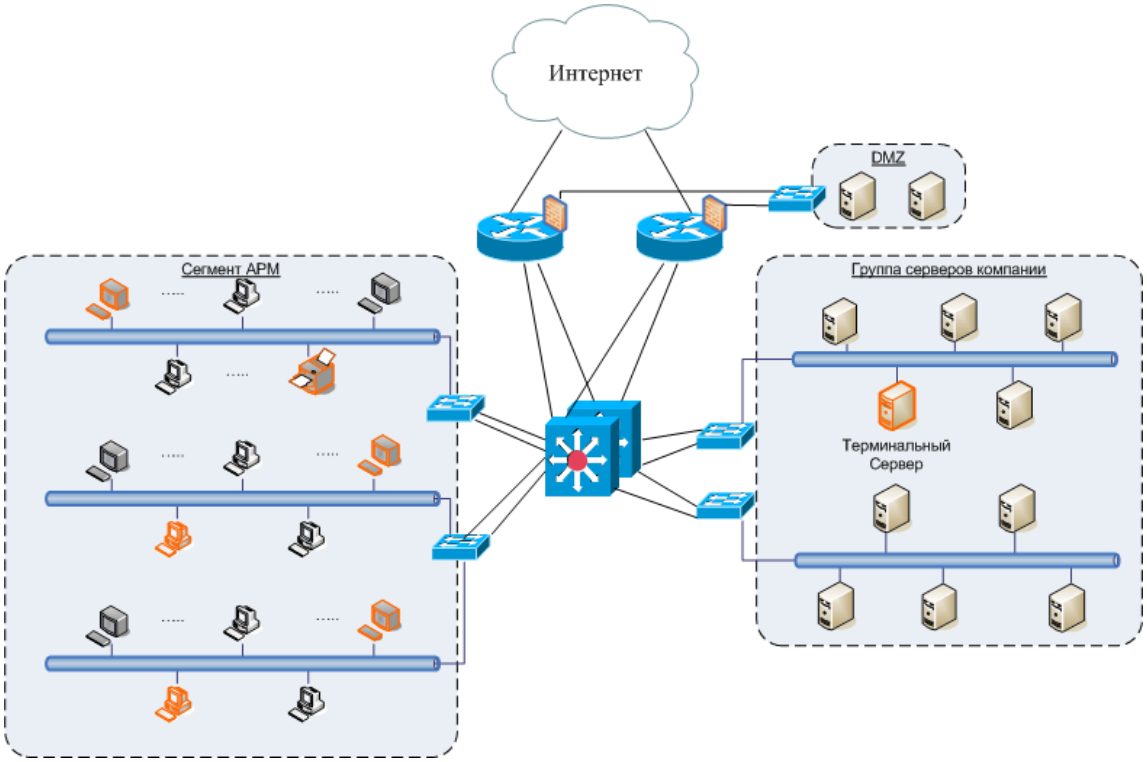

Рисунок 1 – Исходная структура ЛВС

В результате сервера и автоматизированные рабочие места, обрабатывающие персональные данные, были выделены в отдельные сетевые сегменты путем физической перекоммутации устройств, а функции контроля доступа в сегменты были возложены на сертифицированный межсетевой экран[2] (см. рисунок 2).

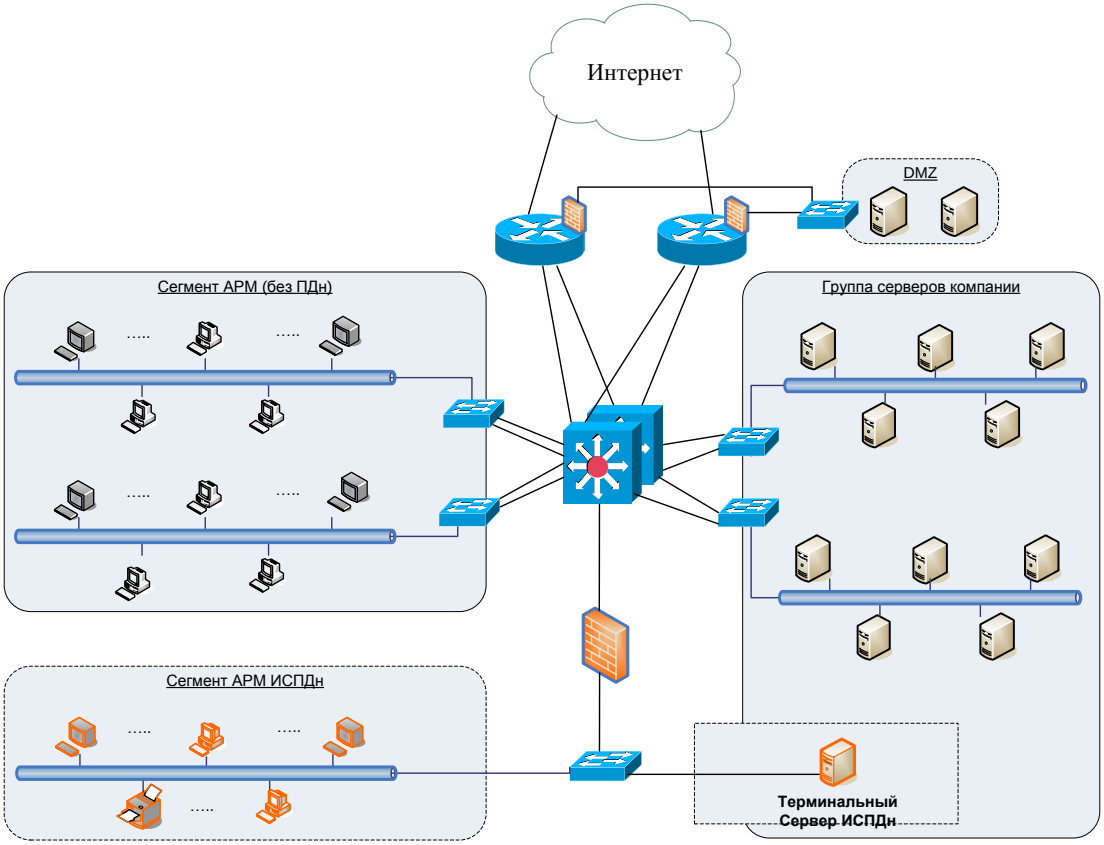

Рисунок 2 – Оптимизированная сетевая инфраструктура

[2] В описываемой системе применен межсетевой экран Stonesoft FW-105 FW/VPN. URL: http://www.ndm.net/firewall/pdf/105.pdf

Защита терминального сервера Citrix XenApp

При рассмотрении вопроса защиты системы терминального доступа обычно основное внимание уделяется защите терминальных серверов. Терминальные сервера являются критичными с точки зрения информационной безопасности ресурсами, и защищаться они должны очень тщательно. Поскольку у нас по исходным данным информационная система персональных данных второго уровня защищенности, на терминальном сервере необходимо обеспечить:

- доверенную загрузку операционной системы,
- идентификацию/аутентификацию пользователей;
- разграничение доступа пользователей к ресурсам сервера,
- регистрацию событий безопасности;
- антивирусную защиту системы.

Поэтому безо всяких колебаний терминальный сервер, входящий в состав информационной системы, был оснащен сертифицированным комплексом СЗИ от НСД[3], который реализует четыре первых перечисленных требования и сертифицированным антивирусным программным обеспечением[4], которое реализует антивирусную защиту системы.

Защита пользовательского сегмента

Для **полнофункциональных ПЭВМ** информационной системы, на которых осуществляется как локальная обработка персональных данных, так и удаленная на серверах в режиме терминального доступа, необходимо, так же, как и для серверов, обеспечить доверенную загрузку, разграничение доступа к ресурсам и антивирусную защиту рабочей станции. В качестве системы защиты таких рабочих мест идеально подошел набор, состоящий из СЗИ от НСД[5] и сертифицированных антивирусных средств[6].

Для отдельных пользователей, в задачи которых входит периодическая работа с Web-ресурсами информационных систем, было определено использовать инновационное и в то же время простое сертифицированное средство защиты класса СОДС (средство обеспечения доверенного сеанса связи)[7], реализующее концепцию доверенного сеанса связи. Доверенный сеанс связи – это период работы компьютера, в рамках которого обеспечивается доверенная загрузка ОС, организуется защищённое соединение (VPN), а также поддерживаются условия, достаточные для работы с электронной подписью. Образ операционной системы, которая будет загружаться с СОДС, формируется по заказу для каждой конкретной системы и включает только необходимые и достаточные для этой системы компоненты. Поскольку у нас работа с помощью СОДС осуществляется с терминальным сервером и с внешними ИС через Web-интерфейс, в состав образа ОС СОДС для нашей информационной системы был включен браузер и клиентское ПО Citrix Receiver.

При работе в режиме доверенного сеанса связи СВТ, к которому подключается СОДС, не оказывает никакого влияния на вычислительную среду пользователя, поэтому в качестве такого СВТ может использоваться что угодно (соответствующее минимальным требованиям, типа наличия USB-разъема не ниже 2.0). Мы используем в этом качестве одну из **ПЭВМ** и один из **тонких клиентов**, которые вне доверенного сеанса связи применяются другими пользователями по другим назначениям (см. таблицу 1). Важно, что взаимовлияние разных рабочих мест, организованных на одном СВТ при таком применении полностью исключено.

---

[3] В описываемой системе применен программно-аппаратный комплекс СЗИ НСД Аккорд-Win64 TSE. URL: http://www.accord.ru/acwin32.html.

[4] В описываемой системе применено ПО Dr.Web Server Security Suite. URL: http://products.drweb.ru/box/soho?lng=ru.

[5] В описываемой системе применены программно-аппаратные комплексы СЗИ НСД Аккорд-Win32 и Аккорд-Win64TSE. URL: http://www.accord.ru/acwin32.html.

[6] В описываемой системе применено ПО DR. Web для Windows. URL: http://products.drweb.ru/box/soho?lng=ru.

[7] В описываемой системе применено СОДС МАРШ!. URL: http://www.sodsmarsh.ru.

Более того, даже при работе в терминальном режиме исключена путаница (случайная или намеренная), подключился пользователь с СОДС или без него, так как аутентифицируется относительно Аккорда на терминальном сервере именно СОДС – уникальное аппаратное устройство.

Тонкие клиенты информационной системы являются ее такой же неотъемлемой частью, и для построения информационной системы с равным уровнем защищенности, необходимо обеспечивать и их защиту в том числе. Тонкие клиенты не являются точной копией полнофункциональных ПЭВМ и имеют ряд особенностей как архитектурных, так и функциональных, что впоследствии оказывает влияние на весь технологический процесс и, как следствие, на технологию защиты от процесса загрузки. Поэтому очевидно, что с точки зрения безопасности изменение процесса загрузки в первую очередь окажет влияние на процедуры контроля целостности. Сам принцип контроля должен оставаться прежним – необходимо убедиться в том, что происходит загрузка проверенной ОС с разрешенных носителей. В данном случае изменяются только объекты контроля, что в свою очередь приводит к изменению технологии контроля целостности.

В нашем арсенале технологий защиты оказалось решение и для такого случая – ПАК[8], реализующий технологию защищенной загрузки по сети ОС терминальной станции, хранящейся на мобильном устройстве. Организация загрузки ПО терминальных станций с помощью этого комплекса позволяет контролировать его целостность и обеспечивать оперативное администрирование прав, назначаемых пользователям в этих образах, так как образы защищаются кодами аутентификации, которые проверяются перед загрузкой на терминальную станцию аппаратным клиентским устройством.

Так же, как и в случае с СОДС, носителем терминального клиента является не СВТ, к которому подключается клиентское устройство, а само клиентское устройство.

Образ, прошедший проверку подлинности, в дальнейшем загружается в оперативную память терминальной станции. Загруженное ПО терминальной станции инициирует соединение с терминальным сервером. С использованием клиентских устройств пользователи терминальных станций осуществляют идентификацию в ПАК СЗИ НСД при входе на терминальный сервер (загрузочное клиентское устройство используется как аппаратный идентификатор).

Поэтому в тех случаях, когда на одном и том же тонком клиенте работают посменно пользователи с ПАК защищенной сетевой загрузки терминалов и с СОДС (см. таблицу 1), в журналах СЗИ НСД на терминальном сервере нет путаницы в том, как подключался пользователь.

Реализация запланированных мер защиты не потребовала изменения физического размещения СВТ из состава ИСПДн: Терминальный сервер остался в комнате Отдела тестирования, а АРМы – в комнате Отдела технической поддержки (см. таблицу 1 и рисунок 3). Единственное – в системе появились новые сущности – Сервер хранения и сетевой загрузки (СХСЗ) ПАК «Центр-Т» и АРМ «Центр» этого же комплекса. СХСЗ разместили на тонком клиенте вместе с терминальным сервером в Отделе тестирования, а АРМ «Центр» разворачиваем по мере необходимости (он требуется не часто) на одной из ПЭВМ в Отделе технической поддержки.

Состав и схема взаимодействия технических средств информационной системы приведены на рисунке 3.

[8] В описываемой системе применен ПАК Центр-Т. URL: http://www.proterminaly.ru/center_terminal.html.

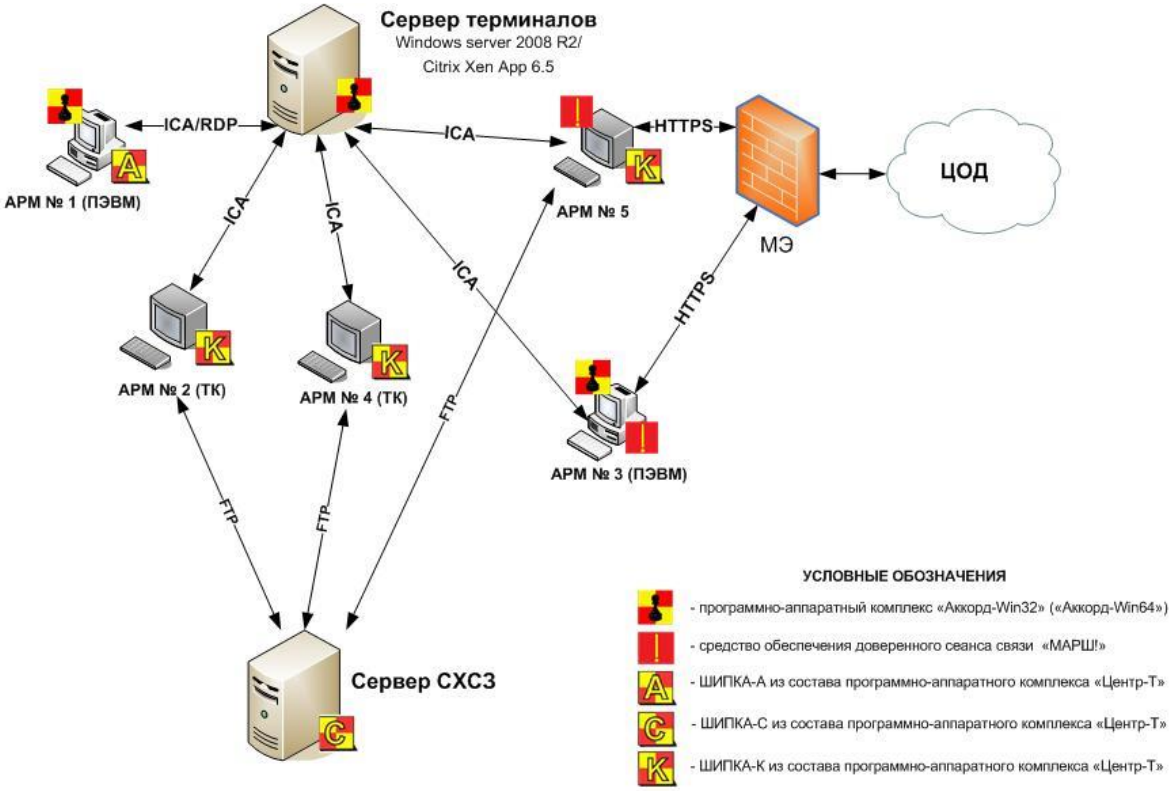

Рисунок 3 - Состав и схема взаимодействия технических средств ИСПДн

В таблице 1 приведено краткое описание технологических процессов обработки информации в информационной системе, а также пользователей, СВТ и СЗИ.

Таблица № 1 – Состав пользователей, СВТ и СЗИ в ИСПДн

	СВТ	Пользователь	Применяемые СЗИ	Технологический процесс
1.	*АРМ № 1* *(Полнофункциональная ПЭВМ)*	USER1	ПАК «Аккорд-Win32» Dr.Web	1 Работа на терминальном сервере с ПДн через Citrix Receiver (по протоколу ICA). 2 Локальная обработка ПДн
2.		Администратор АРМ «Центр»	ПАК «Центр-Т»	Администрирование ПАК «Центр-Т». Загрузка ПЭВМ с ШИПКИ-А (создание и инициализация образов терминальных станций в ПАК «Центр-Т»)
3.		Администратор ИСПДн	ПАК «Аккорд-Win32» Dr.Web	Администрирование терминального сервера через удаленный рабочий стол (по протоколу RDP).
4.	*АРМ № 2* *(Тонкий клиент)*	USER2	ПАК «Центр-Т»	Работа на терминальном сервере с ПДн через Citrix Receiver (по протоколу ICA). Загрузка терминальной станции осуществляется с загрузочного устройства ШИПКА-К (загружается образ начальной загрузки). Получение образа терминальной станции осуществляется по сети с СХСЗ
5.	*АРМ № 3* *(Полнофункциональная ПЭВМ)*	USER3	ПАК «Аккорд-Win32» Dr.Web	1 Работа на терминальном сервере с ПДн через Citrix Receiver (по протоколу ICA). 2 Локальная обработка ПДн
6.		USER6	СОДС «Марш!»	1 Работа на терминальном сервере с ПДн через Citrix Receiver (по протоколу ICA). 2 Работа с Web-ресурсами сторонних ИС. Загрузка ОС терминальной станции осуществляется с загрузочного устройства СОДС

	СВТ	Пользователь	Применяемые СЗИ	Технологический процесс
				«МАРШ!»
7.	*АРМ № 4* *(Тонкий клиент)*	USER4	ПАК «Центр-Т»	Работа на терминальном сервере с ПДн через Citrix Receiver (по протоколу ICA). Загрузка терминальной станции осуществляется с загрузочного устройства ШИПКА-К (загружается образ начальной загрузки). Получение образа терминальной станции осуществляется по сети с СХСЗ
8.	*АРМ № 5* *(Тонкий клиент)*	USER5	ПАК «Центр-Т»	Работа на терминальном сервере с ПДн через Citrix Receiver (по протоколу ICA). Загрузка терминальной станции осуществляется с загрузочного устройства ШИПКА-К (загружается образ начальной загрузки). Получение образа терминальной станции осуществляется по сети с СХСЗ
9.		USER7	СОДС «МАРШ!»	1 Работа на терминальном сервере с ПДн через Citrix Receiver (по протоколу ICA). 2 Работа с Web-ресурсами сторонних ИС. Загрузка ОС терминальной станции осуществляется с загрузочного устройства СОДС «МАРШ!»
10.	*Терминальный сервер*		ПАК «Аккорд-Win64» (TSE) Dr.Web	
11.	*СХСЗ* *(Тонкий клиент)*	Администратор СХСЗ	ПАК «Центр-Т»	Администрирование сервера Загрузка сервера осуществляется с загрузочного устройства ШИПКА-С

Заключение

После внедрения системы защиты успешно была проведена аттестация информационной системы. По результатам аттестационных испытаний был получен аттестат соответствия от 29.07.2015 № 561-15(К), удостоверяющий, что информационная система персональных данных, имеющая второй уровень защищенности, соответствует требованиям нормативной документации по безопасности информации. Теперь мы приглашаем всех желающих посетить нас и посмотреть своими глазами на эту систему. Таким образом каждый сможет лично убедиться в том, что выполнить необходимые требования по безопасности информации и аттестовать систему, построенную на «зоопарке» различных СВТ и технологий – вполне реальная задача. На наш взгляд, полученный опыт является показательным и может быть с известными уточнениями и дополнениями распространен на большое множество промышленных информационных систем разного типа, включая государственные информационные системы или системы частных организаций, в которых обрабатываются сведения конфиденциального характера, помимо персональных данных.