ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО

систем автоматизированного проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.5014-011 98 01-ЛУ

Программно-аппаратные комплексы средств защиты информации от несанкционированного доступа “АККОРД”

Подсистема распределенного аудита и управления «Аккорд-РАУ»

РУКОВОДСТВО ПО УСТАНОВКЕ

11443195.5014-011 98 01

Литера O_1

АННОТАЦИЯ

В документе приведен порядок установки программного обеспечения и аппаратной части подсистемы распределенного аудита и управления (ПРАУ), а также порядок их настройки в соответствии с конфигурацией технических и программных средств ПЭВМ (АС).

Перед установкой и эксплуатацией ПРА необходимо внимательно ознакомиться с комплектом эксплуатационной документации на комплекс, а также принять необходимые защитные организационные меры, рекомендуемые в документации. Применение защитных мер ПРА должно дополняться общими мерами технической безопасности.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Подсистема распределенного аудита и управления («Аккорд-РАУ») предназначена для оперативного наблюдения и управления рабочими станциями в составе ЛВС, защищенными ПАК СЗИ «Аккорд». В состав ПРАУ могут входить:

- автоматизированное рабочее место администратора безопасности информации (АРМ АБИ),
- рабочие станции и файловые сервера, функционирующие под управление 32-битных версий операционной системы Windows NT/2000/XP/2003/Vista/7/2008.
- рабочие станции и файловые сервера, функционирующие под управление 64-битных версий операционной системы Windows XP/2003/Vista/7/2008.

Все объекты ПРАУ должны быть защищены ПАК СЗИ «Аккорд». Функционирование ПРАУ базируется на использовании аппаратной и программной частей СЗИ «Аккорд».

2 ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ

Для установки программного обеспечения ПРАУ необходимо наличие установочного дистрибутива и идентификатора TouchMemory типа DS1996 (TM DS1996). На рабочих станциях должен быть установлены комплексы СЗИ НСД "Аккорд-NT/2000 v.3.0", или "Аккорд-Win32", или "Аккорд-Win64". На АРМ администратора обязательно должен быть установлен комплекс "АККОРД-АМДЗ" и драйвер для соответствующей версии контроллера. Установка СПО разграничения доступа на АРМ АБИ не является обязательной для функционирования «Аккорд-РАУ». Необходимость установки СПО определяется классом защиты АС. Система функционирует в составе локальных и распределенных сетей с использованием протоколов IPX, или TCP/IP. На рабочих станциях допускается использование динамического IP-адреса, на АРМ АБИ IP-адрес должен быть статическим.

Перед установкой ПРАУ необходимо добиться корректного функционирования драйвера аппаратной части комплекса. Версия драйвера должна быть 3.0.15 или выше.

3 ПОРЯДОК УСТАНОВКИ

Установка платы контроллера в свободный слот ПЭВМ производится в соответствии с "Руководством по установке" того типа контроллера, который входит в комплект поставки.

3.1 АРМ АБИ.

АРМ АБИ может функционировать на компьютере под управлением любой из версий ОС Windows 2000/ XP/ 2003/ Vista/7/2008.

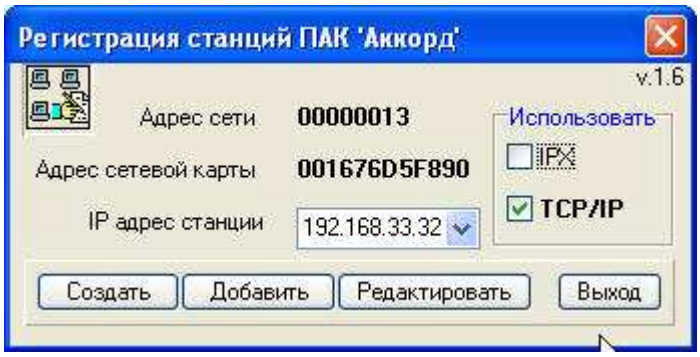
Порядок установки следующий:

- Установить контроллер «Аккорд-АМДЗ», зарегистрировать идентификатор главного администратора. После старта операционной системы и обнаружения нового устройства установить драйвер устройства с компакт-диска, который входит в состав комплекса «Аккорд-АМДЗ». Если компьютер предназначен для многопользовательской эксплуатации, то проинсталлировать СПО «Аккорд» согласно «Руководству по установке» СЗИ НСД. При установке СПО «Аккорд» на жестком диске создается каталог C:\ACCORD.NT (C:\ACCORD.x64 для 64-битных версий). Оптимальным с точки зрения надежности всей системы защиты является установка ПО АРМ АБИ на отдельном компьютере.
- Запустить с установочного диска «Аккорд-РАУ» программу setup.exe.

– Выбрать вариант установки "АРМ администратора безопасности информации" и указать каталог для установки. Если на компьютере установлено СПО «Аккорд», то имя каталога следует указать отличным от C:\ACCORD.NT (C:\ACCORD.x64 для 64-битных версий).

После установки программного обеспечения необходимо провести предварительную регистрацию участников информационного обмена. Взаимная аутентификация рабочих станций и АРМ АБИ выполняется с помощью специальных сетевых пакетов, подписанных ЭЦП. Генерация ключевых пар осуществляется специальной программой на основе последовательности случайных чисел, получаемой с аппаратного ДСЧ на плате контроллера «Аккорд». Носителем (контейнером) ключевой информации при начальной регистрации служит ТМ-идентификатор типа DS1996, или USB устройство ШИПКА 1.6, 1.7, 2.0.

Начинается процедура регистрации с запуска программы ACSETCON.EXE на АРМ АБИ.

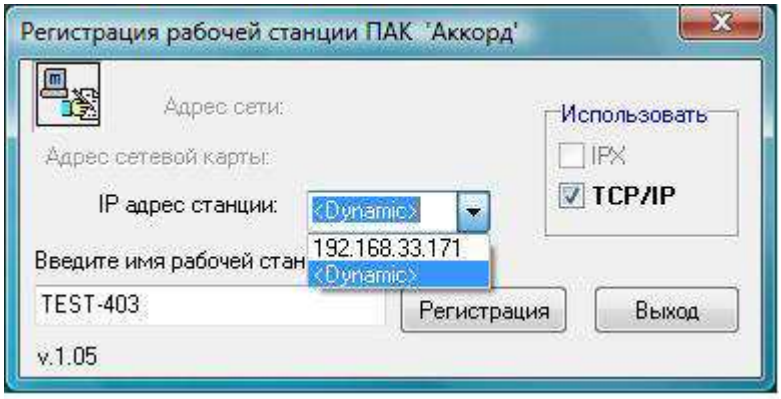


Выбрать пункт меню "Создать". На запрос ключа нужно присоединить идентификатор к съемнику информации. В идентификатор при этом заносится информация, которая будет использоваться при конфигурации рабочих станций. В соответствующем каталоге на жестком диске создается файл ACNODE.LST. В этом файле содержатся данные об АРМ АБИ. Внимание! ПО АРМ АБИ нельзя использовать на компьютере с динамической IP адресацией, когда новый адрес компьютер получает при каждом следующем подключении к серверу.

3.2 На рабочей станции Windows NT/2000/XP/2003/Vista/7/2008.

– Установить комплекс СЗИ НСД "Аккорд-NT/2000 v.3.0", или "Аккорд-Win32", или "Аккорд-Win64";
– Запустить с установочного диска «Аккорд-РАУ» программу setup.exe;
– Выбрать вариант установки "Клиент рабочей станции Windows". Файлы, необходимые для работы, будут скопированы в каталог C:\ACCORD.NT (C:\ACCORD.x64 для 64-битных версий).

Для регистрации рабочей станции запускается программа ACSETWS.EXE. В предложенном диалоге необходимо указать уникальное имя станции. В дальнейшем с АРМ АБИ станция будет доступна под этим именем. По умолчанию используется имя компьютера из системного реестра ОС и текущий IP адрес. Имя можно изменить, а в качестве IP адреса выбрать параметр <Dynamic>, если компьютер получает адрес динамически при подключении к серверу. Нажмите кнопку «Регистрация», предварительно выбрав тип сетевого протокола (IPX, TCP/IP, или два протокола одновременно).



На запрос ключа прикоснуться идентификатором к съемнику информации.

Если в идентификаторе достаточно свободной памяти для записи информации о станции, то становится доступной кнопка «Применить». После выбора этой кнопки удерживайте ТМ-идентификатор в контактном устройстве считывателя, пока в него записывается информация о рабочей станции и открытый ключ станции. После завершения записи нажмите повторно кнопку «Применить». Окно закрывается и в каталоге \ACCORD.NT (\ACCORD.x64) создается файл ACNODE.LST.

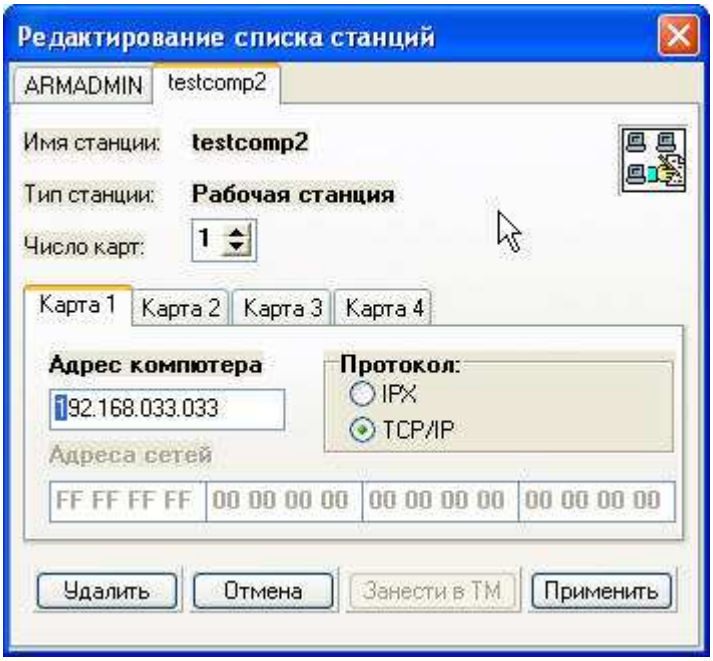
Если вся память в идентификаторе занята данными о рабочих станциях, то выводится сообщение «Свободно 0». В этом случае нужно добавить зарегистрированные станции на АРМ АБИ - память идентификатора очищается после переноса данных в файл.

Эту операцию необходимо произвести на каждой рабочей станции.

3.3 Регистрация рабочих станций и серверов на АРМ АБИ.

После регистрации рабочих станций возвращаемся на АРМ АБИ и в программе ACSETCON.EXE выбираем кнопку «Добавить».

На запрос ключа прикоснуться ТМ-идентификатором к съемнику информации. Информация о рабочих станциях и серверах будет считана из идентификатора и память идентификатора очищается.



После считывания из ТМ-идентификатора информация о рабочих станциях теперь собрана на АРМ АБИ. Выбор кнопки «Редактировать» позволяет просмотреть эту информацию.

На экран выводится информация о станциях:

- имя станции;
- открытый ключ станции;
- список номеров сетевых карт;
- номера сети для каждой сетевой карты (если в Вашей сети несколько серверов, то для каждого сервера номер сети будет индивидуальным).

В дальнейшем можно добавлять новые станции в список на АРМ АБИ с помощью такой же процедуры.

Объем идентификатора DS1996 позволяет хранить данные о 31 рабочей станции и их открытые ключи. Если Вы уже зарегистрировали 31 станцию, то при попытке зарегистрировать следующую выдается сообщение: "Свободно 0". Если в сети остались незарегистрированные станции, то следует добавить список на АРМ АБИ и после очистки памяти идентификатора провести регистрацию остальных рабочих станций.

4 Запуск подсистемы РАУ.

После регистрации рабочих станций на АРМ АБИ следует активизировать сетевой клиент РАУ. Для этого на каждой рабочей станции Windows в сеансе пользователя с правами администратора ОС нужно выполнить команду: ACWS32NT.EXE –INSTALL.

Обратите внимание: –INSTALL – это параметр, его нужно писать через пробел после имени программы и заглавными буквами.

В подсистеме разграничения доступа комплексов "Аккорд-NT/2000 v.3.0", или "Аккорд-Win32", или "Аккорд-Win64" в программе – редакторе ПРД регистрируем нового пользователя в группе «Администраторы» и присваиваем ему тот же идентификатор и пароль, который запускает АРМ АБИ. Это необходимо для получения доступа к списку пользователей и журналам в аппаратной части комплекса. Обычным пользователям в список ПРД добавляем сетевой ресурс – имя компьютера АРМ АБИ в сети и импортируем ПРД из файла acws32.prd. В опциях пользователей включаем флаг «Полный доступ для АРМ АБИ». Выполняем перезагрузку рабочих станций.

Для нормального функционирования системы необходимо синхронизировать содержимое ACNODE.LST на всех рабочих станциях. Для этого необходимо выполнить следующее:

- на АРМ АБИ запустить программу ACCONNET.EXE, предъявить идентификатор и ввести пароль администратора;
- убедиться, что в списке в левой части экрана присутствуют все зарегистрированные рабочие станции;
- отметить станции и выбрать пункт меню "Разослать список станций".

СИСТЕМА УСТАНОВЛЕНА.

5 Рабочий режим функционирования РАУ.

5.1 АРМ АБИ:

Все функции АРМ АБИ реализуются программой ACCONNET.EXE (см. «Руководство администратора»).

5.2 Windows NT/2000/XP/2003/Vista/7/2008.

Клиент РАУ стартует автоматически.

ВНИМАНИЕ! Для успешного функционирования всех функций «Аккорд-РАУ» внутреннее ПО контроллеров АМДЗ на АРМ АБИ и рабочих станциях должно быть выполнено по одному ТУ (у контроллеров с внутренним ПО по требованиям ФСБ заводской номер начинается с 519-). Заводской номер указывается в формуляре.

6 Отключение подсистемы РАУ.

В диспетчере служб остановить службу AcWS32nt.
В режиме командной строки выполнить команду ACWS32NT.EXE –REMOVE.

7 Использование усиленной аутентификации для сети Microsoft.

7.1 АРМ АБИ.

В файле CAUTH32.INI установить в секции Options параметр MSNetAuth=Yes.

7.2 Рабочая станция Windows 2000/XP.

Выполнить следующие действия:
Войти в систему как Администратор локальной станции.
Из папки Auth_2k скопировать файл acxauth.sys в папку Windows\System32\Drivers и запустить программу regini.exe, с параметром acxauth.ini.