

ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО



систем автоматизированного
проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.4012-019 98 02-ЛУ

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа “АККОРД-NT/2000” (версия 3.0)

РУКОВОДСТВО ПО УСТАНОВКЕ

11443195.4012-019 98 02

Литера О₁

АННОТАЦИЯ

Установка комплекса СЗИ НСД "Аккорд-NT/2000" v.3.0 (ТУ 4012-019-11443195-02) и его настройка с учетом особенностей политики информационной безопасности, принятой на объекте информатизации, осуществляется, как правило, специалистами по защите информации организации (предприятия, фирмы и т.д.) в соответствии с требованиями эксплуатационной документации на комплекс.

В документе приведен порядок установки программно-аппаратного комплекса средств защиты информации от несанкционированного доступа (СЗИ НСД) "Аккорд-NT/2000" v.3.0.

Перед установкой и эксплуатацией комплекса необходимо внимательно ознакомиться с комплектом эксплуатационной документации на комплекс, а также принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных мер комплекса "Аккорд" должно дополняться общими мерами технической безопасности.

СОДЕРЖАНИЕ

1. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ОРГАНИЗАЦИОННЫЕ МЕРЫ, НЕОБХОДИМЫЕ ДЛЯ ПРИМЕНЕНИЯ КОМПЛЕКСА	4
1.1. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ.....	4
1.2. ОРГАНИЗАЦИОННЫЕ МЕРЫ.....	4
2. ПОРЯДОК УСТАНОВКИ КОМПЛЕКСА.....	5
2.1. УСТАНОВКА КОМПЛЕКСА СЗИ НСД "АККОРД-АМДЗ"	5
2.2. УСТАНОВКА СПО РАЗГРАНИЧЕНИЯ ДОСТУПА "АККОРД-NT/2000" НА ЖЕСТКИЙ ДИСК	5
2.2.1. Основные параметры настройки комплекса.....	6
2.2.2. Дополнительные параметры настройки комплекса.	9
2.2.3. Использование антивирусного ядра.	19
2.2.4. Особенности настройки комплекса "Аккорд-NT/2000" при использовании SATA жестких дисков, или RAID контроллеров с динамическим подключением томов.	21
2.3. АКТИВИЗАЦИЯ ПОДСИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА.....	22
2.4. УСТАНОВКА ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА (ПРД) ДЛЯ ПОЛЬЗОВАТЕЛЕЙ.....	22
2.5. УСТАНОВКА СЗИ «АККОРД» НА ТЕРМИНАЛЬНОМ СЕРВЕРЕ	22
2.6. ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ПСКЗИ ШИПКА В КАЧЕСТВЕ ПЕРСОНАЛЬНОГО ИДЕНТИФИКАТОРА	28
3. СНЯТИЕ СРЕДСТВ ЗАЩИТЫ КОМПЛЕКСА "АККОРД-NT/2000".....	32

ВНИМАНИЕ!

Перед началом установки комплекса "Аккорд- NT/2000" рекомендуется подробно ознакомиться с эксплуатационной документацией на комплекс, прежде всего с "Описанием применения" (11443195.4012-019 31 02) и настоящим руководством.

1. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ОРГАНИЗАЦИОННЫЕ МЕРЫ, НЕОБХОДИМЫЕ ДЛЯ ПРИМЕНЕНИЯ КОМПЛЕКСА

1.1. Технические требования

Для установки комплекса СЗИ НСД "Аккорд-NT/2000" в. 3.0 требуется следующий минимальный состав технических и программных средств:

- установленная на операционная система Windows NT/2000/XP/2003/Vista;
- объем свободного дискового пространства для установки программных средств комплекса – не менее 20 Мб;
- наличие на HDD и CD ROM для установки СПО разграничения доступа;
- наличие свободного слота на материнской плате для установки контроллера комплекса "Аккорд-АМДЗ". PCI/PCI-X – для контроллеров "Аккорд-5mx" и "Аккорд–5.5", PCI Express для контроллера "Аккорд–5.5e";

При применении комплекса "Аккорд-NT/2000" в. 3.0 количество пользователей, регистрируемых на одном СВТ, не должно превышать 126 человек, так как объем энергонезависимой памяти контроллеров комплекса СЗИ НСД "Аккорд-АМДЗ" позволяет хранить данные на такое количество учетных записей. Данное ограничение не распространяется на подсистему защиты терминального сервера, т. к. пользователи удаленного рабочего стола регистрируются только в БД программной части комплекса.

1.2. Организационные меры^{*}

Для эффективного применения комплекса и поддержания необходимого уровня защищенности и информационных ресурсов **необходимы**:

- физическая охрана СВТ и его средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса СЗИ НСД;
- наличие администратора безопасности информации (супервизора) – привилегированного пользователя, имеющего особый статус и абсолютные полномочия. Администратор БИ планирует мероприятия по защите информации на предприятии (учреждении, фирме и т. д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует установку комплекса в СВТ, эксплуатацию и контроль за правильным использованием СВТ с внедренным комплексом "Аккорд-NT/2000", осуществляет периодическое тестирование средств защиты комплекса. Более подробно обязанности администратора БИ по применению комплекса изложены в Руководстве администратора (11443195.4012-019 90 02).
- использование в СВТ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в ГСЗИ.

^{*} Более подробно организационные меры защиты информации при применении комплекса приведены в "Руководстве администратора" (11443195.4012-019 90 02), "Руководстве оператора (пользователя)", 11333195.4012-019 34 02.

2. ПОРЯДОК УСТАНОВКИ КОМПЛЕКСА

Установка программно-аппаратного комплекса СЗИ НСД "Аккорд- NT/2000" v.3.0 (ТУ 4012-019-11443195-02) включает три основных этапа:

1. Установку в СВТ аппаратной части комплекса – комплекса СЗИ НСД "Аккорд-АМДЗ" (ТУ 4012-006-11443195-97 03) его настройку с учетом конфигурации технических и программных средств, в том числе, регистрацию администратора безопасности информации (или нескольких администраторов) и пользователей. Документация, необходимая для установки и администрирования «Аккорд-АМДЗ», находится на дистрибутивном носителе в папке /AMDZ/doc.

2. Установку в составе ОС драйвера для устройства «Аккорд-АМДЗ». Для РСИ контроллеров установка драйвера выполняется стандартным образом, только размещение указывается в папке /Drivers/ на дистрибутивном носителе, который входит в состав комплекса "Аккорд-NT/2000".

3. Установку на жесткий диск специального программного обеспечения разграничения доступа с дистрибутивного носителя.

4. Назначение правил разграничения доступа (ПРД) для пользователей в соответствии с политикой информационной безопасности, принятой в организации и активизацию подсистемы разграничения доступа с помощью программы настройки комплекса (ACSETUP.EXE).

2.1. Установка комплекса СЗИ НСД "Аккорд-АМДЗ"

ВНИМАНИЕ!

Перед установкой тщательно изучите эксплуатационную документацию на комплекс СЗИ НСД "Аккорд-АМДЗ"

Установка и настройка аппаратной части СЗИ НСД "Аккорд-АМДЗ" из состава комплекса "Аккорд-NT/2000" v.3.0 производится с учетом модификации комплекса в соответствии с "Руководством по установке" (11443195.4012-006 98 03), поставляемым в составе эксплуатационной документации на комплекс "Аккорд-АМДЗ".

2.2. Установка СПО разграничения доступа "Аккорд-NT/2000" на жесткий диск

Установка СПО на жесткий диск СВТ осуществляется в следующей последовательности:

1. После установки "Аккорд-АМДЗ" загрузить ОС с правами Администратора. Установить драйвер нового устройства из папки \Drivers\ которая находится на компакт-диске, поставляемом в составе комплекса. Установку драйвера выполнять в зависимости от типа контроллера АМДЗ и типа ОС.

2. Запустить находящуюся на диске программу SETUP.EXE из папки ACNT2000.

3. Выбрать диск и каталог для установки ПО комплекса. По умолчанию установка выполняется в папку C:\Accord.NT, но администратор может выбрать другие варианты. Программа создаст на заданном логическом диске папку C:\ACCORD.NT (или имя, заданное администратором) со всеми необходимыми подкаталогами и скопирует туда программное обеспечение. В подкаталог DOC копируется комплект эксплуатационной документации.

На данном этапе в составе ОС не производится никаких изменений, кроме создания каталогов или файлов на жестком диске.

4. Перезагрузить и запустить редактор прав доступа – программу ACED32.EXE из каталога C:\ACCORD.NT для синхронизации файла ПРД подсистемы разграничения доступа комплекса "Аккорд-NT/2000" со списком пользователей, который находится в контроллере комплекса "Аккорд-АМДЗ".

5. Назначить ПРД в соответствии с принятой политикой информационной безопасности и полномочиями пользователей. Описание программы и порядок ее применения приведен в документе "Установка правил разграничения доступа. Программа ACED32. Руководство пользователя" (11443195.4012-019 97 02), в составе эксплуатационной документации на комплекс "Аккорд-NT/2000" v. 3.0.

6. Провести активизацию подсистемы разграничения доступа комплекса. Для этого необходимо запустить программу ACSETUP.EXE из каталога C:\ACCORD.NT.

При этом осуществляется авторизация администратора БИ (запрашивается идентификатор и пароль администратора БИ). Если проверка прошла успешно, то на экране появляется окно для настройки подсистемы разграничения доступа комплекса, показанное на Рис. 1.

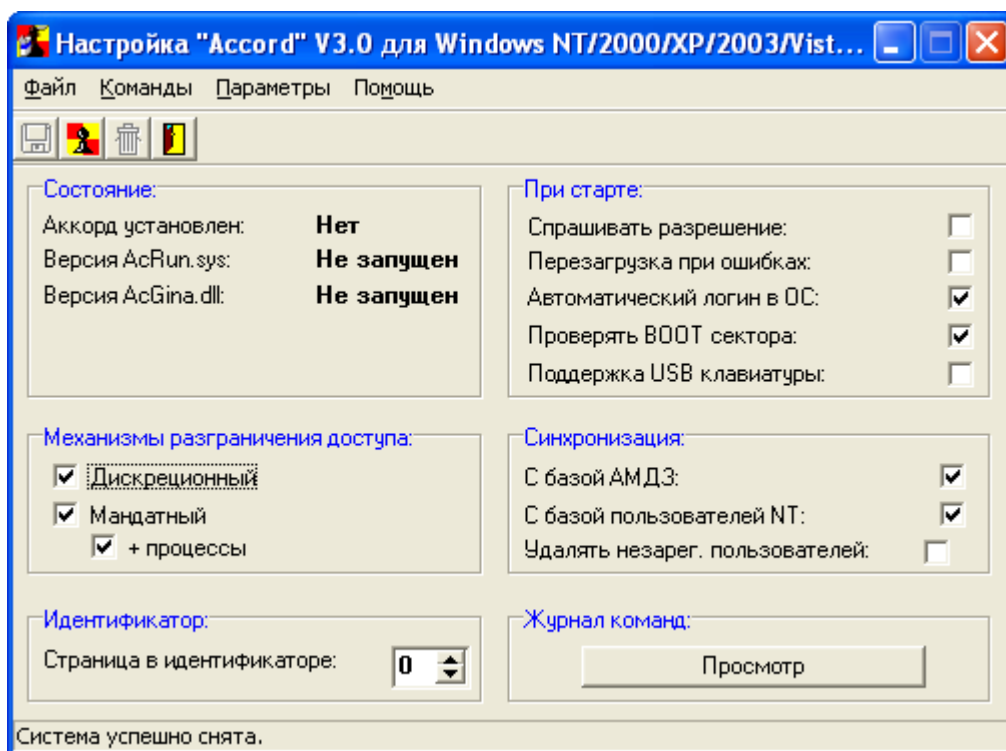


Рис. 1. Главное окно программы настройки комплекса «Аккорд-NT/2000»

2.2.1. Основные параметры настройки комплекса

В правой части окна размещено поле "**При старте**", предназначенное для задания режимов загрузки "монитора разграничения доступа" – программы ACRUN.SYS. Выбор режима загрузки осуществляется путем установки/снятия соответствующего флага:

"Спрашивать разрешение" – при включении этого режима в момент загрузки ACRUN.SYS выводится запрос и можно отказаться от запуска программы. **Этот режим допустим только на период тестирования системы.**

"Перезагрузка при ошибках" – если установлен этот флаг, то при обнаружении ошибок (например, пользователь не зарегистрирован в базе данных, выявлены изменения в контролируемых файлах и т.д.) происходит принудительная перезагрузка. **Это основной режим функционирования системы разграничения доступа!** В том случае, когда установлен такой режим работы системы защиты, и возникает ошибка, не позволяющая продолжить загрузку, для администратора предусмотрен резервный механизм отключения старта монитора безопасности. Действует он только для пользователя «Гл. Администратор» и для его корректной работы в настройке аппаратной части комплекса в параметре «Результаты И/А» должны быть включены первые пять флагов. Если эти требования соблюдены, то в начале загрузки ОС после корректной идентификации в аппаратной части администратор может нажать клавишу с буквой S и

остановить загрузку монитора безопасности. Нажимать клавишу следует в тот момент, когда на экран в текстовом режиме начинается вывод сообщений СЗИ «Аккорд».

"Автоматический логин в ОС" - при включении этого режима в момент загрузки модуль ACGINA.DLL получает информацию о пользователе, который был идентифицирован контроллером комплекса "Аккорд-АМДЗ". При этом вход в систему может осуществляться двумя способами:

- контроллер комплекса "Аккорд-АМДЗ" передает подсистеме доступа имя пользователя. Первые четыре флага установлены в разделе «Результаты I/A» параметров пользователя. В этом случае при логине в ОС требуется ввести с клавиатуры пароль пользователя. Имя пользователя изменить нельзя.
- контроллер комплекса "Аккорд-АМДЗ" передает подсистеме доступа имя и пароль пользователя (первые пять флагов установлен в разделе "Результаты I/A" в настройках контроллера). В этом случае при логине в ОС ввода пароля не требуется.

Если СВТ подключено к сети, то у пользователя есть возможность выбрать имя домена или сервера, к которому он может получить доступ, даже если включен параметр «Автологин». Для этого администратору перед активизацией подсистемы разграничения доступа нужно включить расширенный режим входа в систему (кнопка «Параметры» в стандартном окне запроса имени и пароля пользователя).

"Проверить BOOT сектора" - в момент загрузки ядра ОС модуль AcRun.SYS производит запись в журнал регистрации событий СЗИ «Аккорд». Операционная система Windows определяет факт записи на диск до начала «официального» сеанса работы пользователя и выставляет флаг некорректно заверщенного сеанса. Чтобы при каждой не запускался перезагрузке chkdsk, AcRun.sys восстанавливает исходное значение загрузочной записи. По умолчанию флаг включен. Отключать его следует только в том случае, если какой-либо системный модуль дополнительно проверяет boot записи логических разделов диска.

"Поддержка USB клавиатуры" – этот флаг необходимо включать, если на Вашем компьютере используется USB клавиатура или мышь. В этом случае при старте операционной системы в нижней части окна появляется запрос, который позволяет изменить параметры загрузки монитора разграничения доступа. Действовать эти настройки будут только в том случае, если установлен флаг «Спрашивать разрешение». Такой алгоритм работы приходится использовать потому, что в момент старта модуля AcRun.sys поддержка USB клавиатуры из системного BIOS уже отключена, а драйвер из состава ОС еще не загружен. Кроме того, установка этого флага обеспечивает корректную блокировку USB клавиатуры и мыши при работе хранителя экрана.

Поле **"Синхронизация"** определяет режимы синхронизации базы данных пользователей. Флаг **"С базой АМДЗ"** определяет режим, при котором параметры пользователя из контроллера считываются в базу данных редактора ПРД. При выходе из редактора ПРД выполняется синхронизация с базой данных контроллера.

Флаг **"С базой пользователей NT"** определяет режим, при котором программа-редактор добавляет пользователей СЗИ «Аккорд» в базу операционной системы. Этот флаг необходим, если включен режим "Автоматический логин в ОС". В противном случае пользователь не сможет войти в Windows.

Примечание: Учетная запись «Гл.администратор» автоматически синхронизируется с системной учетной записью «Администратор» в русской версии Windows, или с записью «Administrator» в английской версии. Если в составе ОС учетная запись «Администратор» заблокирована, то СЗИ «Аккорд» создает запись Supervisor и включает ее в группу «Администраторы».

"Удалять незарегистрированных пользователей" – установка этого дополнительного флага определяет способ синхронизации пользователей СЗИ «Аккорд» с базой ОС Windows. Если флаг не установлен, то пользователи СЗИ просто добавляются в базу пользователей ОС. Если флаг установлен, то в базе пользователей операционной системы останутся ТОЛЬКО пользователи СЗИ «Аккорд».

При установленной СЗИ «Аккорд» в автоматизированной системе (компьютер + ПО) появляются 3 базы пользователей:

- база в контроллере АМДЗ;
- база в составе СПО NT/2000 (файл Accord.AMZ);
- база учетных записей в составе ОС.

Есть 2 флага отвечающих за синхронизацию этих баз:

- флаг "синхронизация с АМДЗ". Если установлен этот флаг, то при старте редактора ПРД ACED32 считываются пользователи из АМДЗ. Если пользователь заведен в программе администрирования АМДЗ, то он автоматически заносит в ACCORD.AMZ с теми ПРД, которые установлены как общие параметры группы, в которую включен пользователь. Если в файле ACCORD.AMZ есть пользователь, но его нет в базе контроллера АМДЗ, то такой пользователь удаляется из ACCORD.AMZ. При завершении работы редактора Aced32 с сохранением изменений файл ACCORD.AMZ полностью синхронизируется с базой пользователей в контроллере АМДЗ, т.е. такие параметры как имя пользователя, идентификатор, пароль, параметры пароля, временные ограничения, результаты И/А, полностью идентичны.
- флаг "синхронизация с NT". Если установлен этот флаг, то при выходе из редактора Aced32 созданные пользователи заносятся в базу пользователей ОС. В этот момент проверяется флаг 'Удалять незарегистрированных пользователей'. Если он установлен, и если в ОС зарегистрированы пользователи, не существующие в Accord.AMZ, то эти пользователи удаляются из базы NT. При этом администратор должен позаботиться о том, чтобы политики парольной защиты (минимальная длина, набор символов, срок действия) совпадали в настройках ОС и СЗИ «Аккорд».

Таким образом, если включены 3 флага синхронизации: "с АМДЗ" + "с NT" + "Удалять незарегистрированных пользователей", то все 3 базы идентичны по именам пользователей и паролям. Если флаги не установлены, то возможны случаи, когда в одних базах будет больше/меньше пользователей, чем в других, а пароли одного и того же пользователя будут различны для включения компьютера (в АМДЗ) и для загрузки ОС.

В любом случае СПО «Аккорд NT/2000» работает со своей базой (Accord.AMZ). Вы можете установить режимы синхронизации, а можете отдельно завести пользователя в АМДЗ и в редакторе Aced32 (даже с разными паролями), при этом пользователь всегда идентифицируется своим идентификатором.

Если все пользователи работают в домене, и локальный вход не нужен (или вообще запрещен), то синхронизацию с базой NT можно смело убирать. В настройках комплекса нужно включить флаги "Использовать полное имя в учетных записях NT" и "Автологин", а в редакторе ПРД в поле "Полное имя" ввести <доменное имя юзера>@<имя домена>. Единственное ограничение – пароль нужно менять, когда пользователь уже авторизовался на домене через Ctrl-Alt-Del и кнопку "Смена пароля".

Поле **“Механизмы разграничения доступа”** определяет те методы разграничения доступа, которые будут использоваться при реализации политики безопасности. Подробнее см. документ “Установка правил разграничения доступа. Программа ACED32”.

В поле **“Идентификатор”** только один параметр – **“Страница в идентификаторе”**. По умолчанию он установлен в 0. Изменять этот параметр КАТЕГОРИЧЕСКИ НЕ РЕКОМЕНДУЕТСЯ! В эту и следующую страницу памяти идентификатора записывается секретный ключ пользователя при его регистрации. Изменение этого параметра приведет к тому, что ранее зарегистрированные идентификаторы будут восприниматься системой защиты как недопустимые. Изменение этого параметра возможно, если используется ПО сторонних производителей, которое записывает свою информацию в те же страницы памяти. После изменения этого параметра ВСЕ используемые идентификаторы должны быть перерегистрированы с генерацией нового секретного ключа пользователя.

2.2.2. Дополнительные параметры настройки комплекса.

В пункте меню “**Параметры**” можно изменить дополнительные параметры и настройки СЗИ “Аккорд” (Рис. 2.).

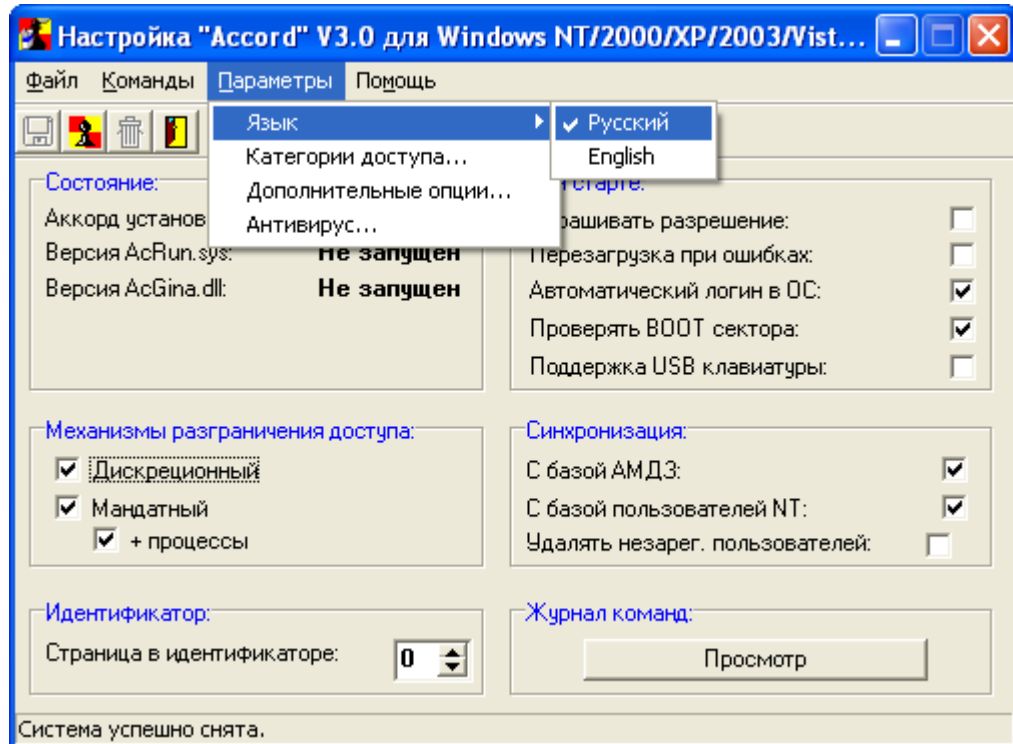


Рис. 2. Дополнительные параметры и настройки.

Пункт меню “**Язык**” позволяет выбрать язык, на котором будут выводиться сообщения программ, входящих в состав комплекса «Аккорд NT/2000». При старте программы настройки комплекса устанавливается язык, соответствующий основному языку операционной системы. Если у Вас установлена английская версия Windows NT/2000/XP, то программа начинает работу на английском языке. Если в английской версии ОС установлена поддержка русского языка, то после старта программы в пункте “Параметры”-”Язык” можно выбрать “Русский” для вывода сообщений на русском языке.

Пункт меню “**Категории доступа**” позволяет редактировать список категорий доступа, который используется в реализации мандатного механизма разграничения доступа (Рис.3.).

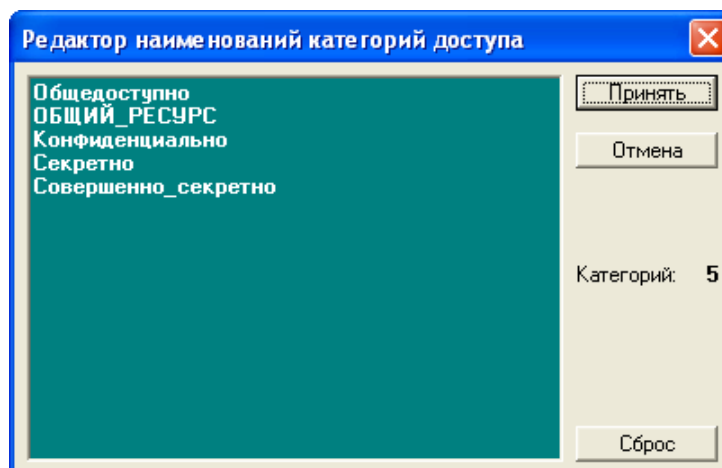


Рис. 3. Редактирование списка категорий доступа.

При установке СЗИ «Аккорд» в списке уже содержатся пять категорий доступа. Администратор безопасности информации может менять количество и наименование категорий доступа в соответствии с принятой политикой защиты информации. В подсистеме мандатного доступа допускается использование до 8 категорий доступа.

Пункт меню **«Дополнительные опции»** открывает доступ к настройкам расширенных функций и параметров системы защиты (Рис. 4.).

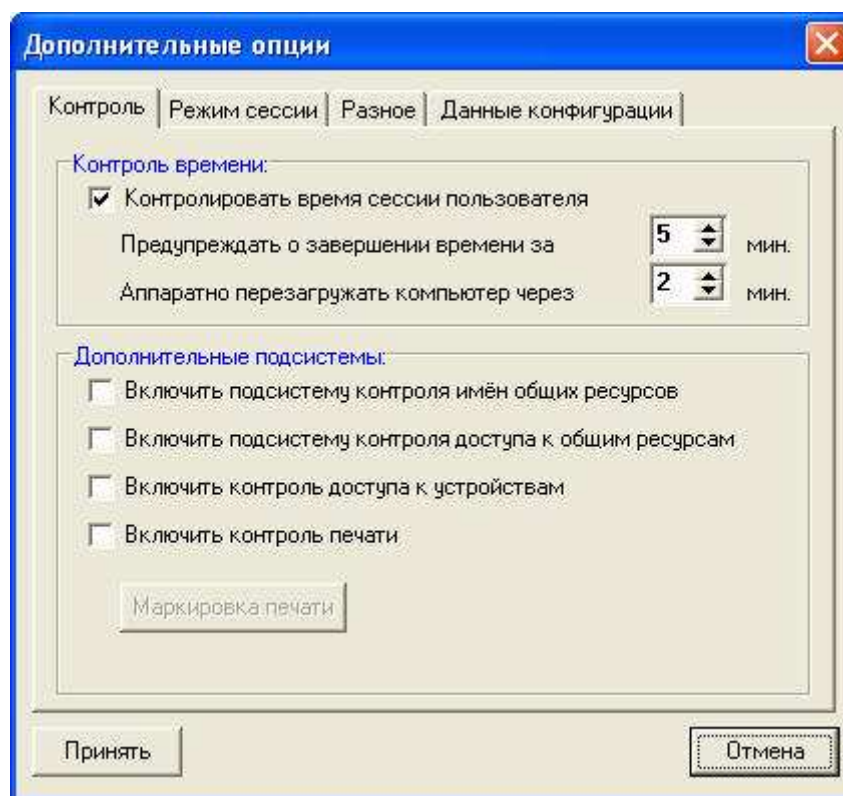


Рис. 4. Дополнительные параметры в настройке СЗИ.

Дополнительные опции сгруппированы по функциональному назначению и выбираются нажатием левой кнопки мыши на соответствующей закладке.

Закладка **«Контроль»** содержит две группы параметров: «Контроль времени» и «Дополнительные подсистемы».

«Контроль времени» определяет режим принудительного завершения сеанса пользователя, если в редакторе ПРД установлены соответствующие ограничения по времени работы. Подробнее см. документ «Установка правил разграничения доступа. Программа ACED32». Если контроль времени включен, то администратор задает интервал в минутах до завершения сеанса, когда пользователю выводится предупреждение об окончании работы. Второй параметр – это интервал времени в минутах, через который аппаратно перезагружается компьютер после попытки выполнить перезагрузку обычным способом. Эта процедура может потребоваться, если какое-либо приложение «зависло» и не отвечает на системные запросы.

Группа параметров **«Дополнительные подсистемы»** отвечает за активизацию функций СЗИ «Аккорд», которые не относятся непосредственно к разграничению доступа, но определяют режимы работы защищенной рабочей станции в составе сети (автоматизированной системы).

«Включить подсистему контроля имён общих ресурсов» – установка данного параметра активизирует (после перезагрузки) процедуру контроля заданных в редакторе ПРД общих ресурсов, т.е. устройств, папок и файлов данного компьютера, предоставленных в общий доступ пользователям сети. Подробнее см. документ «Установка правил разграничения доступа. Программа ACED32» пункт «Установка фиксированных сетевых имен ресурсов общего пользования».

“Включить подсистему контроля доступа к общим ресурсам” – установка данного параметра активизирует (после перезагрузки) процедуру контроля доступа к ресурсам данного компьютера из сети. Предыдущей параметр регламентирует выделение ресурсов данного компьютера в общий доступ с фиксированными именами, а данный флаг включает драйвер, который разрешает, или запрещает доступ из внешней сети к ресурсам компьютера на время сеанса работы конкретного пользователя. Режим контроля определяется опцией *«Запрет доступа к общим ресурсам»* в опциях настройки пользователя. Подробнее см. документ “Установка правил разграничения доступа. Программа ACED32” пункт «Установка дополнительных опций работы пользователя».

“Включить контроль доступа к устройствам” – установка данного параметра активизирует подсистему контроля устройств. После выхода из программы настройки с сохранением данного изменения в программе – редакторе ПД в списке объектов для установки атрибутов доступа появляется группа «Устройства», т.е. объект вида \DEVICE\PARALLELO, \DEVICE\SERIAL0, \DEVICE\SYSAUDIO и др. Включение такого объекта в список ПД означает запрет на доступ к этому объекту, в списке атрибутов доступна только регистрация попыток доступа на чтение, или запись. Проверка доступа выполняется на уровне файловых операций ввода-вывода, поэтому мышь на Com1 будет работать через свой драйвер, даже если в ПД запрещен доступ к последовательному порту, а вот модем, или программа обмена файлами с другим компьютером получают отказ в доступе.

“Включить контроль печати” – установка данного параметра активизирует подсистему контроля и маркировки печати.

“Маркировка печати” – данная кнопка предназначена для вызова программы настройки информации, выводимой на маркированный печатный документ. Режим контроля и маркировки печатных документов определяется опцией *«контроль печати»* в настройках опций пользователя. Подробнее см. документ “Установка правил разграничения доступа. Программа ACED32” пункт «Установка опций настройки».

В программе настройки маркировки документов параметры сгруппированы в несколько секций, которые открываются при выборе соответствующей закладки.

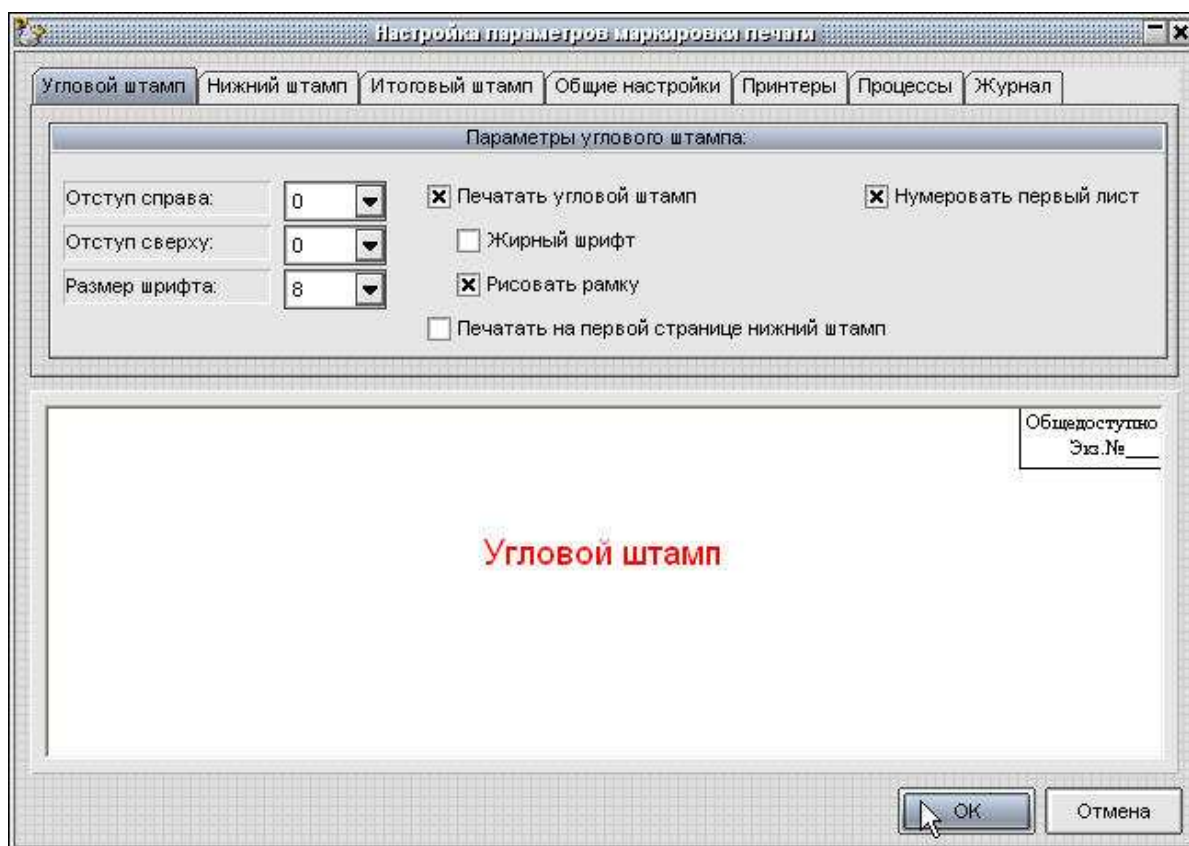


Рис. 5. Настройка маркировки первой страницы документа.

Закладка «Угловой штамп» (Рис. 5) определяет вид информации, выводимой на первой странице маркируемого документа. Параметры «Отступ справа» и «Отступ сверху» определяют положение углового штампа на первой странице. «Размер шрифта» соответствует принятому в ОС Windows типоразмеру шрифтов. Параметры «Жирный шрифт» и «Рисовать рамку» очевидны и не требуют дополнительной детализации. Параметр «Печатать на первой странице нижний штамп» определяет способ маркировки, при котором на первой странице кроме верхнего углового штампа печатается еще информация нижнего колонтитула, которая выводится на всех страницах документа, но в отдельных случаях не требуется именно на первой странице. Параметр «Нумеровать первый лист» показывает, будет ли печататься на первом листе номер страницы.

Закладка «Нижний штамп» (Рис. 6) определяет вид информации, выводимой в нижней части страницы маркируемого документа.

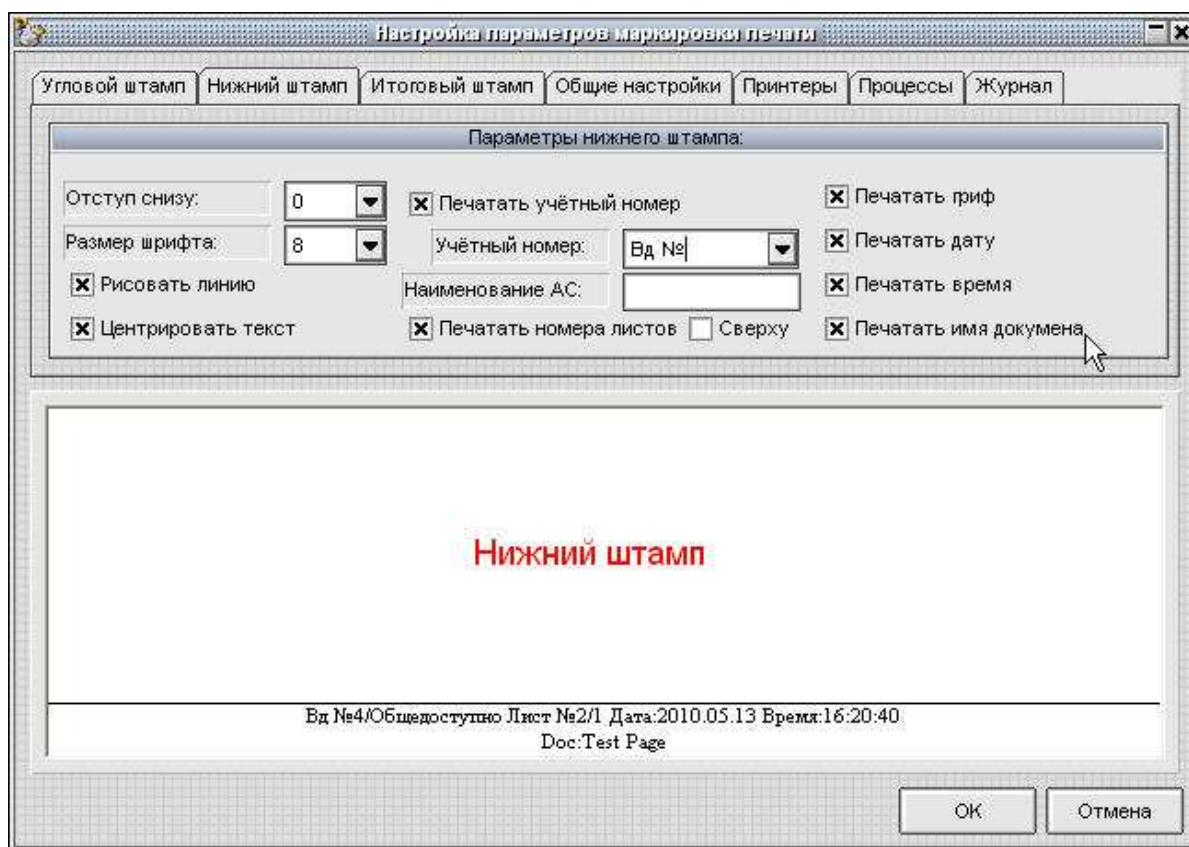


Рис. 6. Настройка нижнего колонтитула маркированного документа.

Параметры «Отступ снизу» и «Размер шрифта» задают положение на странице и размер шрифта маркирующей информации. Флаг «Рисовать линию» включает «отбивку» нижнего штампа линией, а флаг «Центрировать текст» определяет положение на странице. Флаги в правой части окна определяют, какую информацию печатать в нижнем штампе. Отдельного разъяснения требует флаг «Печатать гриф» - это информация о грифе конфиденциальности документа. Корректно определить гриф при выводе на печать можно только при включенном механизме мандатного контроля доступа. Если мандатный механизм без контроля процессов, то гриф определяется меткой доступа редактируемого объекта. Если мандатный механизм с контролем процессов, то гриф определяется уровнем доступа процесса, открывшего документ (в процедуре управления потоками информации нельзя бесконтрольно понижать гриф, а для процесса с высоким уровнем секретности доступны на чтение все объекты с метками нижестоящего уровня, т.е. нужно исключить вариант, когда программа открывает общедоступный файл, добавляет в него секретные сведения и отправляет на печать без грифа секретности). Если такой механизм маркировки грифа не подходит по регламенту, то администратор может в общих настройках маркировки включить флаг «Гриф указывается пользователем» и эта информация будет

вводится пользователем в экранной форме, которая появляется перед печатью документа. «Учетный номер» не может определяться автоматически, поэтому значение этого параметра пользователь также вводит вручную. Если в поле «Наименование АС» администратор вводит текстовую информацию, то эти данные будут автоматически выводиться при маркировке документа. Флаг «Печатать номера листов» определяет, будут ли печататься номера листов. Флаг «Сверху» переводит печать нижнего штампа в верхнюю часть страницы.

Закладка **«Итоговый штамп»** (Рис. 7) определяет вид информации, выводимой на последней странице документа. По требованиям делопроизводства эта информация печатается на оборотной стороне последней страницы. Флаг «Выводить предупреждение о печати последней страницы» требуется включить, если принтер не оборудован устройством подачи бумаги для двусторонней печати. В таком варианте печать последней страницы выполняется после подтверждения пользователя и можно вручную перевернуть страницу.

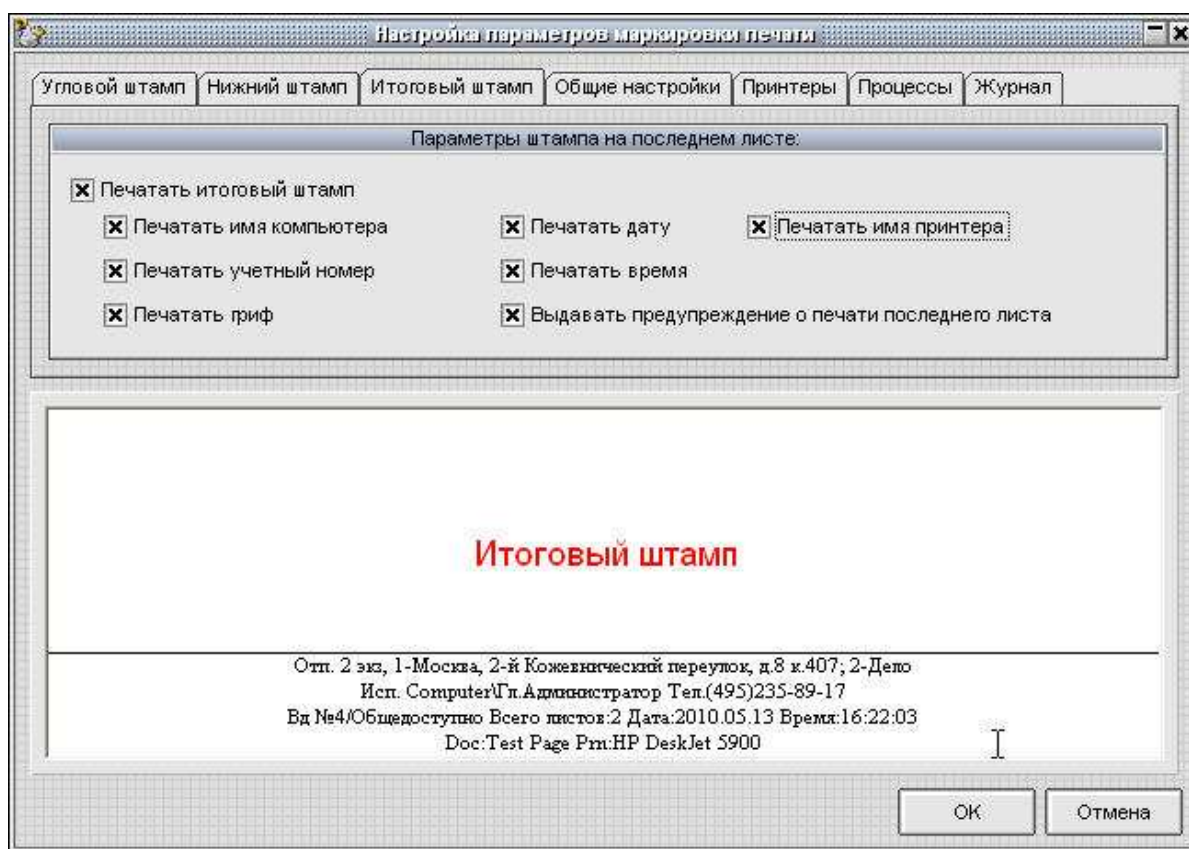


Рис. 7. Настройка маркировки последней страницы документа.

Закладка **«Общие настройки»** (Рис. 8) определяет режимы работы подсистемы контроля печати. Администратор может выбрать уровень конфиденциальности документов, начиная с которого выполняется маркировка, возможность ручного ввода грифа и названия документа, фамилии пользователя и общего количества печатных листов. Если администратор запрещает ручной ввод ФИО пользователя, то документ маркируется полным именем из базы данных СЗИ «Аккорд», а если это поле не заполнено, то коротким. В журнал регистрации печати всегда выводится имя из базы данных, даже если разрешен ручной ввод этого параметра. «Регистрационный номер машинного носителя» - это текстовое поле, которое выводится на последней странице печатного документа по требованию регламента некоторых организаций.

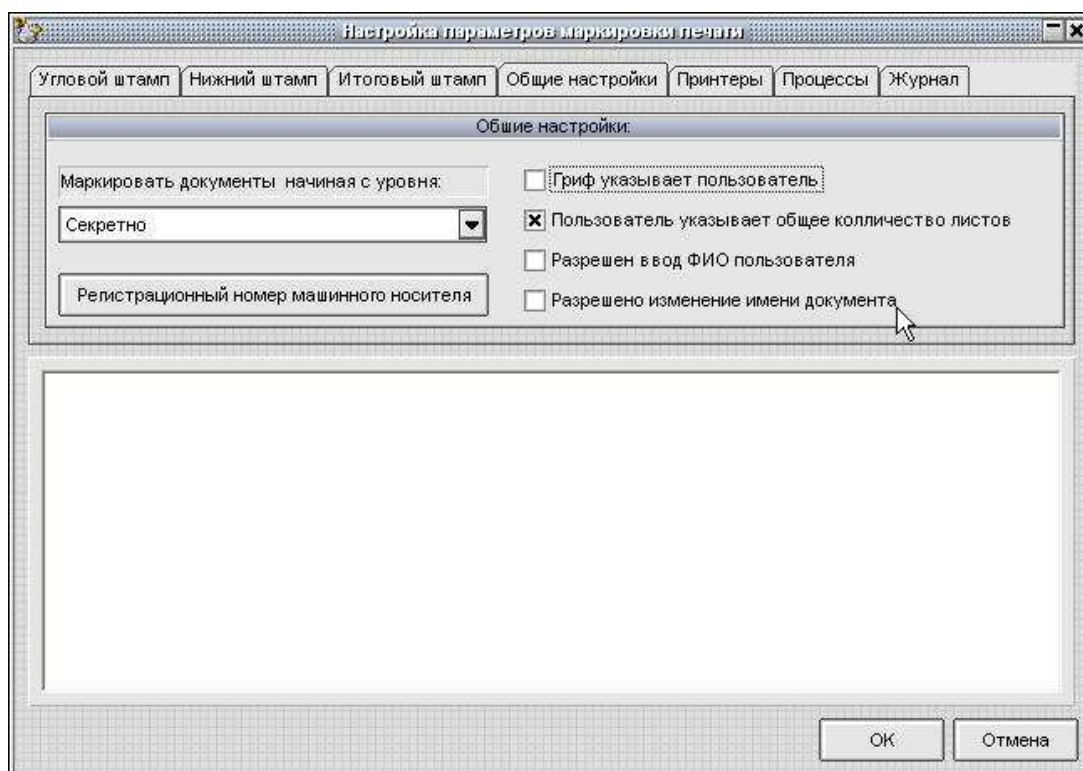


Рис. 8. Общие настройки режима маркировки.

Закладка «Принтеры» (Рис.9) позволяет администратору исключить отдельные печатающие устройства из процесса маркировки документов. Например, устройство Converter PDF – это виртуальный принтер, и вывод осуществляется в файл. Вполне возможно, что в таком варианте маркировка не потребуется.

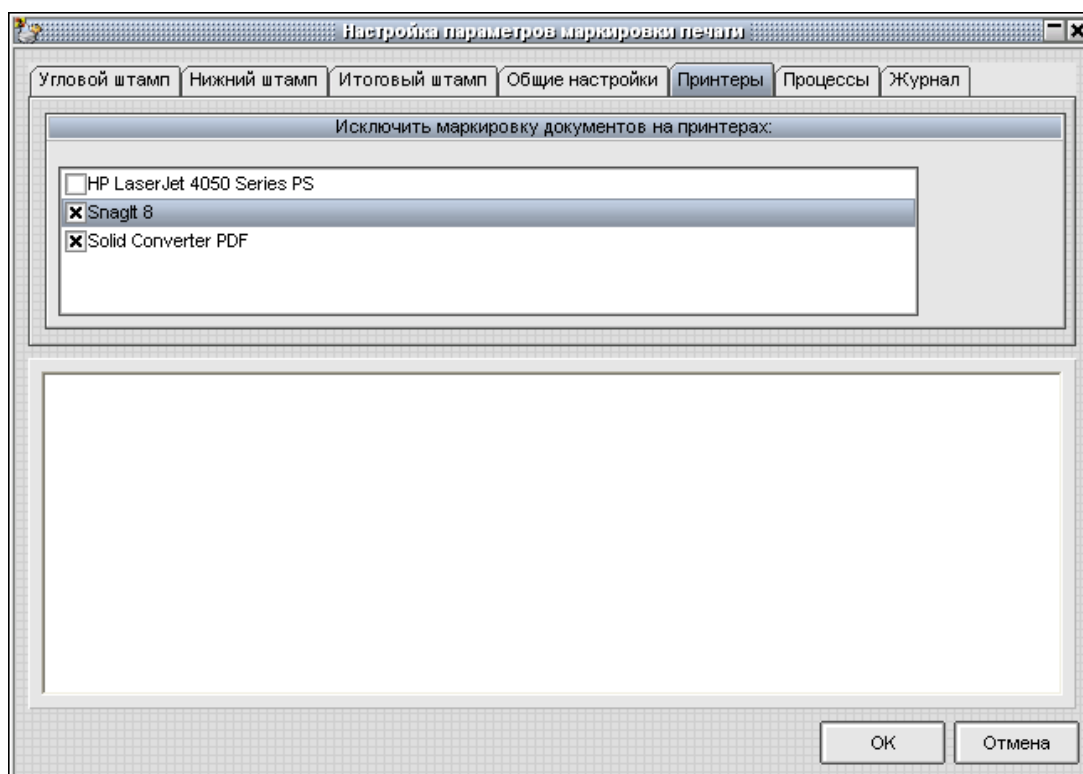


Рис. 9. Выбор печатающих устройств.

Закладка «**Процессы**» позволяет администратору сформировать список процессов, для которых маркировка документов средствами СЗИ «Аккорд» выполняться не будет. Такой режим пригодится в том случае, когда прикладное ПО самостоятельно формирует маркировочную информацию в документах, выводимых на печать. Если не сформировать список исключений, то документ будет маркироваться дважды.

Выбор закладки «**Журнал**» открывает режим просмотра журнала регистрации событий вывода на печать. В журнале документы, которые выводились без маркировки, отображаются черным шрифтом, с маркировкой – синим, а красным шрифтом отображаются события, которые завершились с кодом ошибки.

На рисунке 10 приведена форма, которая выводится на экран перед отправкой документа на печать, если для данного пользователя включен режим маркировки.

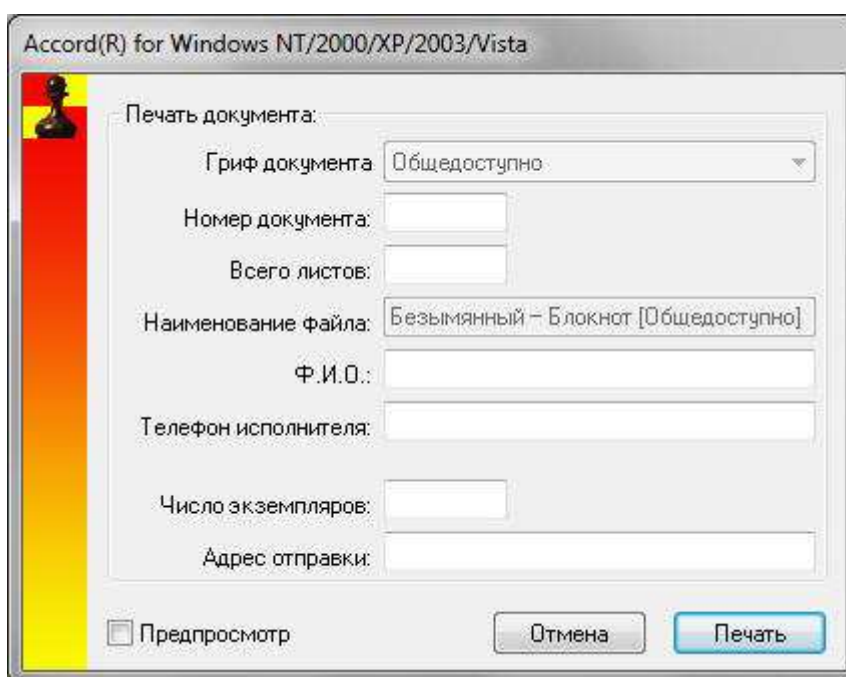


Рис. 10. Окно ввода дополнительных полей маркировки документа.

Часть полей обязательна для ввода, часть задается администратором в настройках. Если пользователь не заполнил одну или несколько строк обязательной информации, то печать документа не выполняется, а в открытом окне курсор мигает в той строке, которую требуется ввести.

После закрытия окна «Маркировка печати» программа возвращается к настройкам режимов работы комплекса СЗИ. Закладка «**Режим сессии**» определяет процедуры начала и завершения работы монитора системы безопасности ACRUN.SYS (Рис.11).

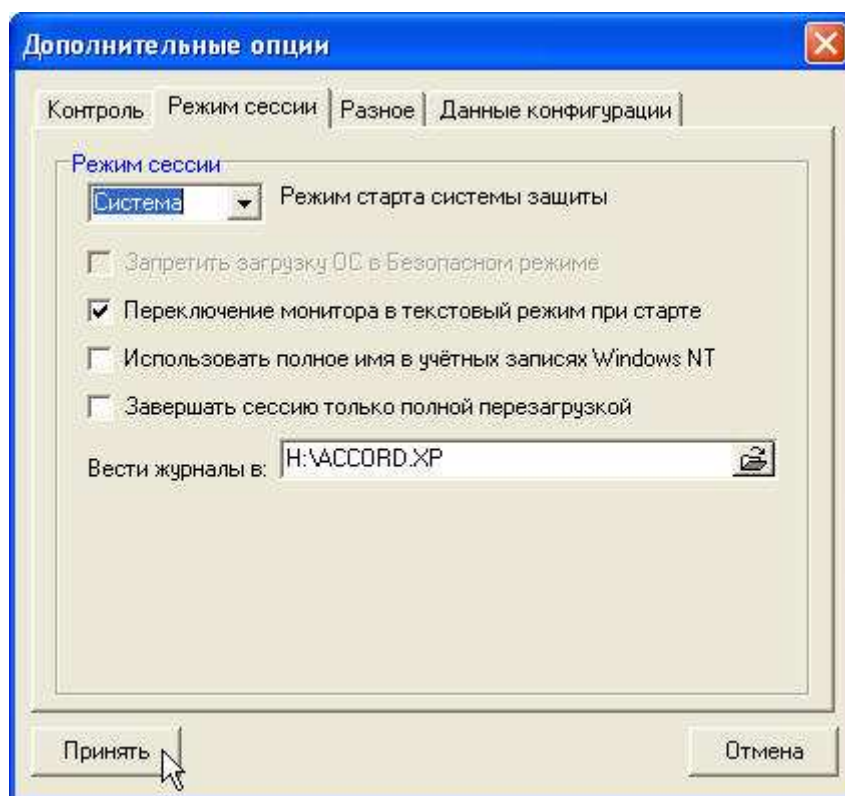


Рис. 11. Дополнительные параметры «Режим сессии» в настройке СЗИ.

“**Режим старта системы защиты**” – в этом поле можно выбрать вариант загрузки монитора безопасности. По умолчанию установлено значение “**Система**”, т.е. ACRUN.SYS стартует как системный драйвер. При выборе значения “**Загрузка**” ACRUN.SYS будет стартовать как загрузочный драйвер. При этом появляется возможность запретить доступ к драйверам различных устройств. Выбор значения “**Вручную**” определяет, что монитор безопасности стартует позже, и подключает правила доступа на основании информации, полученной от модуля AcGina.DLL. В этом случае в качестве идентификатора используется персональное средство защиты информации «ШИПКА», которое подключается к стандартному разъему USB в составе системного блока компьютера. Если USB разъем находится на плате контроллера АМД3, то обмен с идентификатором «ШИПКА» выполняется внутренним ПО контроллера, и режим старта «Вручную» выбирать не нужно. Такой режим может потребоваться для функционирования подсистемы разграничения доступа на мобильном компьютере, в который нет возможности установить плату контроллера. Для функционирования СЗИ в таком режиме необходимо выполнить такую последовательность настроек:

1. После установки программного обеспечения «Аккорд NT/2000» на жесткий диск из папки C:\Accord.NT\Shipka_ID\ копируются файлы osciapi.dll и TmDrv32.dll в папку Windows\System32\.
2. Из папки C:\Accord.NT\ переносится на резервный носитель, или в резервную папку файл TmDrv32.dll (по умолчанию эта библиотека устанавливается для работы с ТМ-идентификаторами) и на ее место копируется одноименная библиотека из папки C:\Accord.NT\Shipka_ID\.
3. Запустить программу «Настройка комплекса Аккорд». На экране появится сообщение: «База данных пользователей не найдена! (User database not found!)». Нажмите мышкой кнопку <Ok> для продолжения работы. В окне основных настроек отключите флаг «Синхронизация с базой АМД3» (контроллер не установлен). После этого работа с программой настроек завершается с сохранением изменений. Теперь можно запускать редактор ПРД и создавать базу пользователей. Все дальнейшие операции выполняются стандартно, согласно документации, только в качестве персонального идентификатора используется ПСЗИ «ШИПКА» вместо ТМ. При первом подключении

ПСЗИ «ШИПКА» в USB-порт необходимо установить драйвер для этого устройства из папки C:\Accord.NT\Shipka_ID\.

4. После создания базы данных пользователей запустите программу «Настройка комплекса Аккорд» и в разделе «Дополнительные опции» установите режим сессии <Вручную>. После этого можно активировать подсистему разграничения (меню <Команды> пункт <Инсталляция>). При выборе режима сессии «Вручную» становится доступным флаг «Запретить загрузку ОС в безопасном режиме». Этот флаг блокирует возможность выбора старта ОС в безопасном режиме, т.к. этот режим позволяет не загружать отдельные драйверы и запускает стандартную процедуру WinLogOn, которая не предусматривает дополнительной идентификации пользователя, тем самым допускает «обход» модулей СЗИ. В режимах старта СЗИ «Загрузка» и «Система» этой опасности нет, т.к. монитор безопасности грузится на уровне ядра системы и его обход невозможен в любом варианте загрузки ОС.

ВНИМАНИЕ! Данные настройки необходимо выполнять только в варианте комплекса, предназначенного для защиты рабочих станций. Вариант комплекса, предназначенный для защиты терминального сервера (TSE – Terminal Server Edition) поддерживает работу одновременно с ТМ-идентификаторами и устройствами ШИПКА.

Флаг **«Запретить загрузку ОС в Безопасном режиме»** устанавливается в том случае, когда выбран режим старта «Вручную», или когда администратор безопасности хочет исключить возможность загрузки системы в обход процедуры WinLogOn. В любом случае включать этот флаг следует только после окончательной настройки работы компьютера в защищенном режиме.

Флаг **«Переключение монитора в текстовый режим при старте»** установлен по умолчанию. Если отключить этот флаг, то информация о старте монитора безопасности будет выводиться в графическом режиме, но только по английски, т.к. на этапе загрузки ядра ОС еще нет поддержки MUI и возможности выбора графических шрифтов.

«Использовать полное имя в учетных записях Windows NT» – при установке этого параметра имя пользователя, заданное в редакторе ПРД ACED32 в поле «Полное имя», будет использоваться при синхронизации с базой учетных записей ОС. Такой режим необходим в том случае, когда пользователь подключается к контроллеру домена, который использует «длинные» имена. Данная опция позволяет администратору обойти ограничение на длину имени в 12 символов, которое накладывается контроллером АДЗ.

«Завершить сессию только полной перезагрузкой» – при установке этого параметра после завершения сеанса пользователя выполняется принудительная перезагрузка компьютера, т.е. нельзя завершить сеанс работы одного пользователя и начать другой без перезагрузки компьютера.

Старт модуля ACRUN.SYS в режиме загрузочного драйвера и завершение сессии перезагрузкой могут понадобиться, например, при включении драйверов сетевой карты в список запрещенных (скрытых) файлов. В таком варианте пользователь (и любая системная или прикладная программа) не получит доступа к сетевым ресурсам, но восстановление подключения к сети для другого пользователя возможно после полной перезагрузки.

Закладка **«Разное»** содержит ряд дополнительных параметров, влияющих на режим функционирования СЗИ (Рис.12).

Первые три параметра относятся к дисциплине гарантированного удаления остаточной информации, которая включается флагом «Удаление файлов с очисткой» в дополнительных опциях пользователя.

«Число проходов при очистке файлов» – этим параметром задается количество циклов заполнения случайными данными области на жестком диске, занимаемой удаляемым файлом.

«Очищать файлы, начиная с уровня» - параметр работает при включенном механизме мандатного доступа, когда требуется очищать остаточную информацию для файлов с определенного уровня конфиденциальности.

«Очищать файл подкачки» – включение этого параметра означает, что файл подкачки (виртуальная память ОС) будет очищен при завершении сеанса работы пользователя.

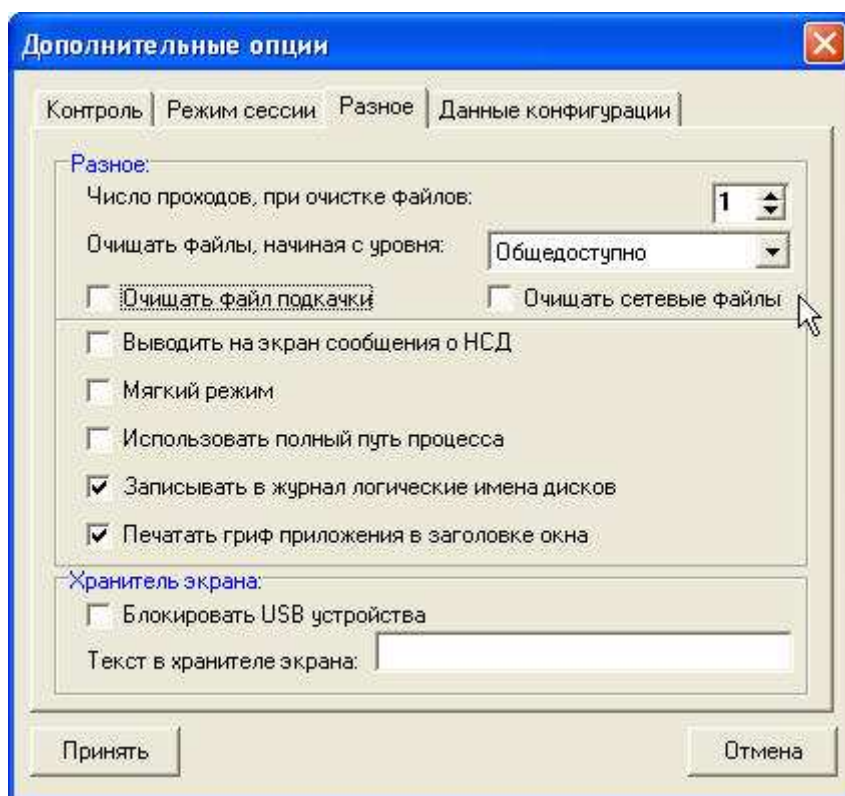


Рис. 12. Дополнительные параметры «Разное» в настройке СЗИ.

“Очищать сетевые файлы” – включение этого параметра означает, что файлы будут удаляться с очисткой и на сетевых дисках.

Остальные параметры определяют различные дополнительные режимы работы СЗИ.

“Выводить на экран сообщения о НСД” - включение этого параметра означает, что сообщения об НСД будут выводиться вначале от имени СЗИ “Аккорд”, а потом будут дублироваться отказами системы. Этот режим может понадобиться на период настройки и отладки политики безопасности, чтобы понять, какие ограничения накладываются СЗИ, а какие – настройками политик ОС. В обычном режиме СЗИ «Аккорд» генерирует код ошибки, передает его системным службам и все отказы в доступе выводятся на уровне стандартного интерфейса ОС.

“Мягкий режим” – установка этого параметра позволяет собирать статистику о ресурсах, которые необходимы для работы прикладного ПО и операционной системы. В этом режиме при обращении к запрещенному (недоступному) ресурсу системой “Аккорд” выводится сообщение об НСД, если включен соответствующий параметр (см. предыдущий пункт), попытка НСД заносится в журнал регистрации событий, но выполнение операции не прерывается. Использование этого режима допускается только на период отладки системы защиты и сбора статистики.

“Использовать полный путь процесса” – этот параметр определяет варианты проверки пути доступа при вызове или контроле процессов. По умолчанию этот флаг не установлен и процесс в файле настроек ПРД описывается только по имени. Включение данного параметра означает, что проверка будет осуществляться по полному пути, т.е. \устройство\том\каталог\файл. Такой режим проверки более строгий.

“Записывать в журнал логические имена дисков” – этот параметр определяет форму записи в журнал регистрации событий. В NT-подобных версиях Windows логические разделы жесткого диска представляются в виде устройство\том\, например: DEVICE\HardDisk0\Volum1\. Включение данного параметра позволяет вести запись журнала в формате Лог.устройство\каталог\файл, например: C:\WINNT\TEMP. После начальной установки СЗИ «Аккорд» этот флаг включен.

«Печатать гриф приложения в заголовке окна» - параметр относится к работе процессов с разными уровнями доступа. При включенном параметре в заголовке окна приложения выводится текущий уровень доступа процесса. В каждый момент пользователь имеет информацию о полномочиях работающего приложения.

Панель **«Хранитель экрана»** содержит только один параметр

«Блокировать USB устройства» – этот параметр позволяет отключать USB порты на время работы хранителя экрана. В обычном режиме, когда порты остаются включенными, появление нового USB устройства снимает Screen Saver и выводит на экран стандартное сообщение о подключении нового устройства. При работе на защищенных СВТ с конфиденциальной информацией такой режим обычно противоречит политике безопасности, поэтому данный параметр должен быть включен администратором. Выключение этого параметра может потребоваться в случае, когда к компьютеру через USB порт подключен принтер (или другое устройство), который выделен в общий доступ для других пользователей в сети. При такой конфигурации включение хранителя экрана и блокировка USB отключают доступ к устройству другим пользователям.

«Текст в хранителе экрана» – Строка символов, которая отображается на экране в момент работы Screen Saver Аккорд.

Закладка **«Данные конфигурации»** содержит настройки аппаратной части комплекса – контроллера АМДЗ (Рис.13), что позволяет менять интервалы времени для идентификации и ввода пароля, а также количество попыток для успешной авторизации.

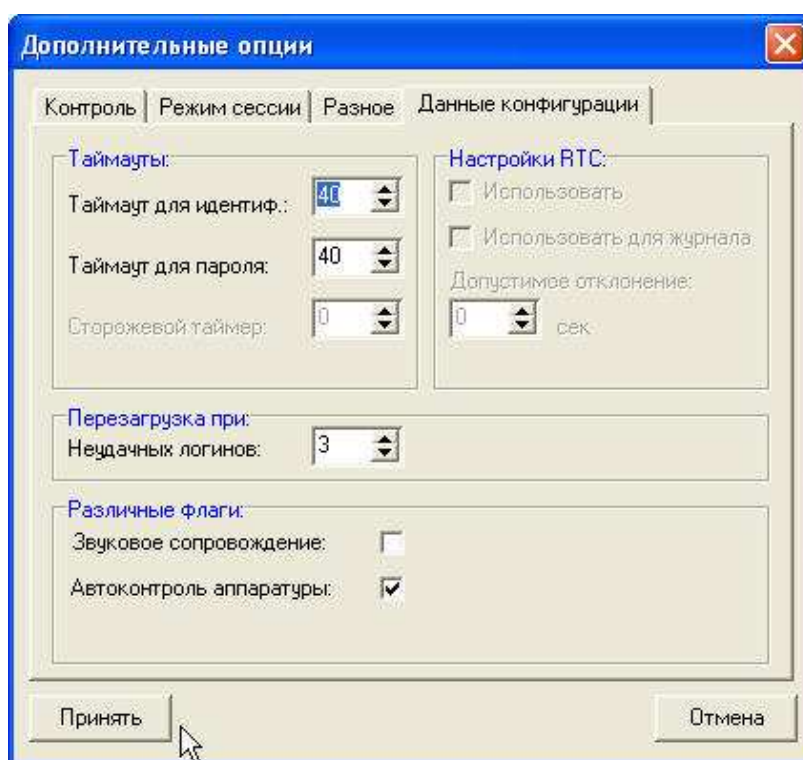


Рис. 13. Параметры «Данные конфигурации» в настройке СЗИ.

Подробно настройка этих параметров описана в документации на «Аккорд-АМДЗ».

2.2.3. Использование антивирусного ядра.

Пункт меню **«Антивирус»** включает/выключает использование антивирусного ядра для проверки файлов на наличие вирусов (Рис. 14.). В настоящий момент поддерживается ядро антивирусной программы «Dr.WEB». В дальнейшем, при достижении соответствующих соглашений, планируется поддержка продуктов других производителей антивирусных программ.

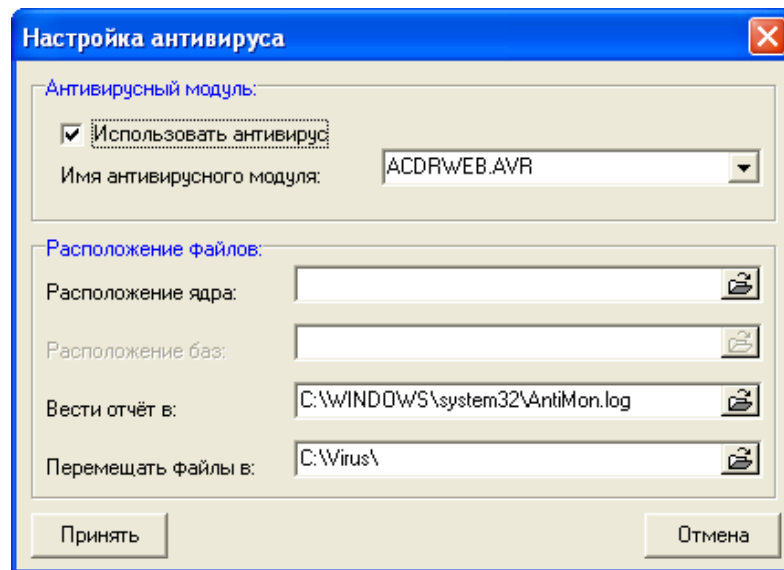


Рис. 14. Настройка использования модуля антивирусной защиты.

После включения этой опции СЗИ «Аккорд» выполняет функции монитора-антивируса, т.к. использует схожие механизмы перехвата дискового ввода/вывода. Таким образом, отпадает необходимость запуска стандартного монитора антивирусной системы, компьютер работает быстрее (вместо двух операций перехвата выполняется одна), но уровень защищенности не уменьшается.

ВНИМАНИЕ! Для использования этой функции необходимо иметь стандартную лицензию антивирусной системы Dr.WEB! Антивирусным модулем СЗИ «Аккорд» используется стандартный набор антивирусных баз.

В строке «Расположение ядра» нужно указать папку на жестком диске, в которой находится библиотека DrWeb32.dll. Обычно это папка, в которую выполняется установка антивирусной системы. Настройку антивирусного монитора следует производить после активизации подсистемы разграничения доступа. После перезагрузки компьютера с включенной подсистемой разграничения доступа и модулем антивирусной защиты появляется дополнительная кнопка в окне, которое вызывается при щелчке левой клавишей мыши на иконке с шахматной фигурой, расположенной на панели задач (Рис. 15.).

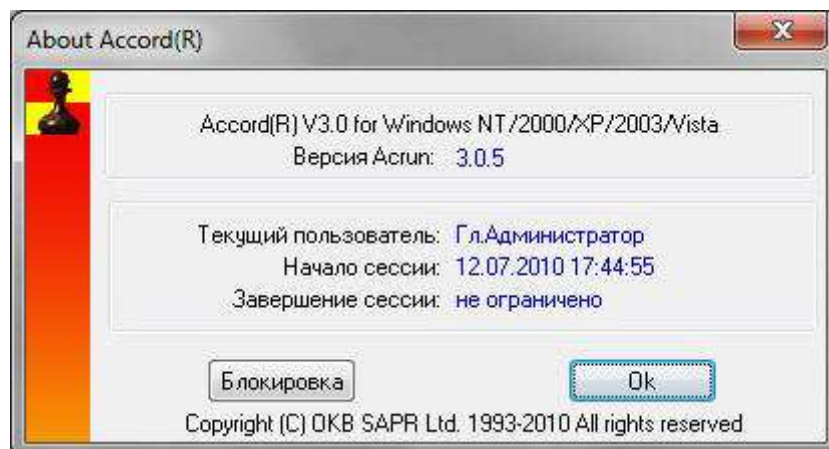


Рис. 15. Окно текущих настроек монитора разграничения доступа.

Щелчок левой клавишей мыши по кнопке «Антивирус» (кнопка появляется только в том случае, когда указана библиотека) открывает доступ к настройкам антивирусного ядра (Рис.16.).

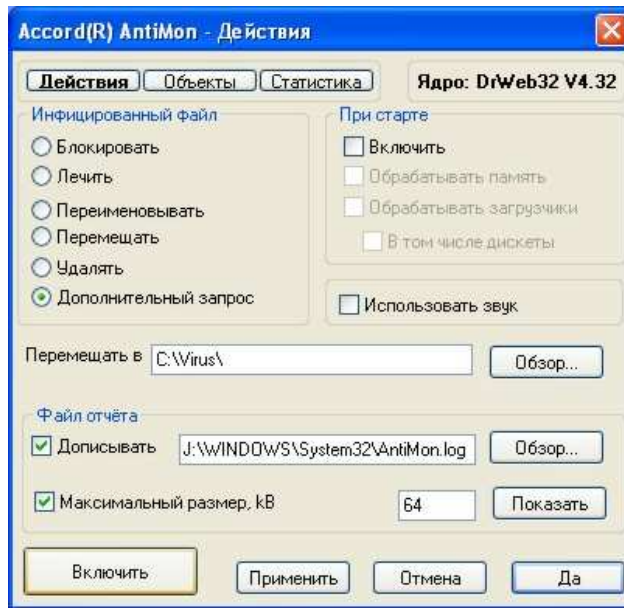


Рис. 16. Настройки антивирусного ядра.

В окне настроек следует установить флаг «При старте - Включить» и нажать кнопку «Включить» в левом нижнем углу. При обнаружении вируса выполняется установленное действие, или выводится диалоговое окно (при настройке «Дополнительный запрос»), в котором пользователь может выбрать операцию, которую необходимо выполнить с зараженным файлом.

2.2.4. Особенности настройки комплекса «Аккорд-NT/2000» при использовании SATA жестких дисков, или RAID контроллеров с динамическим подключением томов.

В современных компьютерах все чаще используются жесткие диски, подключаемые по интерфейсу SATA. При этом на материнских платах используются встроенные RAID контроллеры. Логические тома жесткого диска в такой конфигурации могут подключаться динамически. Поскольку монитор разграничения доступа AcRun.SYS стартует на самом раннем этапе загрузки (практически вся загрузка ОС выполняется под его контролем), могут возникнуть трудности с определением соответствия логических имен разделов жесткого диска и их полных системных имен. Если в редакторе ПРД в списке объектов доступа файл отображается не в привычном виде, например, C:\TMP\my_file.txt, а, к примеру, таким образом:

\DEVICE\HARDDISKDMVOLUMES\EDSRV01DG0\VOLUME1\TMP\my_file.txt, то у Вас именно такой случай. Для успешной работы комплекса «Аккорд» нужно предпринять следующие действия:

1. Закрыть редактор ПРД AcEd32.EXE без сохранения изменений.
2. Удалить файл C:\Accord.NT\accord.amz.
3. В файле C:\Accord.NT\accord.ini для параметра UseLogicalDisksNames изменить значение No (значение по умолчанию) на Yes.
4. Выполнять все дальнейшие действия и настройки ПРД стандартным способом, как описано в документации на комплекс.

ВНИМАНИЕ! Если используются логические имена, то невозможно будет разграничить доступ к съемным дискам (флоппи, USB и др.).

2.3. Активизация подсистемы разграничения доступа.

ВНИМАНИЕ!

Для активизации подсистемы разграничения доступа в пункте меню "Команды" выбираете подпункт "Инсталляция". Подсистема будет установлена и запустится при следующей загрузке.

ВНИМАНИЕ!

Программа ACSETUP.EXE предназначена как для установки, так и для снятия подсистемы разграничения доступа, поэтому рекомендуется скопировать эту программу и хранить ее на отдельном магнитном носителе.

ВНИМАНИЕ!

Для изменения настроек и дополнительных параметров подсистемы защиты не требуется каждый раз устанавливать/снимать подсистему, достаточно запустить программу ACSETUP.EXE, включить или выключить соответствующие параметры и выйти из программы, сохранив изменения. Исключение составляют параметры «При старте», «Режим сессии» и «Мягкий режим». После изменения этих параметров требуется перезагрузка компьютера.

Внимание! Для полноценной работы комплекса «Аккорд» в каталог, где установлено ПО Accord NT/2000 должен быть скопирован файл лицензии Accord.key, который поставляется отдельно на флоппи-диске, или в ТМ-идентификаторе серии DS1993. Если в каталоге с программным обеспечением этого файла нет, то при первом запуске программа настройки запрашивает ТМ-идентификатор, считывает из него информацию и сохраняет в файл Accord.key на диске. После этого идентификатор можно использовать для регистрации пользователя. В этом файле содержится информация о серийном номере контроллера АМДЗ и типе продукта (для рабочей станции или терминального сервера). При отсутствии файла, несовпадении серийного номера контроллера, или несовпадении контрольной суммы файла процедура инсталляции подсистемы разграничения доступа не выполняется.

2.4. Установка правил разграничения доступа (ПРД) для пользователей

Установка правил разграничения доступа (ПРД) для пользователей СВТ, утвержденных в соответствии с политикой информационной безопасности, принятой в организации (предприятии, фирме и т.д.), осуществляется администратором БИ с использованием программ ACED32.EXE. Описание программы, порядок ее применения приведен в документе "Установка правил разграничения доступа. Программа ACED32." (11443195.4012-019 97 02) из комплекта эксплуатационной документации на комплекс "Аккорд-NT/2000" v. 3.0. Примеры ПРД приведены в документе "Руководство администратора" (11443195.4012-019 90 02).

2.5. Установка СЗИ «Аккорд» на терминальном сервере

Программное обеспечение комплекса СЗИ НСД «Аккорд NT/2000» содержит модули, которые обеспечивают выполнение защитных функций при работе терминального сервера. В качестве серверного ПО может использоваться Windows 2000/2003 Terminal Server, или Citrix Metaframe. Инсталляция программного обеспечения на жесткий диск выполняется стандартным образом, только в программе инсталляции включается флаг «Поддержка Terminal Server». При этом различия проявляются только в программе настройки комплекса. В подменю «Параметры» появляется дополнительный пункт «Terminal Server» (Рис. 17).

Внимание! Для варианта установки комплекса «Аккорд» Terminal Server Edition в файле лицензии Accord.key содержится информация о серийном номере контроллера АМДЗ и количестве обрабатываемых терминальных сессий. Обратите внимание, что в этом файле параметр [Products] имеет значение Accord TS Edition! При несоответствии варианта установки ПО с информацией в файле лицензии выдается сообщение «Ключевой файл лицензии не подходит для этого продукта!» и программа настройки не запускается.

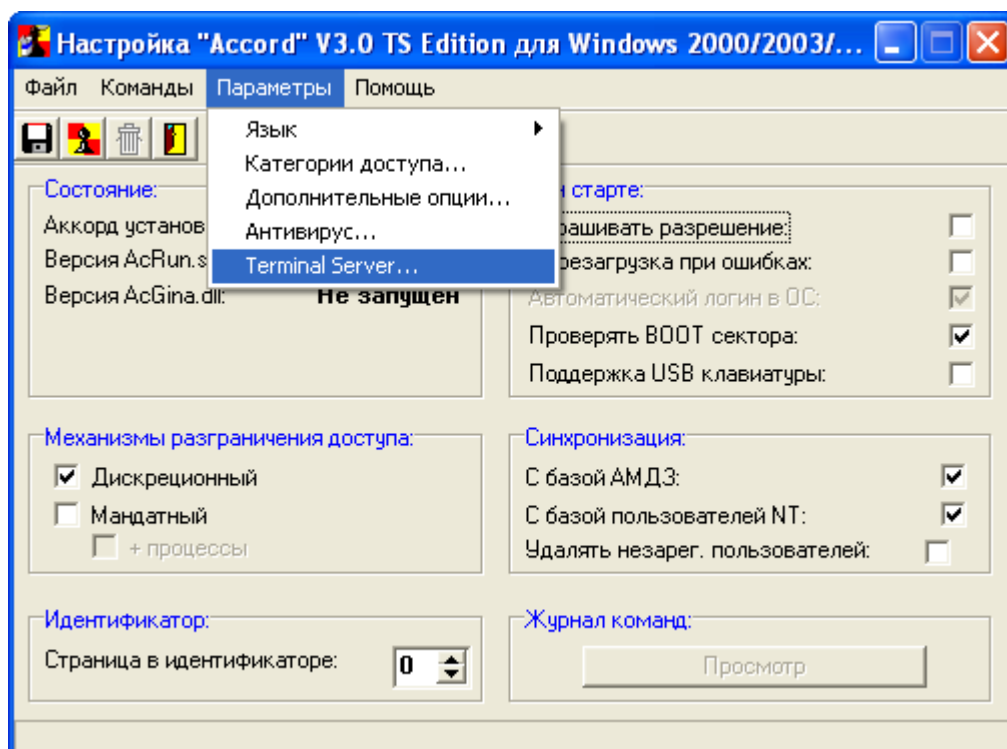


Рис. 17. Пункт меню «Terminal Server» в программе настройки комплекса.

Выбор пункта «Terminal Server» в меню «Параметры» открывает окно настроек сессий терминального доступа (Рис. 18.).

Для начала необходимо выбрать протокол виртуального канала, по которому будет осуществляться связь с терминалами. «Аккорд» поддерживает протокол RDP для Windows 2000/2003 Terminal Server и ICA для Citrix Metaframe. Необходимо выбрать хотя бы один протокол, но возможна работа одновременно по двум протоколам.

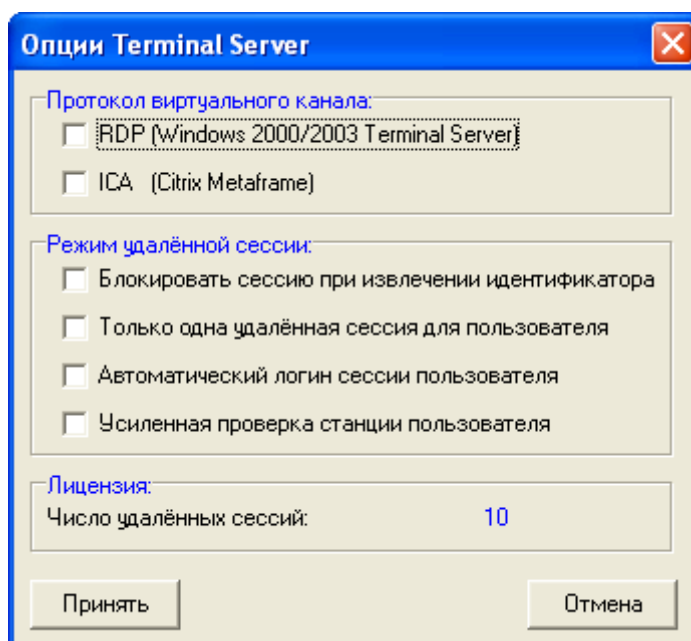


Рис. 18. Настройки режимов работы Terminal Server.

Режим удаленной сессии определяет варианты взаимодействия с клиентскими терминалами.

Блокировать сессию при извлечении идентификатора – флаг определяет режим работы сессии, при котором при извлечении идентификатора сессия будет блокироваться.

Только одна удаленная сессия для пользователя – вариант работы, когда удаленный пользователь не может одновременно открыть несколько удаленных сессий.

Автоматический логин сессии пользователя – флаг определяет режим работы пользовательского терминала, при котором результаты идентификации/аутентификации пользователя передаются от аппаратной части СЗИ (Аккорд-АМДЗ) программному обеспечению, которое обрабатывает начало сессии удаленного пользователя.

Усиленная проверка станции пользователя – этот флаг включает режим проверки не только идентификационных параметров пользователя, но также и идентификационных параметров удаленного терминала на основе информации, которая хранится в энергонезависимой памяти контроллера «Аккорд-АМДЗ».

Все остальные настройки правил разграничения доступа на сервере не отличаются от стандартных. Администратор создает пользователя, регистрирует его ТМ-идентификатор, назначает пароль и правила доступа к ресурсам, которые находятся на жестком диске терминального сервера. Особенность администрирования на терминальном сервере заключается в том, что терминальные пользователи должны регистрироваться в отдельной группе, которая будет синхронизироваться не только с группой Users, но и с группой Remote Desktop Users.

В свойствах группы есть параметр «NT группы». Нажав на кнопку в правой части этого поля, мы получим доступ к списку групп в составе ОС и можем выбрать политику синхронизации пользователей СЗИ «Аккорд» с учетными записями в операционной системе (Рис. 19). Как включить пользователя СЗИ «Аккорд» в несколько групп в составе ОС – также описывается в документе «Установка правил разграничения доступа. Программа Aced32.exe» (11443195.4012-019 97 02) пункт 6.17.

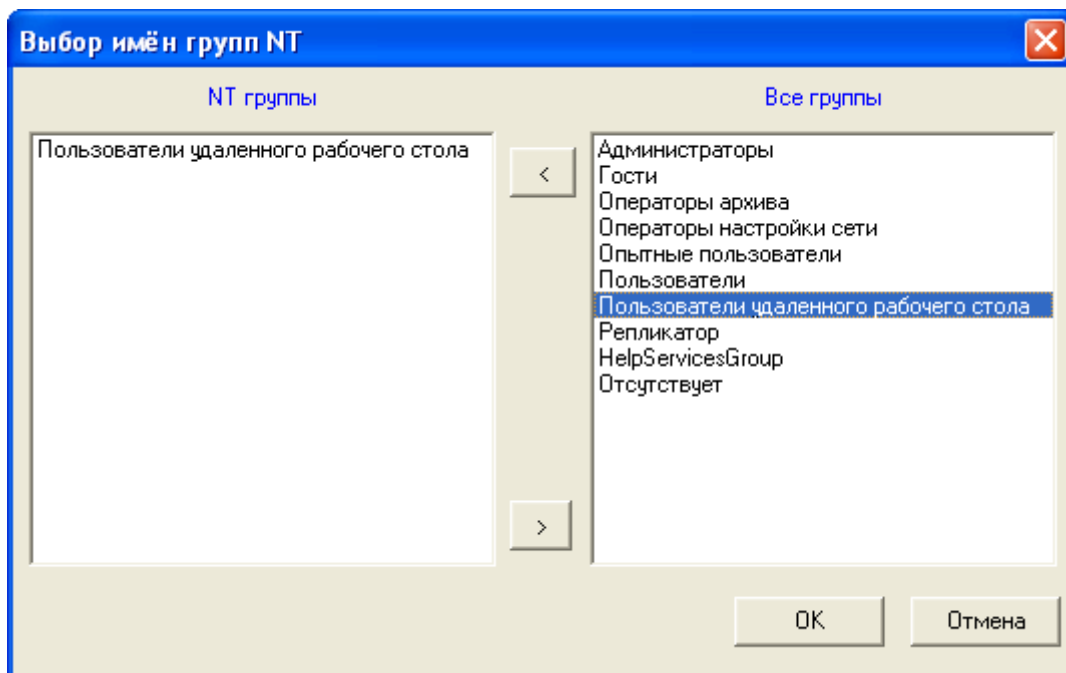


Рис. 19. Выбор групп в составе ОС для синхронизации пользователей СЗИ «Аккорд».

На удаленном терминале устанавливается клиентское ПО СЗИ «Аккорд» из папки TS_Client на дистрибутивном носителе. После установки ПО необходимо выполнить настройку терминального клиента СЗИ «Аккорд». Последовательно выбирая мышью <Пуск> <Программы> <Аккорд-ТС> <Настройка терминального клиента>, запускаем необходимое приложение (Рис. 20).



Рис. 20. Окно настройки терминального клиента СЗИ «Аккорд».

Необходимо выбрать один, или оба протокола и тип используемого на терминале персонального идентификатора. Если компьютер, на котором установлено клиентское ПО, допускает установку плат расширения, то можно установить контроллер «Аккорд - АМДЗ» и использовать ТМ-идентификаторы серий DS1992-1996. Если на удаленном терминале нет никаких портов расширения, кроме USB, то задача решается использованием ПСКЗИ ШИПКА в качестве уникального идентификатора. Как смешанный вариант возможно использование и тех, и других идентификаторов, но одно правило остается неизменным: «Один пользователь – один уникальный идентификатор».

После выбора параметров нужно нажать кнопку «Install» для активирования службы терминального клиента СЗИ «Аккорд».

После этого привычная процедура подключения к терминальному серверу слегка видоизменяется. После запуска программы mstsc (Microsoft Terminal Server Client) можно обычным образом выбрать сервер, или его IP-адрес (Рис. 21).



Рис. 21. Выбор терминального сервера.

Но после выбора кнопки <Connect> (Подключение) выполняется дополнительная процедура идентификации (Рис. 22)...

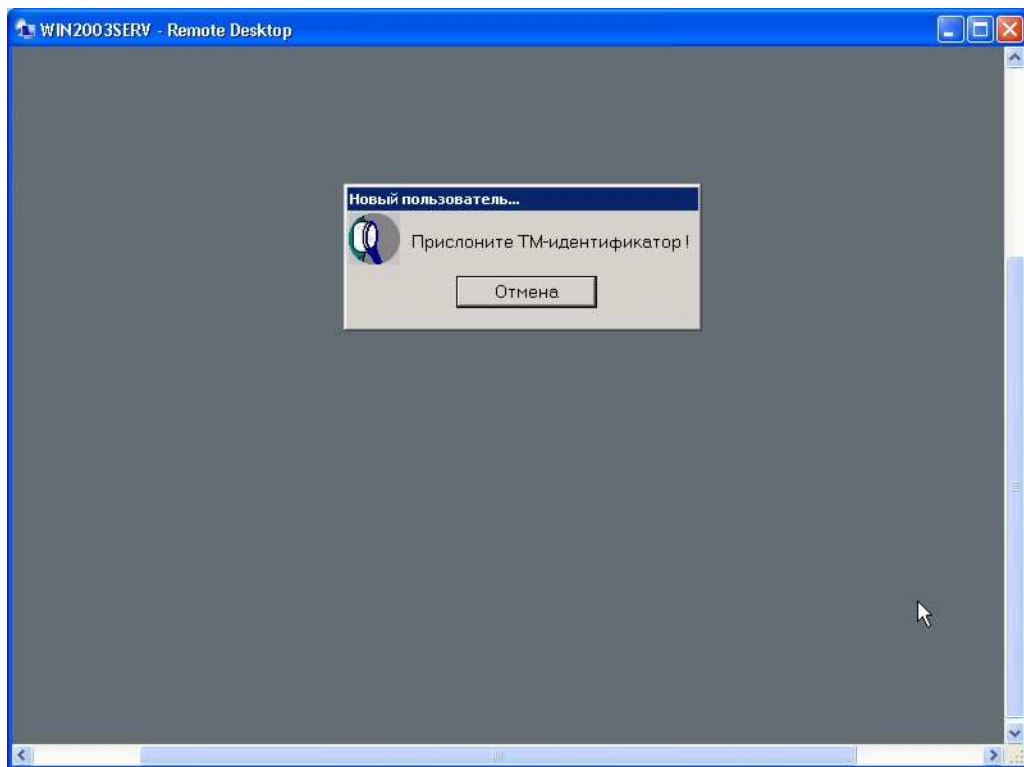


Рис. 22. Идентификация пользователя.

И аутентификации пользователя (Рис. 23).

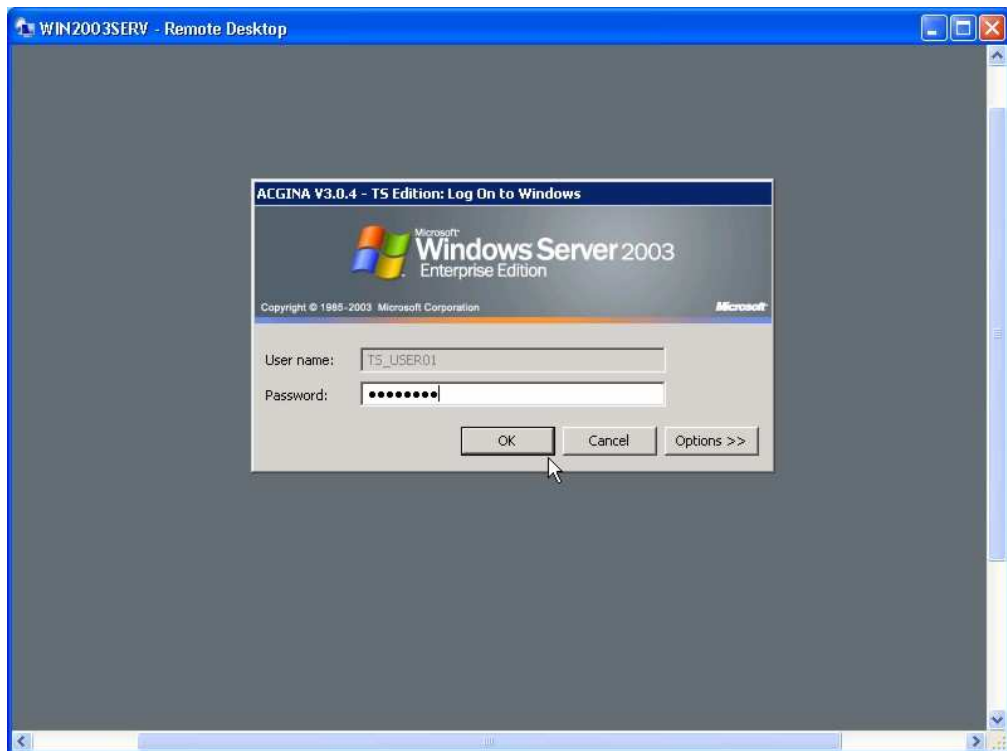


Рис. 23. Аутентификация пользователя по паролю.

В случае использования ПСКЗИ ШИПКА идентификатором служит уникальный серийный номер конкретного устройства, который записывается при изготовлении и впоследствии не меняется даже при форматировании внутренней памяти ШИПКи.

Результаты И/А передаются на сервер в защищенном виде, и уже серверная часть СЗИ «Аккорд» ищет учетную запись в своей базе данных. Если пользователь успешно провел процедуру идентификации/аутентификации, то для него открывается сессия с тем набором правил разграничения доступа (ПРД), который установил администратор безопасности на терминальном сервере.

На терминальном сервере монитор безопасности СЗИ «Аккорд» функционирует в многопользовательском и многозадачном режиме, т.е. для каждого сеанса терминального пользователя выполняется индивидуальная политика работы с ресурсами сервера, основанная на сертифицированных механизмах дискреционного и мандатного доступа. В том случае, когда сформирована ИПС (изолированная программная среда), то и набор исполняемых модулей жестко регламентирован для каждого пользователя. Реализованная в СЗИ «Аккорд» процедура динамического контроля целостности существенно усиливает стойкость защиты, т.к. исполняемый модуль, включенный в список контроля, проверяется непосредственно перед каждым запуском, что гарантирует неизменность среды во время всего сеанса работы.

Приведенные на рисунках примеры относятся к тому случаю, когда средой для работы терминального клиента являются ОС Windows 2000/ XP/ Embedded. Однако специалистами ОКБ САПР разработаны варианты клиентской части и для Windows CE v.5-6, и для Linux (версия ядра 2.6).

2.6. Особенности использования ПСКЗИ ШИПКА в качестве персонального идентификатора

При использовании СЗИ «Аккорд NT/2000» для защиты терминальных систем может возникнуть ситуация, когда удаленный терминал по своим конструктивным особенностям не предполагает установку каких-либо плат расширения. В этом случае в качестве персонального идентификатора используется USB-устройство ПСКЗИ ШИПКА. Администратору безопасности необходимо выполнить несколько предварительных операций по инициализации этого устройства, прежде чем регистрировать его как идентификатор.

Примечание. Все действия по инициализации устройства ШИПКА, изложенные в этом пункте, выполняются однократно для нового устройства. Если инициализация уже выполнялась, то не требуется повторения данных операций перед использованием устройства ШИПКА.

Прежде чем начать использовать новое устройство ШИПКА, необходимо провести процедуру инициализации (начального форматирования).

ВНИМАНИЕ! Без выполнения этой процедуры пользователю недоступны никакие внутренние функции устройства ШИПКА.

Перед выполнением процедуры инициализации необходимо установить параметры PIN-кода: минимальную длину, количество попыток ввода, алфавит символов, а также наличие/отсутствие PUK-кода и его параметры. Для настройки параметров предназначена специальная программа.

Доступ к встроенным функциям ПСКЗИ ШИПКА и персональной информации пользователя (ключей, паролей и пр.) предоставляется только после ввода аутентифицирующей информации (PIN-кода). PIN-код представляет собой последовательность символов длиной от 6 до 32 знаков. В качестве символов PIN-кода можно использовать цифры, буквы, спецсимволы. Возможность комбинирования различных типов символов повышает надежность процедуры аутентификации. Мощность алфавита (общее число символов) становится больше, а, следовательно, количество вариантов PIN-кода резко возрастает. Минимальная длина PIN-кода и алфавит используемых символов задаются в программе настройки параметров авторизации.

Следующий важный параметр – количество попыток для ввода PIN-кода. Если за отведенное количество попыток пользователь не введет правильный PIN-код, то доступ к устройству ШИПКА блокируется. Способ разблокирования устройства также задается в программе настройки параметров инициализации. Если устройство отформатировать с формированием специального PUK-кода, то с помощью этого кода можно разблокировать ПСКЗИ ШИПКА. Если форматирование выполнялось без формирования PUK-кода, то разблокировать устройство нельзя. Можно только повторно отформатировать. При этом стираются во внутренней памяти **ВСЕ** персональные ключи и пароли пользователя! Следует очень внимательно относиться к настройке параметров авторизации.

Архитектура ПСКЗИ ШИПКА такова, что доступ к информации имеет только владелец, но правила доступа к устройству задает *администратор* в соответствии с корпоративными документами, что позволяет правильно использовать персональное средство защиты информации в корпоративной среде. Администратор ШИПКИ может только назначать параметра авторизации в устройстве, никаких других прав у него нет.

Если устройство используется персонально, то администратором устройства является сам его владелец.

Для настройки следует в папке Accord.NT\SHIPKA_ID запустить программу shauth.exe. На экран выводится окно выбора параметров (Рис. 24).

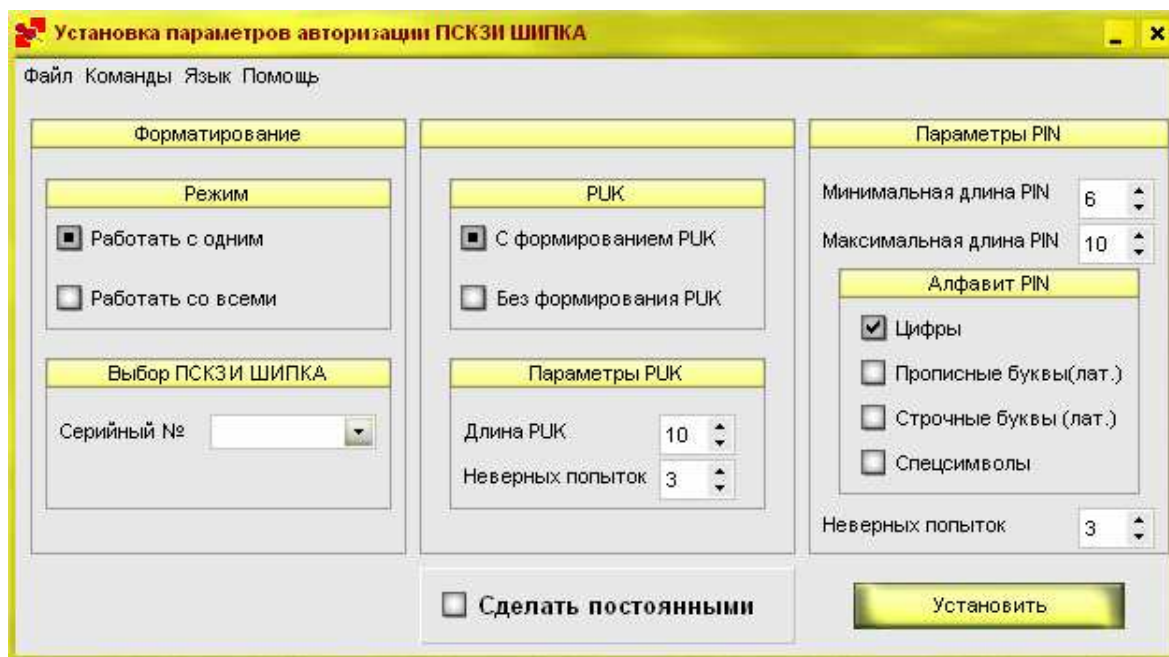


Рис. 24. Окно установки параметров авторизации ПСКЗИ ШИПКА

В левой части окна можно выбрать конкретное устройство по серийному номеру, либо установить режим «Работать со всеми». В этом случае параметры авторизации будут установлены для всех устройств ШИПКА, подключенных в данный момент времени к USB-портам компьютера.

В средней части окна можно настроить режим форматирования «С формированием PUK», или «Без формирования PUK».

PUK-код представляет собой последовательность из цифр и букв, выработанную случайным образом в процессе форматирования. Для возможности генерации PUK-кода данная опция должна быть включена при инициализации, и должны быть заданы параметры PUK-кода:

- длина PUK - число символов в PUK-коде;
- неверных попыток – количество ошибок, допустимых при вводе PUK-кода. После исчерпания числа попыток ввода PUK-кода доступ к ПСКЗИ ШИПКА полностью блокируется.

В правой части окна устанавливаются параметры PIN-кода.

- **минимальная и максимальная длина** – эти параметры определяют нижнюю и верхнюю границы для количества знаков в PIN-коде.
- Параметр «**Алфавит**» определяет множество символов, которые будут использоваться при первом вводе PIN-кода и его последующих сменах. Можно указать как один, так и несколько наборов символов, поставив отметку напротив нужного пункта. Набор «**Спецсимволы**» содержит символы, вводимые при нажатии комбинации клавиш Shift-(0-9).
- Параметр «**количество неверных попыток**» характеризует количество допустимых ошибок при вводе PIN. После превышения количества попыток ПСКЗИ ШИПКА блокируется.

ВНИМАНИЕ! Следующий параметр очень важен для всей последующей работы с устройством ШИПКА. Если включить флаг «**Сделать постоянными**» и нажать кнопку «Установить», то выбранные параметры авторизации ПСКЗИ ШИПКА будут установлены раз и навсегда, т.е. изменить их будет невозможно даже с помощью данной программы. Задавать этот параметр следует только в том случае, если есть уверенность, что выбранные настройки будут полностью удовлетворять политике безопасности, и не придется в дальнейшем задавать другие параметры. Если такой уверенности нет, лучше не использовать эту опцию.

Если флаг **«Сделать постоянными»** не включен, то при выборе кнопки «Установить» выводится запрос на ввод и подтверждение пароля администратора.

Если выбран режим работы со всеми ПСКЗИ ШИПКА, находящимися в USB портах, то предполагается, что пароль администратора одинаков для всех устройств.

После нажатия кнопки «Установить» и ввода пароля администратора выполняется очистка области памяти, отведенной для пользовательской информации (ключи, пароли и пр.) и записываются в служебную память установленные параметры, в соответствии с которыми пользователь может в дальнейшем выполнять форматирование и разблокировку устройства. Пароль администратора также записывается в устройство ШИПКА и потребуется для последующих изменений параметров авторизации.

Администратор в любой момент может поменять пароль авторизации через меню <Команды>-<Сменить пароль>. Все остальные данные в устройстве ШИПКА при этой операции не меняются.

Пароль администратора позволяет многократно изменять параметры авторизации устройства ШИПКА. После изменения параметров авторизации устройство **обязательно форматируется**, и после форматирования ПСКЗИ ШИПКА политика доступа и блокировки изменится в соответствии с новыми заданными параметрами.

Следующий необходимый шаг – непосредственная инициализация (форматирование) устройства ШИПКА. Как уже упоминалось ранее, программа настройки параметров авторизации только задает правила формирования PIN и PUK кодов, а сама инициализация выполняется отдельной утилитой. Все операции, которые выполняются в этой программе, не требуют ввода пароля администратора, но жестко регламентируются политикой, заданной в процедуре установки параметров авторизации. Изменить эти параметры пользователь самостоятельно не может.

Вызов утилиты инициализации выполняется следующим образом: в папке Accord.NT\SHIPKA_ID запустить программу shinit.exe. В главном окне программы (Рис. 25) три закладки: «Сменить PIN», «Форматировать» и «Разблокировать».

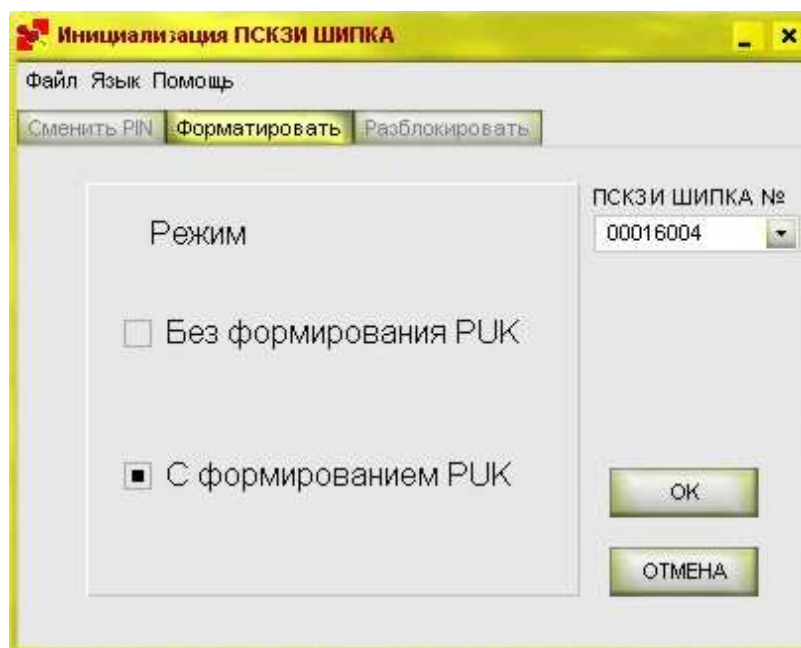


Рис. 25. Форматирование устройства ШИПКА

Первая операция, которая выполняется с новым устройством ШИПКА – это форматирование.

Выберите закладку «Форматировать» и нажмите кнопку «Ок». Если администратором установлен режим форматирования с формированием PUK-кода (настоятельно рекомендуется

устанавливать именно этот режим, потому что это поможет избежать проблем в случае блокировки устройства), то первое форматирование должно обязательно производиться с формированием PUK, обойти это правило нельзя. В процессе выполнения операции выводится окно со сгенерированным PUK-кодом и предложением сохранить этот PUK-код в файл (Рис. 26).

Пользователь может принять сохранение, или отказаться от него, но резервная копия кода разблокировки поможет в случае, если пользователь его забыл. Этот файл можно перенести на любое сменное устройство и хранить в надежном месте.

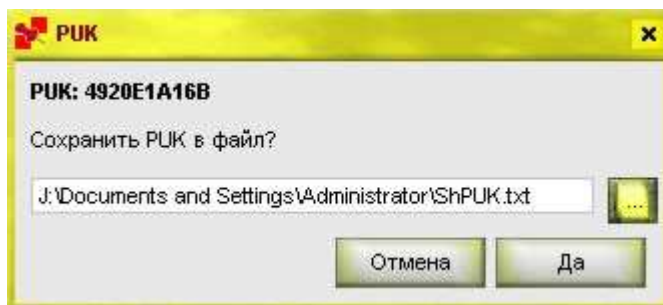


Рис. 26. Запрос на сохранение PUK-кода в файл

После форматирования и успешного сохранения PUK-кода выводится сообщение (Рис. 27).

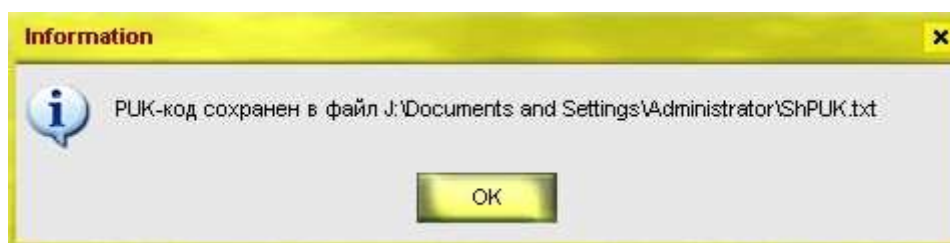


Рис. 27. Подтверждение записи PUK-кода в файл

Если пользователь попытается отформатировать устройство ШИПКА с параметрами, отличными от тех, которые были заданы в программе установки параметров авторизации, то на экран выводится сообщение о невозможности выполнения операции и причина отказа (Рис. 28). В данном случае была попытка отформатировать устройство без создания PUK-кода, в то время как параметры авторизации требуют его генерации.

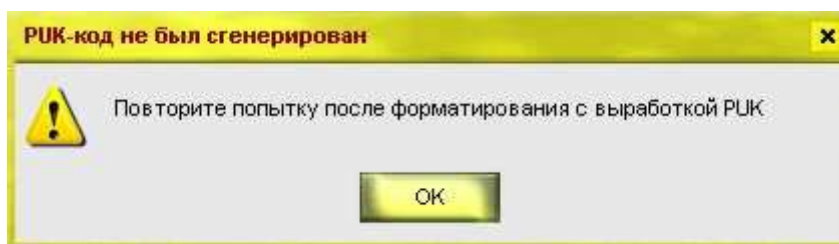


Рис. 28. Предупреждение о невозможности отформатировать устройство ШИПКА без формирования PUK-кода

После успешного форматирования можно регистрировать устройство ШИПКА в качестве персонального идентификатора пользователя в программе – редакторе ПРД. Более подробная документация об использовании ПСКЗИ ШИПКА находится на компакт-диске, поставляемом вместе с устройством. При первом подключении ПСКЗИ «ШИПКА» в USB-порт необходимо установить драйвер для этого устройства из папки C:\Accord.NT\Shipka_ID\.

3. СНЯТИЕ СРЕДСТВ ЗАЩИТЫ КОМПЛЕКСА "АККОРД-NT/2000".

ВНИМАНИЕ!

Снятие защиты разрешено только администратору БИ (супервизору).

Для снятия защиты необходимо выполнить следующие действия:

1. Включить и войти в систему с параметрами администратора БИ.
2. Запустить программу ACSETUP.EXE из каталога \ACCORD.NT. При этом повторно запрашивается идентификатор администратора БИ. Если идентификация администратора БИ прошла успешно, то на экран выводится окно, показанное на Рис. 1.
3. В пункте меню "Команды" следует выбрать подпункт "Снятие". Система разграничения доступа будет отключена, и при следующей загрузке не будет активизироваться. Каталог ACCORD.NT остается на жестком диске. Для полной деинсталляции системы «Аккорд» необходимо перезагрузить компьютер и запустить файл UnWise.EXE из каталога ACCORD.NT.
4. Отключить питание.
5. Вскрыть корпус системного блока.
6. Извлечь аппаратную часть комплекса (контроллер).