

ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО



систем автоматизированного
проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.4012-019 99 02-ЛУ

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

**ПОДСИСТЕМА РЕГИСТРАЦИИ.
ПРОГРАММЫ РАБОТЫ С
ЖУРНАЛАМИ РЕГИСТРАЦИИ.**

11443195.4012-019 99 02

Литера О₁

АННОТАЦИЯ

Программа LOGVIEW.EXE предназначена для работы с журналами регистрации, которые создаются в процессе функционирования подсистемы разграничения доступа комплекса СЗИ НСД "Аккорд-NT/2000" v.3.0 (ТУ 4012-019-11443195-02).

Программа используется администратором безопасности информации комплекса СЗИ НСД "Аккорд-NT/2000" v.3.0 и входит в состав специального ПО комплекса.

Настоящий документ предназначен для конкретизации действий администратора безопасности информации (БИ) (либо субъектов доступа, наделенными правами администратора) при работе с журналами регистрации.

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

Применение защитных механизмов комплекса должно дополняться общими мерами технической безопасности, а также физической охраной СВТ.

СОДЕРЖАНИЕ

1	НАЗНАЧЕНИЕ ПРОГРАММЫ	5
2	ПОРЯДОК РАБОТЫ С ПРОГРАММОЙ.....	5
2.1	ЗАПУСК ПРОГРАММЫ LOGVIEW	5
2.2	ПРОСМОТР ЖУРНАЛА РЕГИСТРАЦИИ СОБЫТИЙ	7
2.2.1	<i>Фильтрация по имени процесса.....</i>	<i>7</i>
2.2.2	<i>Фильтрация по результату операции</i>	<i>7</i>
2.2.3	<i>Фильтрация по коду события</i>	<i>8</i>
2.2.4	<i>Фильтрация по наименованию объекта</i>	<i>10</i>
2.3	ВЫВОД НА ПЕЧАТЬ	11
2.4	ВЫХОД ИЗ ПРОГРАММЫ	11
3	ПРЕДВАРИТЕЛЬНАЯ СОРТИРОВКА ЖУРНАЛОВ.....	11
3.1	АРХИВАЦИЯ/РАЗАРХИВАЦИЯ ЖУРНАЛОВ.....	12
4	ФОРМИРОВАНИЕ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА НА ОСНОВЕ ИНФОРМАЦИИ В ЖУРНАЛЕ РЕГИСТРАЦИИ СОБЫТИЙ.....	13
4.1	РАБОТА С ПРОГРАММОЙ LOGTOPRD	13
4.2	РАБОТА С ПРОГРАММОЙ ACPROC	15
	РАБОТА С ПРОГРАММОЙ READPRD	17

ПРИНЯТЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

PM (Protected Mode)	- защищенный режим работы 32-битных приложений
Registry (реестр)	- главная иерархическая база данных Windows NT/2000, в которой хранится информация об аппаратных средствах, конфигурации системы и прикладного ПО, профилях пользователей.
Screen-Saver	- хранитель экрана (программа-заставка). Предназначена для временной блокировки экрана СВТ. В ПАК СЗИ НСД "Аккорд" дополнена дополнительной функцией идентификации пользователя по идентификатору при разблокировании СВТ
ПАК СЗИ НСД	- программно-аппаратный комплекс средств защиты информации от несанкционированного доступа
Профиль пользователя	- индивидуальные настройки пользователей в Windows NT/2000

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа LOGVIEW.EXE предназначена для работы с журналами регистрации, которые создаются в процессе функционирования подсистемы разграничения доступа ПАК СЗИ НСД "Аккорд-NT/2000" v.3.0.

Доступ к программе обеспечивается только администратору БИ, либо субъектам доступа, наделенным правами администратора.

Для каждого сеанса работы пользователя создается отдельный файл журнала. Имя файла генерируется с помощью системной даты, времени и некоторой случайной компоненты (чтобы исключить совпадение имен файлов журнала).

2 ПОРЯДОК РАБОТЫ С ПРОГРАММОЙ

При работе программно-аппаратного комплекса средств защиты от несанкционированного доступа "Аккорд-NT/2000" события регистрируются в файлах журнала в упакованном формате (для экономии дискового пространства). Если комплекс защиты используется в сетевой версии, то в журнале фиксируется имя станции.

2.1 Запуск программы LOGVIEW

Запустите программу LOGVIEW.EXE из каталога C:/ACCORD.NT.

При запуске программы на экран выводится окно выбора журнала для просмотра, показанное на Рис.1.

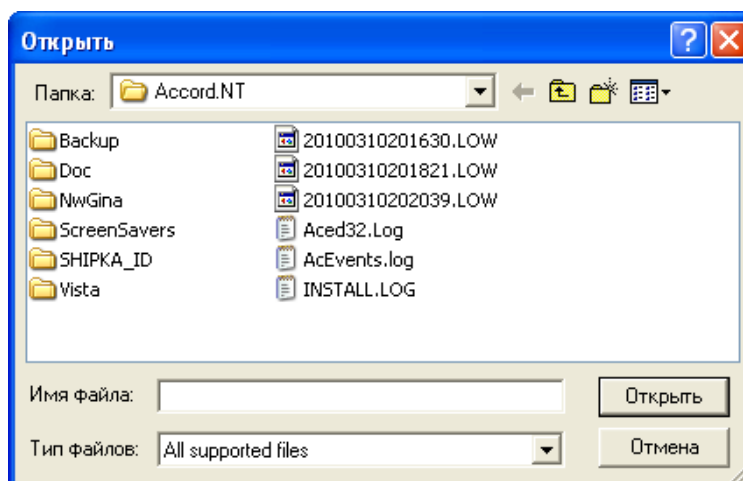


Рис. 1. Окно выбора файла журнала.

Выбрав "мышью" нужный файл, нажмите кнопку "Открыть". На экран выводится окно просмотра журнала, показанное на Рис. 2.

№	Дата	Время	Имя процесса	Результат	Код события	Параметр	Объект
01	10.03.2010	20:18:21:269	WINLOGON.EXE	OK	С:И	0	Login
02	10.03.2010	20:18:21:284	WINLOGON.EXE	OK	С:И	0	System: Windows XP [Build 2600 free. Service Pack 3], Acron.sys: v3.0.4.12
03	10.03.2010	20:18:21:300	WINLOGON.EXE	OK	С:И	0	Settings: SM=No, DA=Yes, MA=No, CP=No, DNSD=No, WLN=Yes, FPP=No
04	10.03.2010	20:18:23:363	WINLOGON.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\BDRP.DLL
05	10.03.2010	20:18:23:363	WINLOGON.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\KBDDUS.DLL
06	10.03.2010	20:18:29:441	WINLOGON.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\CSCUL.DLL
07	10.03.2010	20:18:29:472	WINLOGON.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\MSXML3.DLL
08	10.03.2010	20:18:29:503	WINLOGON.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\POWRPROF.DLL
09	10.03.2010	20:18:29:519	WINLOGON.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\DCDDLL.DLL
10	10.03.2010	20:18:29:863	SVCHOST.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WUAPI.DLL
11	10.03.2010	20:18:29:863	DWRCS.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WTSAPI32.DLL
12	10.03.2010	20:18:29:878	DWRCS.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WINSTA.DLL
13	10.03.2010	20:18:29:894	DWRCS.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\DWRCSL3.EXE
14	10.03.2010	20:18:29:909	SVCHOST.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WUUPS.DLL
15	10.03.2010	20:18:29:925	SVCHOST.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WSCNTFY.EXE
16	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\NTDLL.DLL
17	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\KERNEL32.DLL
18	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\DWRCSL3.EXE
19	10.03.2010	20:18:30:066	WSCNTFY.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\MM32.DLL
20	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\USER32.DLL
21	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\GDI32.DLL
22	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\MM32.DLL
23	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\ADVAPI32.DLL
24	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\RPCRT4.DLL
25	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\SF11R32.DLL
26	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\PROGRAMS\KASPER\KASPER\2.0\FVADIALHK.DLL
27	10.03.2010	20:18:30:066	WSCNTFY.EXE	OK	Exec	H=0	C:\PROGRAMS\KASPER\KASPER\2.0\FVADIALHK.DLL
28	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\SHLWAPI.DLL
29	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\MSVCRT.DLL
30	10.03.2010	20:18:30:066	DWRCSL3.EXE	OK	Exec	H=0	C:\PROGRAMS\KASPER\KASPER\2.0\FVADIALHK.DLL
31	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\VERSION.DLL
32	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\SHELL32.DLL
33	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\COMMON-CONTROLS_6595B64144CCF1DF_6.0.2600.5512_x-ww_35D4CE83.COM
34	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\OLE32.DLL
35	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WSOCK32.DLL
36	10.03.2010	20:18:30:081	WSCNTFY.EXE	OK	Exec	H=0	C:\PROGRAMS\KASPER\KASPER\2.0\FVADIALHK.DLL
37	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WS2_32.DLL
38	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WS2HELP.DLL
39	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WINMM.DLL
40	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\MRPC.DLL
41	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\UXTHEME.DLL
42	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\MSCFTIME.IME
43	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\PROGRAM FILES\MICROSOFT\FIREWALL CLIENT 2004\FWCSWP.DLL
44	10.03.2010	20:18:30:081	WSCNTFY.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\ACUSERMOD.DLL
45	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\OLEAUT32.DLL
46	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\MSWSOCK.DLL
47	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\HNETCFG.DLL
48	10.03.2010	20:18:30:081	DWRCSL3.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\WSHTCPIP.DLL

Рис. 2. Главное окно программы LOGVIEW.

По умолчанию в главном меню программы выводятся следующие параметры регистрации:

- дата;
- время с точностью до тысячных долей секунды;
- имя процесса, который выполнил операцию;
- результат операции:
 - НСД – попытка несанкционированного доступа;
 - ОК – нормальное выполнение операции;
 - Ошибка – системная ошибка при выполнении операции;
- код события (расшифровка кодов событий выводится в нижней строке состояния окна программы; полный список кодов событий приведен в Приложении 2 документа «Руководство администратора» (11443195.4012-019 90 02));
- параметр;
- объект.

Программу LOGVIEW.EXE можно запустить с ключом /ALL. В этом случае выводятся все поля базы данных регистрации. Эти поля предназначены только для разработчиков и описаны в SDK.

С помощью "мыши" можно изменять ширину колонок. В нижней панели окна выводится имя пользователя и рабочей станции, а также дата и время начала и окончания сеанса данного пользователя. Если сеанс был завершён не стандартными средствами ОС, а выключением питания компьютера, то в поле Logout Time выводится слово "RESET!!!".

В верхней части окна расположены функциональные кнопки. При установке на клавишу курсора мыши выводится подсказка.

Для работы с журналом доступны следующие команды:

- загрузить файл – выбор файла журнала для просмотра;

11443195.4012-019 99 02

- прочитать журнал АДЗ – просмотр журнала из АДЗ;
- на первую страницу – быстрый переход в начало файла;
- на страницу вперед – переход на следующую страницу;
- на страницу назад - переход на предыдущую страницу;
- на последнюю страницу – быстрый переход в конец файла;
- печать журнала (страницы) – вывод текущей страницы в текстовый файл;
- установить/снять все фильтры;
- выход из программы.

2.2 Просмотр журнала регистрации событий

В этом режиме для удобства просмотра и анализа журнала можно устанавливать фильтры для отдельных полей базы данных.

2.2.1 Фильтрация по имени процесса

Установите курсор на заголовке колонки "Имя процесса" и нажмите левую кнопку мыши. На экран выводится окно установки фильтра (Рис. 3.).

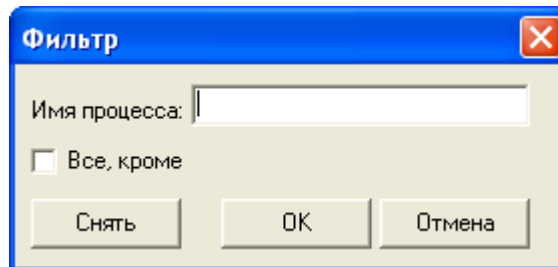


Рис. 3. Установка фильтра по имени процесса.

Можно ввести как полное имя процесса, так и часть имени. После нажатия на кнопку "ОК" происходит поиск в журнале, и на экран выводятся только те записи, которые удовлетворяют заданному критерию фильтрации.

Поиск производится без учета регистра введенных символов.

2.2.2 Фильтрация по результату операции

Установите курсор на заголовке колонки "Результат операции" и нажмите левую кнопку мыши. На экран выводится окно установки фильтра, показанное на Рис. 4.

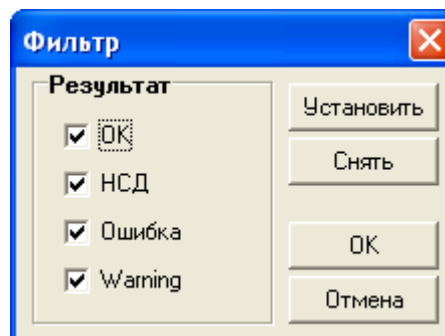


Рис. 4. Установка фильтра по результату операции.

Нажатием на левую клавишу "мыши" можно установить/сбросить отметку возле каждой операции.

После нажатия кнопки "ОК" на экран выводятся только те события, результат которых совпадает с операциями, отмеченными для фильтрации.

2.2.3 Фильтрация по коду события

Установите курсор на заголовке колонки "Код события" и нажмите левую кнопку мыши. На экран выводится окно выбора фильтров, показанное на Рис. 5.

Все события, регистрируемые подсистемой регистрации комплекса "Аккорд-NT/2000", разделены на пять групп: "Сообщения СЗИ", "Хранитель экрана", "Проверка файлов", "Файловые операции", "Реестр".

Для каждой группы событий можно установить, или снять отметку фильтрации.

При нажатии на кнопку "Выбор" выводится полный список событий данной группы.

Для каждого события в группе также можно установить метку фильтрации.

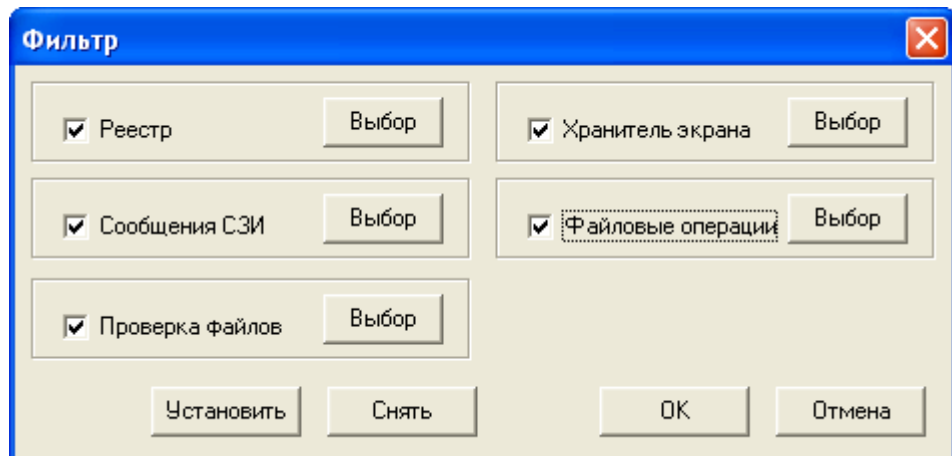


Рис. 5. Установка фильтров кодов событий.

Рассмотрим подробнее регистрируемые события.

Сообщения СЗИ:

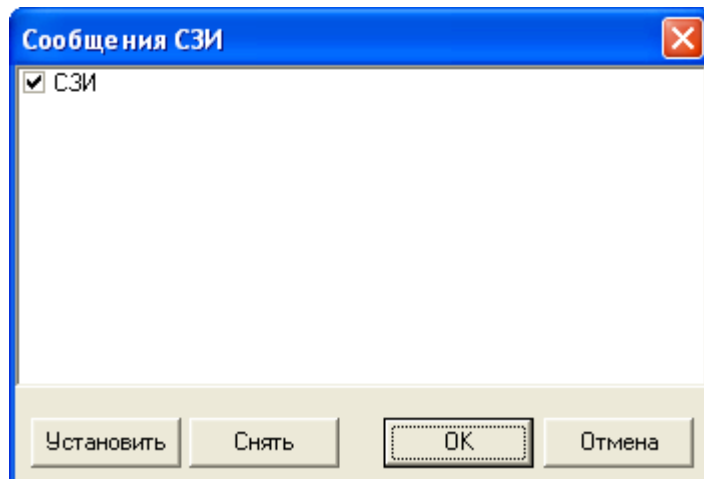


Рис. 6. Установка фильтра для событий класса "Сообщения СЗИ".

В этой группе событий фиксируется только одно событие – СЗИ – это сообщения, возникающие при работе СЗИ "Аккорд-NT/2000". Хотя событие одно, но его содержание может быть различным, и текст этих сообщений отображается в поле "Объект".

Хранитель экрана

В этой группе собраны события, которые относятся к обработке операций блокировки и разблокировки экрана и клавиатуры (Рис. 7.).

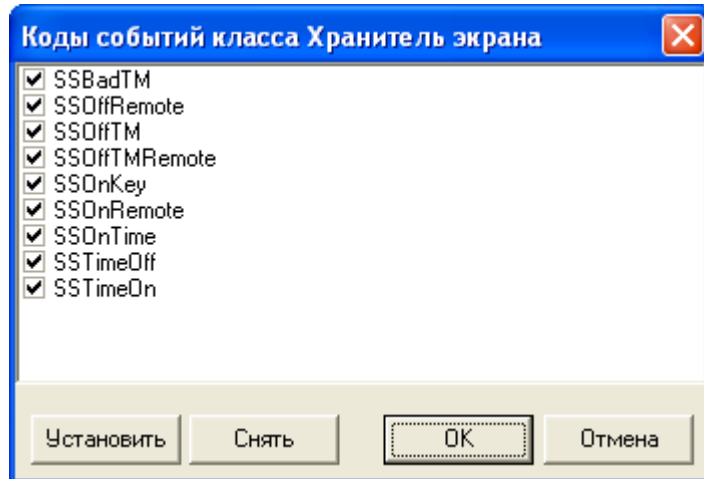


Рис. 7. Установка фильтра для событий класса "Хранитель экрана".

Проверка файлов

В этой группе собраны события, которые относятся к операциям контроля целостности файлов и процессов (Рис. 8.).

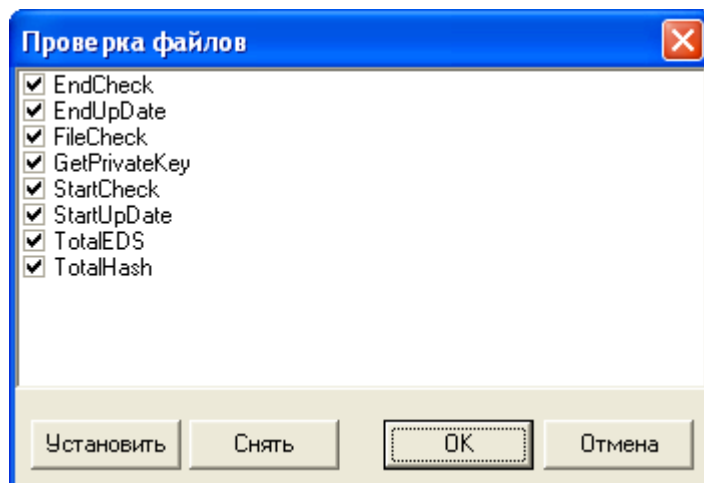


Рис. 8. Установка фильтра для событий класса "Проверка файлов".

Файловые операции*

Это группа событий, которые относятся к контролю файловых операций (Рис. 9.).

* в Windows NT/2000 все операции с файлами и каталогами на жестком диске выполняются в защищенном режиме (Protected Mode). Поэтому выбрано такое обозначение класса регистрируемых событий

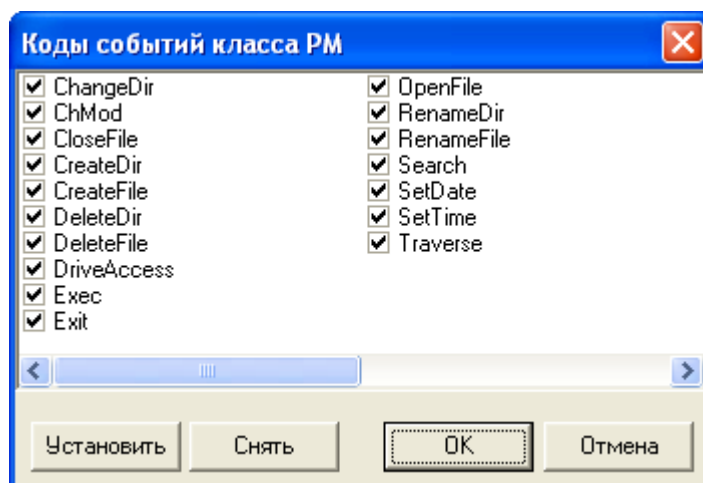


Рис. 9. Установка фильтра для событий класса "РМ".

Реестр

События данной группы регистрируются только в том случае, когда в опциях СЗИ установлен флаг "Контролировать доступ к реестру". Список событий на Рис. 10.

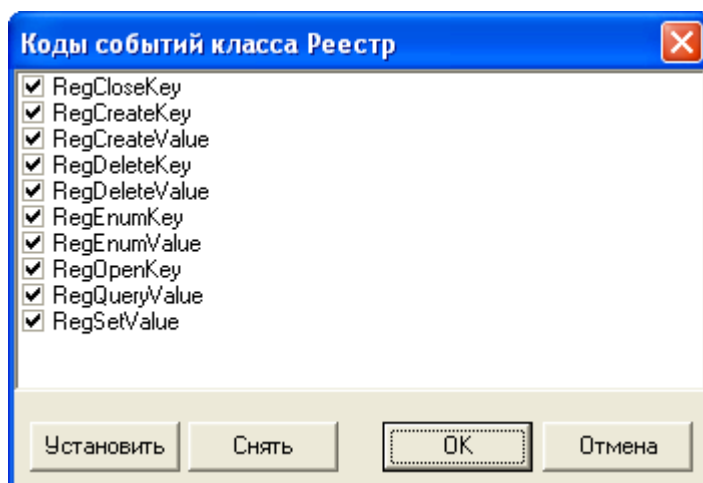


Рис. 10. Установка фильтра для событий класса "Реестр".

Следует отметить, что для операций в журнале событий можно получить полное название операции. Для этого достаточно установить курсор на нужный Вам код события и нажать левую кнопку "мыши". В нижней строке окна появится полное название события.

2.2.4 Фильтрация по наименованию объекта

Установите курсор на заголовке колонки "Объект" и нажмите левую кнопку мыши. На экран выводится окно установки фильтра (Рис. 11.).

3.1 Архивация/Разархивация журналов

С помощью программы LOGBASE.EXE администратором БИ может осуществляться архивация/разархивация журналов.

При нажатии кнопки "Поместить в архив" главного меню программы (см. Рис. 12) выводится окно выбора файла для его архивации, показанное на Рис.13.

Если файл архива уже существует, то его можно выбрать мышью, если в строке "Имя файла" ввести наименование нового архива - то он будет создан.

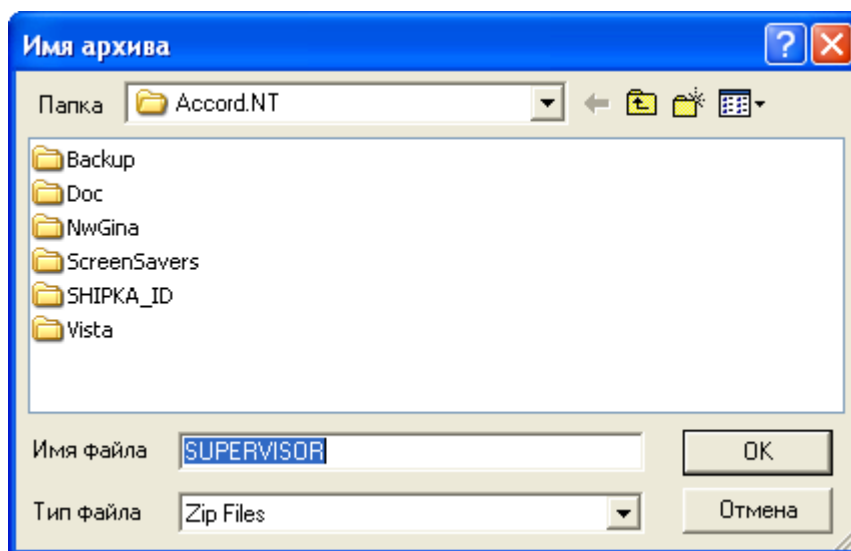


Рис. 13. Окно выбора файла для архивации.

Далее в открывшемся окне необходимо выбрать файл, или группу файлов для архивации.

При нажатии кнопки "Извлечь из архива" главного меню программы (см. Рис. 12.) выводится окно выбора файла из архива, показанное на Рис.14.

Файл архива можно выбрать мышью, или в строке "Имя файла" ввести имя архива. В открывшемся окне можно выбрать каталог, в который будут помещены разархивированные файлы журнала. При этой операции происходит извлечение всех файлов из выбранного архива.

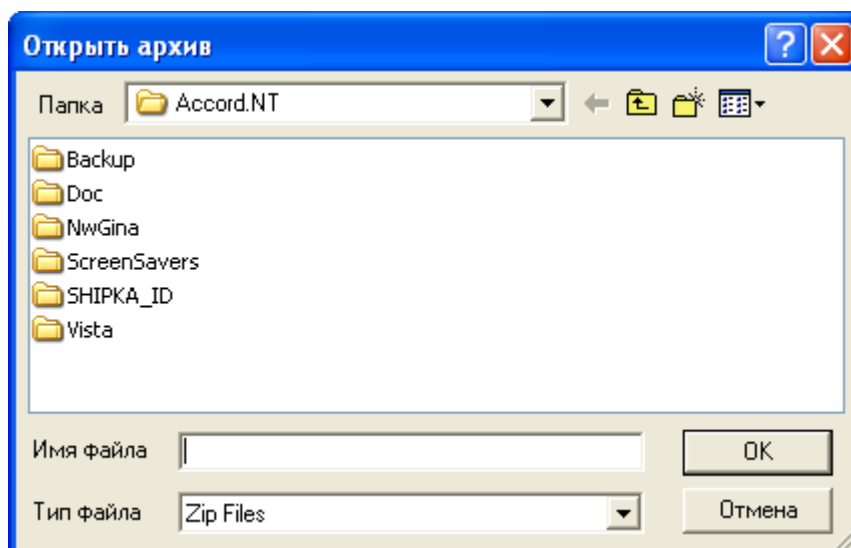


Рис. 14. Окно выбора файла архива для извлечения журнала (разархивации).

4 ФОРМИРОВАНИЕ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА НА ОСНОВЕ ИНФОРМАЦИИ В ЖУРНАЛЕ РЕГИСТРАЦИИ СОБЫТИЙ

В состав комплекса “Аккорд NT/2000” входят две сервисные утилиты, которые позволяют на основе информации, записанной в журнале регистрации событий, создавать файлы с описанием правил разграничения доступа. Администратор с помощью редактора ПРД ACED32.EXE может импортировать данные из файлов с расширением .prd в настройки пользователя, или группы пользователей. Программа LogToPRD.EXE формирует ПРД для объектов на основе дискреционных атрибутов доступа. Программа AcProc.EXE формирует ПРД для процессов на основе мандатных атрибутов доступа. Работа этих программ основывается на анализе журналов регистрации событий. Выполняется просмотр выбранного файла журнала, и объекты помещаются в список. Администратор может выбрать нужные объекты, установить для них атрибуты доступа и сохранить результат в файле, который в дальнейшем может быть импортирован программой-редактором.

4.1 Работа с программой LogToPRD

При запуске программы LogToPRD.EXE на экран выводится главное окно, разделенное на два поля (Рис.15.). Левое поле предназначено для списка объектов, сформированного на основе анализа журнала. Правое поле – это список выбранных объектов с установленными атрибутами доступа, который предназначен для сохранения.

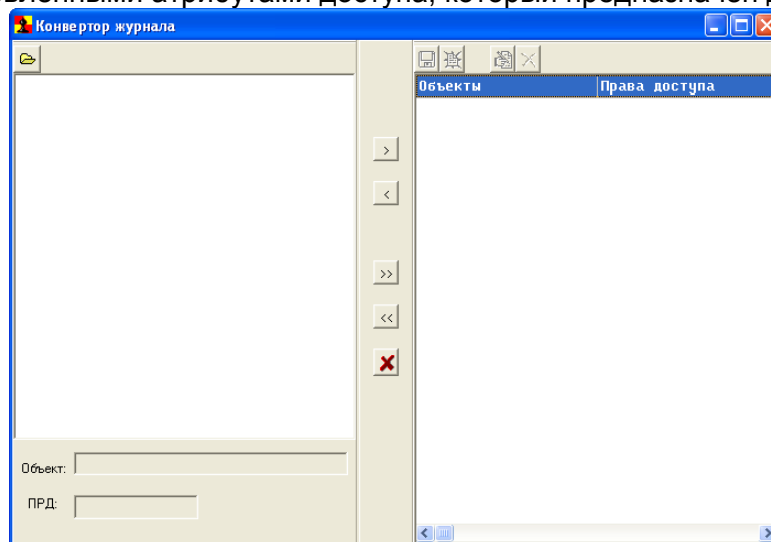


Рис. 15. Главное окно программы.

Для выбора анализируемого журнала нажмите кнопку с изображением папки в левом верхнем углу. Открывается окно выбора файла журнала (Рис. 16.).

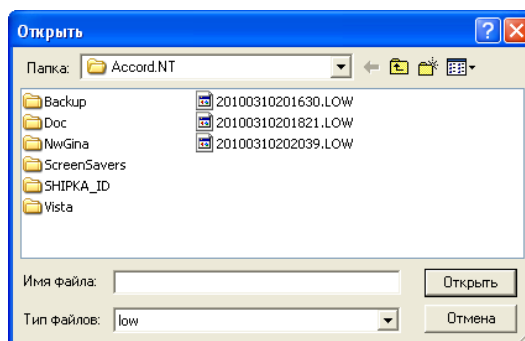


Рис. 16. Выбор журнала для анализа.

11443195.4012-019 99 02

Отметьте файл журнала, который необходимо проанализировать и нажмите кнопку «Открыть». На экран выводится сообщение «Выполняется обработка журнала. Ждите...». После завершения обработки журнала в левом поле главного окна отображается список объектов в виде дерева каталогов и файлов (Рис. 17.).

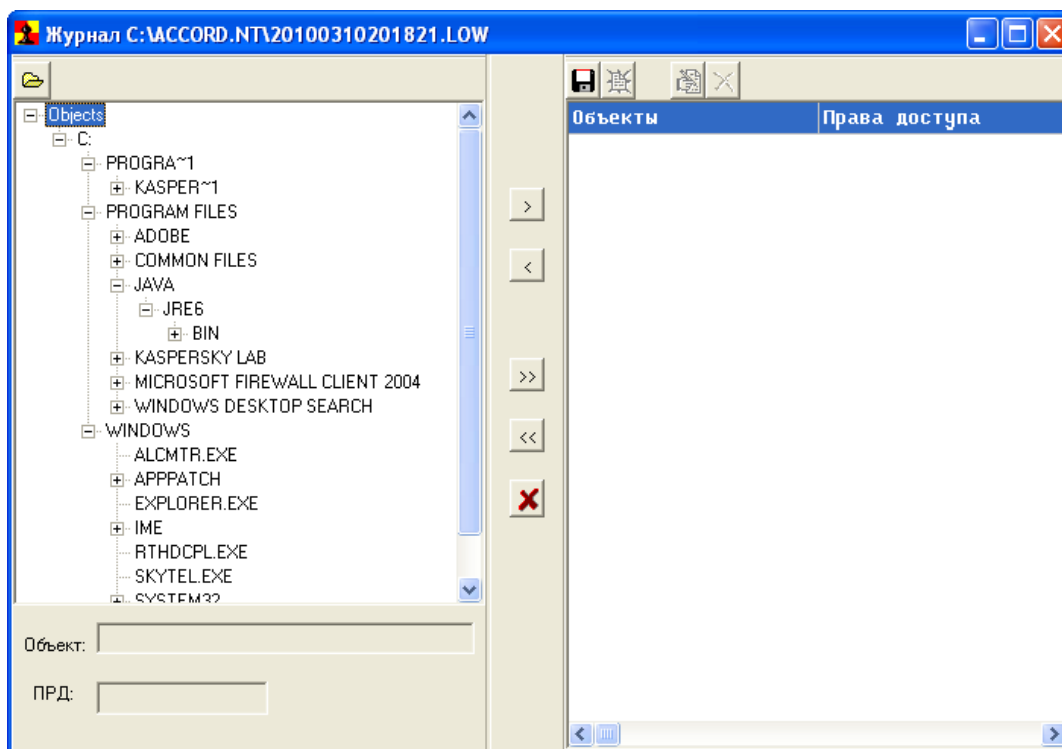


Рис. 17. Список объектов, полученный на основе анализа журнала.

С левой стороны от наименования каталога (подкаталога) выводится знак <+>, если в этом каталоге имеются вложенные файлы и папки. Щелчок левой кнопкой мыши на этом знаке открывает каталог на следующий уровень. Чтобы поместить объект в правое поле, нужно отметить его в списке и нажать одну из кнопок с изображением стрелок. Нажатие кнопки с одиночной стрелкой (>) помещает в список ПРД имя выбранного файла, или каталога. Нажатие кнопки с двойной стрелкой (>>) помещает в список ПРД все объекты из отмеченного каталога. Чтобы удалить из списка ПРД какой-либо объект, нужно отметить его и нажать клавишу с одиночной обратной стрелкой (<). Нажатие двойной обратной стрелки (<<) полностью очищает список ПРД в правом поле окна.

После того, как список объектов сформирован, необходимо назначить правила разграничения доступа каждому объекту. Окно установки ПРД открывается при двойном щелчке мыши на строке в правом списке, или после выбора строки и нажатия клавиши <Enter> (Рис. 18.).

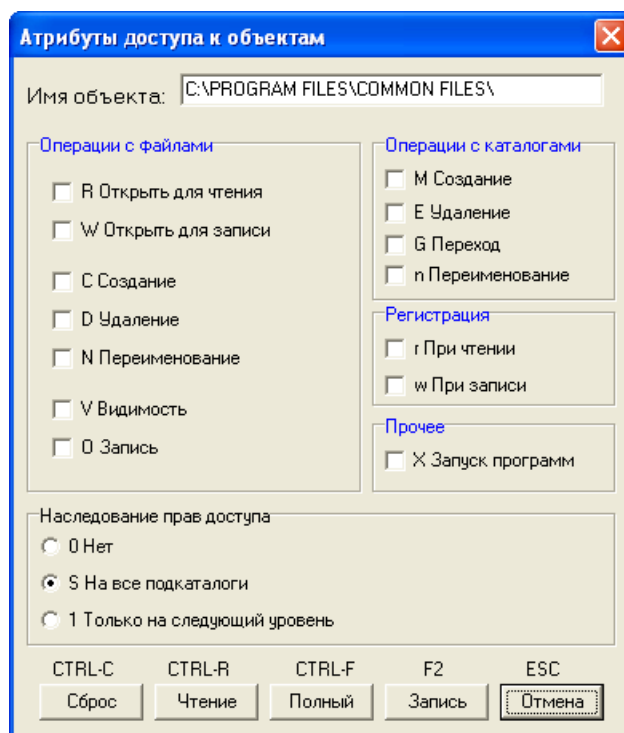


Рис. 18. Окно установки атрибутов доступа.

После того, как установлены атрибуты доступа к объектам, следует сохранить настройки в файл. Нажмите кнопку с изображением дискеты над правым полем главного окна программы. Открывается диалог выбора файла для сохранения (Рис.19.).

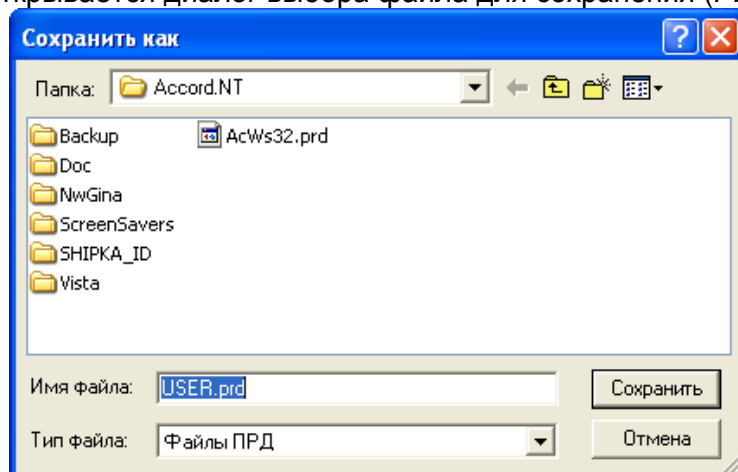


Рис.19. Выбор файла для сохранения ПРД.

Можно выбрать существующее имя файла, или ввести новое. Изменение расширения файла не допускается. Данные из сохраненного файла можно импортировать пользователю, или группе пользователей в программе ACED32.EXE.

4.2 Работа с программой AcProc

При запуске программы AcProc.EXE на экран выводится окно, представленное на Рис.20.

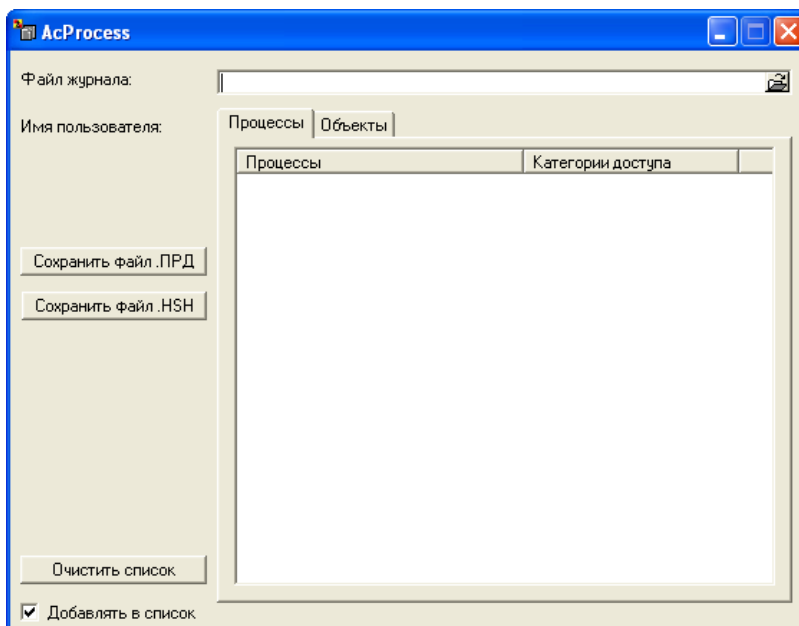


Рис.20. Главное окно программы AcProc.EXE.

Поле “Файл журнала” предназначено для выбора анализируемого журнала регистрации. Щелкните мышью по кнопке с изображением папки в правой части поля. Открывается окно выбора журнала (Рис.16.). Отметив нужный файл, нажмите кнопку “Открыть”. Программа сканирует журнал и выводит в окне список процессов с указанием уровня доступа (Рис.21.). Если установлен флаг “Добавлять процессы в список”, то можно собрать в одном списке процессы из нескольких журналов. Для этого необходимо выполнить выбор следующего журнала. Процессы, которых нет в списке, будут добавлены. Эту процедуру можно повторять несколько раз.

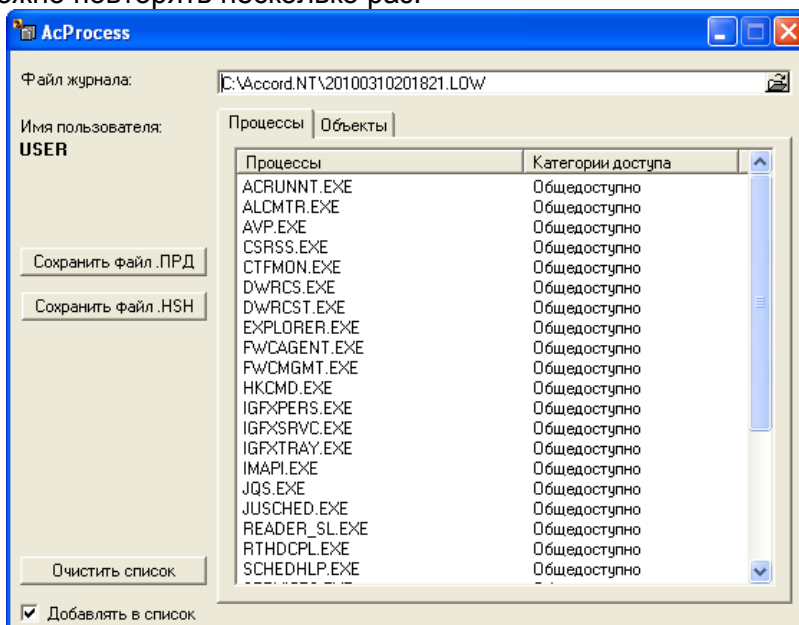


Рис.21. Сформированный список процессов.

При включении в список все процессы получают самый низкий уровень доступа. Администратор может изменить уровень доступа процесса в соответствии с принятой политикой безопасности. Для изменения уровня доступа необходимо двойным щелчком мыши выбрать нужный процесс. На экран выводится окно установки (Рис. 22.).

11443195.4012-019 99 02

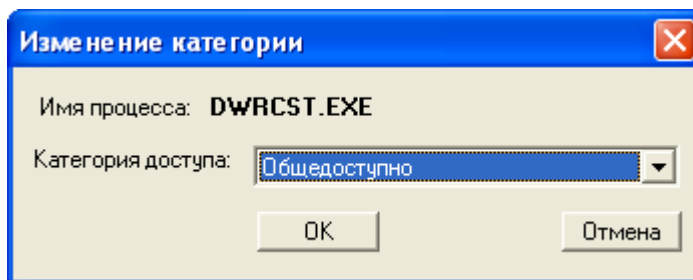


Рис.22. Установка нового уровня доступа.

Нажатие кнопки со стрелкой в поле “Категория доступа” выводит список установленных в СЗИ уровней доступа, которые можно присвоить данному процессу.

После того, как список полностью откорректирован, необходимо выполнить сохранение настроек в файле правил доступа. Нажмите кнопку “Сохранить файл ПРД”. В окне сохранения (Рис.19.) введите имя файла и нажмите кнопку “Сохранить”. Данные из сохраненного файла можно импортировать пользователю, или группе пользователей в программе ACED32.EXE.

Список исполняемых файлов можно сохранить в файл с расширением .HSH. Этот файл предназначен для импорта списка файлов в процедуру контроля целостности в программе-редакторе ACED32.EXE (см. документ «УСТАНОВКА ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА ПРОГРАММА ACED32.» п.7.10). Например, файлы, которым установлены уровни доступа, будут контролироваться на целостность в процедуре динамического контроля перед каждым запуском, что повышает уровень защищенности системы. Для сохранения списка нажмите кнопку “Сохранить файл HSH”. В окне сохранения (Рис.23.) введите имя файла и нажмите кнопку “Сохранить”. Данные из сохраненного файла можно импортировать пользователю в программе ACED32.EXE.

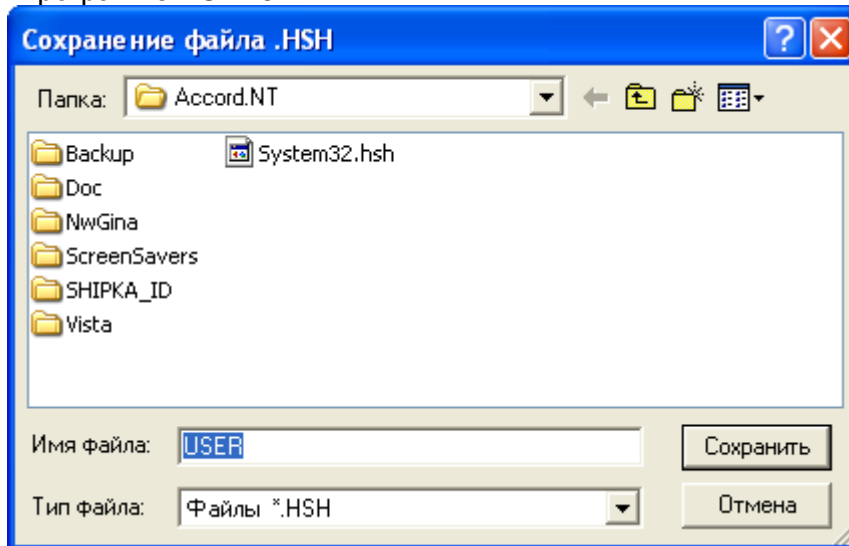


Рис. 23. Сохранение списка файлов для процедуры контроля целостности.

Внимание! После импорта файлов в редакторе ACED32 необходимо пересчитать контрольные суммы.

Работа с программой ReadPrd

Для быстрого просмотра файлов, содержащих описание правил доступа (файлы с расширением .PRD) предназначена программа ReadPrd.EXE. При запуске программы на экран выводится окно, представленное на Рис.24. Описание параметров правил

разграничения доступа приведены в документе «Установка правил разграничения доступа. Программа ACED32 (11443195.4012-019 97 02)»

Для выбора файла нажмите кнопку <Открыть файл> в левом верхнем углу основного окна. На экран выводится окно выбора файла для просмотра (Рис. 25.). Отметив нужный файл, нажмите кнопку «Открыть». Программа считывает данные из файла и выводит в различных окнах, отмеченных закладками, список процессов с указанием уровня доступа, список объектов с присвоенными правилами доступа и другие параметры пользователя (Рис.26.).

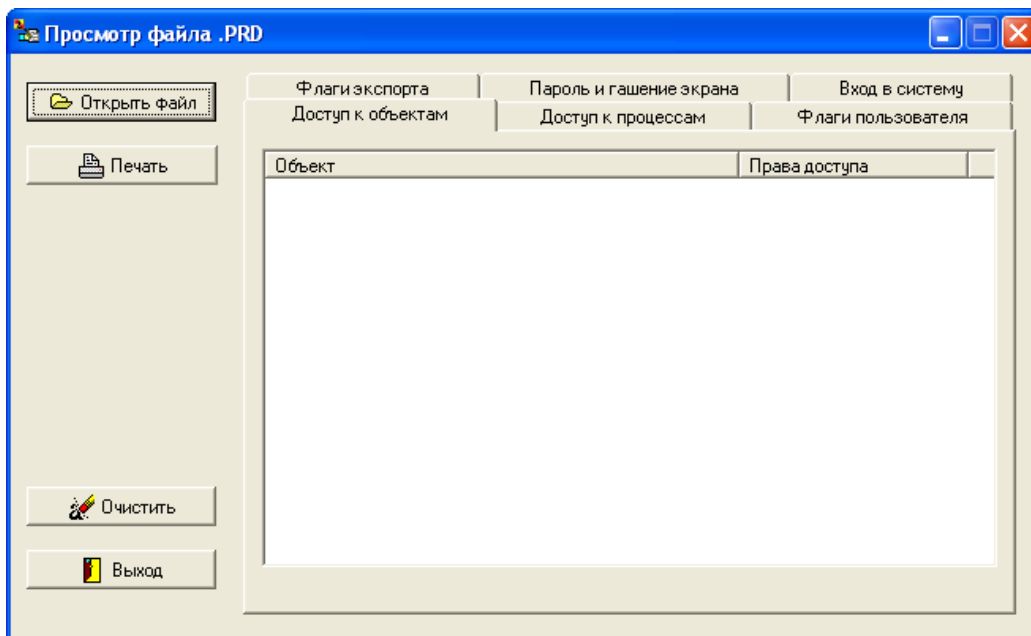


Рис. 24. Главное окно программы ReadPrd.

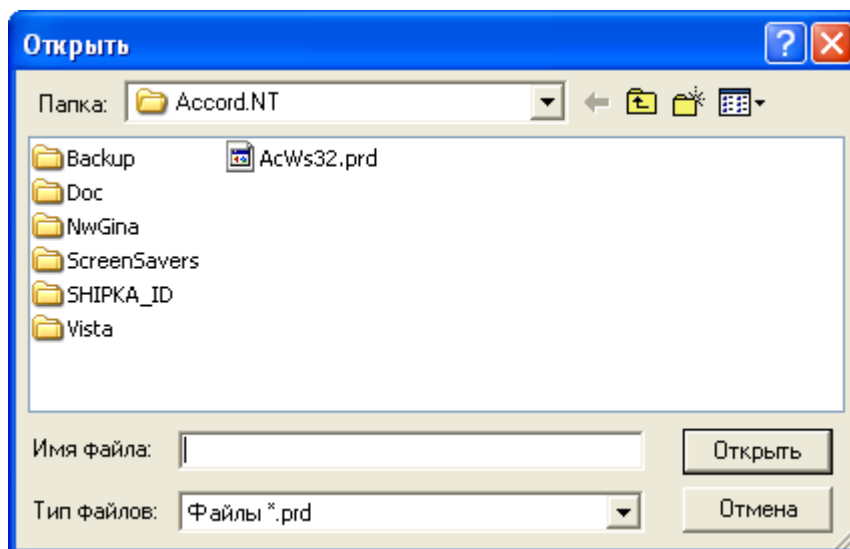


Рис. 25. Окно выбора файла PRD для просмотра.

Объем отображаемой информации зависит от того, какой программой создан файл PRD. Если файл создавался программой LogToPrd.EXE, то доступны только правила дискреционного доступа к объектам. Если файл был создан программой AcProc.EXE, то доступен список процессов с присвоенными уровнями мандатного доступа. Если файл PRD экспортировался из программы Aced32.EXE, то доступны для просмотра те параметры

11443195.4012-019 99 02

пользователя, которые отмечались флагами в процедуре экспорта.

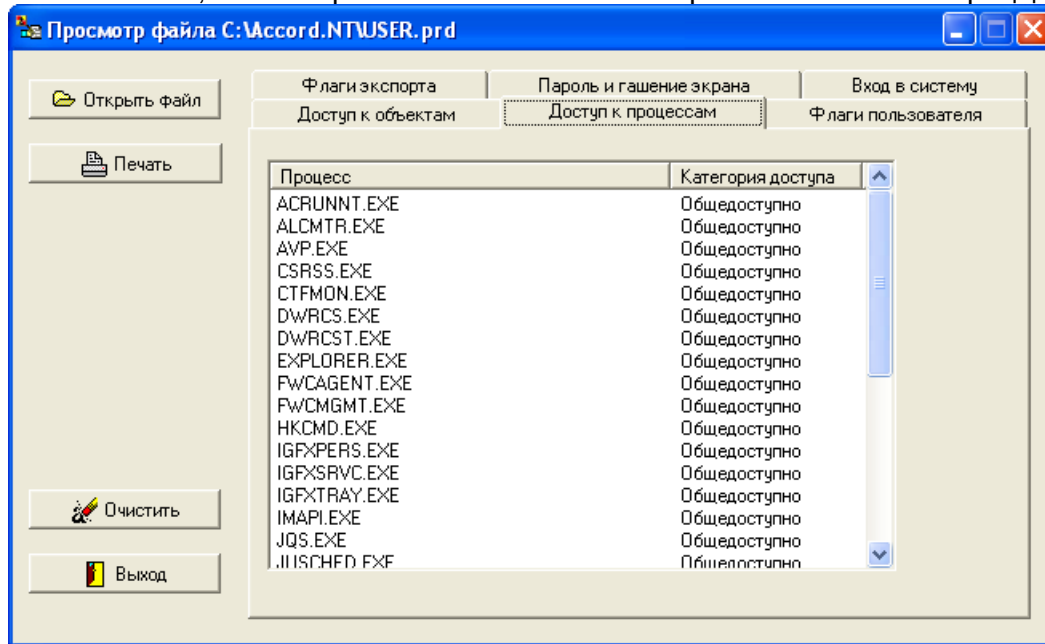


Рис. 26. Данные о правилах доступа и настройках пользователя.