

ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО



систем автоматизированного
проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.4012-036 99 -ЛУ

**Программно-аппаратный комплекс
средств защиты информации от
несанкционированного доступа
“АККОРД-Win32” (версия 4.0)**

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

11443195.4012-036 99

Литера О₁

АННОТАЦИЯ

Программа LOGVIEW.EXE предназначена для работы с журналами регистрации, которые создаются в процессе функционирования подсистемы разграничения доступа комплекса СЗИ НСД "Аккорд-Win32" v.4.0 (ТУ 4012-036-11443195-2010).

Программа используется администратором безопасности информации и входит в состав специального ПО комплекса СЗИ НСД "Аккорд".

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	10
2.4	ВЫХОД ИЗ ПРОГРАММЫ	10
3	ПРЕДВАРИТЕЛЬНАЯ СОРТИРОВКА ЖУРНАЛОВ.....	11
3.1	АРХИВАЦИЯ/РАЗАРХИВАЦИЯ ЖУРНАЛОВ.....	11
4	ФОРМИРОВАНИЕ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА НА ОСНОВЕ ИНФОРМАЦИИ В ЖУРНАЛЕ РЕГИСТРАЦИИ СОБЫТИЙ.....	12
4.1	РАБОТА С ПРОГРАММОЙ LOGTOPRD	13
4.2	РАБОТА С ПРОГРАММОЙ ACPROC	16
4.3	РАБОТА С ПРОГРАММОЙ READPRD	20

ПРИНЯТЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

PM (Protected Mode)	- защищенный режим работы 32-битных приложений
Registry (реестр)	- главная иерархическая база данных Windows, 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

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

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

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" 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.

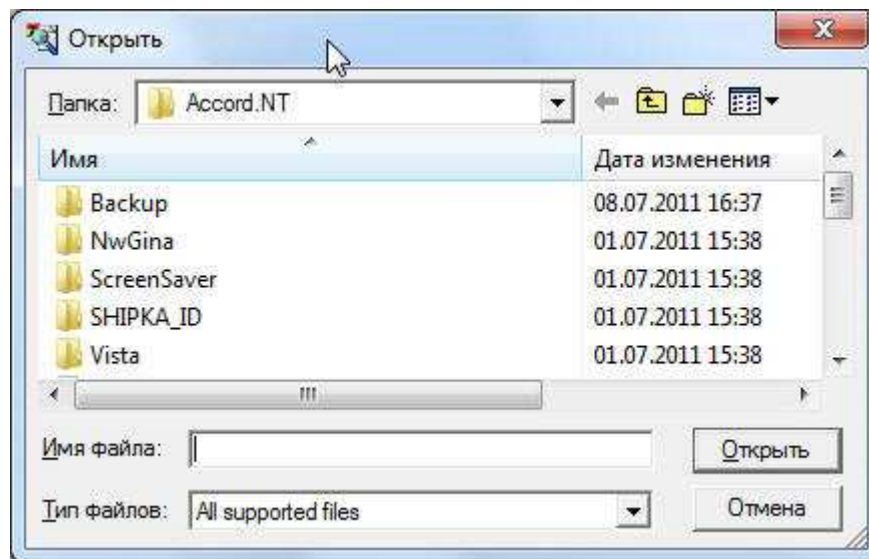


Рис.1. Окно выбора файла журнала.

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
1	04.07.2011	17:00:49:034	SYSTEM	OK	СЗМ	0	Login
2	04.07.2011	17:00:49:034	SYSTEM	OK	СЗМ	0	System: Windows 7 [Build 7601 free, Service Pack 1], Acrun.sys: v4.0.2.20, SN=183554645
3	04.07.2011	17:00:49:034	SYSTEM	OK	СЗМ	0	Settings: SM=No, DA=Yes, MA=No, CP=No, DNSD=No, WLN=Yes, FPP=No
4	04.07.2011	17:00:52:221	SYSTEM	OK	Ехес	H=0	C:\WINDOWS\SYSTEM32\SMSS.EXE
5	04.07.2011	17:00:52:221	SMSS.EXE	OK	Ехес	H=0	C:\WINDOWS\SYSTEM32\AUTOCHK.EXE
6	04.07.2011	17:00:52:221	SMSS.EXE	OK	СЗМ	0	Start disks checking
7	04.07.2011	17:00:52:221	AUTOCHK.EXE	OK	СЗМ	0	Stop disks checking
8	04.07.2011	17:00:52:221	AUTOCHK.EXE	OK	Exit	H=0	
9	04.07.2011	17:00:52:659	SYSTEM	НСД	Traverse	H=0	\DEVICE\HARDDISK\VOLUME1\
10	04.07.2011	17:00:52:659	SYSTEM	НСД	Traverse	H=0	\DEVICE\HARDDISK\VOLUME1\
11	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
12	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
13	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
14	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
15	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
16	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
17	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
18	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
19	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
20	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
21	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
22	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
23	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
24	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
25	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
26	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
27	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
28	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
29	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
30	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
31	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
32	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
33	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
34	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
35	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
36	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
37	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
38	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
39	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
40	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
41	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
42	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
43	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
44	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
45	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
46	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD
47	04.07.2011	17:00:52:659	SMSS.EXE	НСД	OpenFile	Read	\DEVICE\HARDDISK\VOLUME1\BOOT\BCD

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» (11443195.4012-036 90));
- 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;
- прочитать журнал АМДЗ – просмотр журнала из АМДЗ;
- 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.).

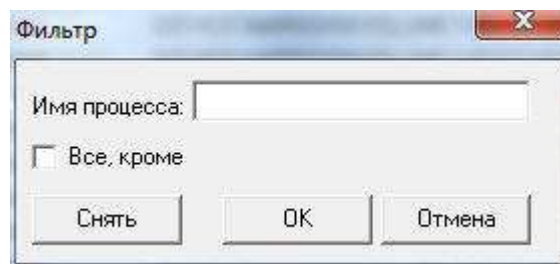


Рис. 3. Установка фильтра по имени процесса.

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.

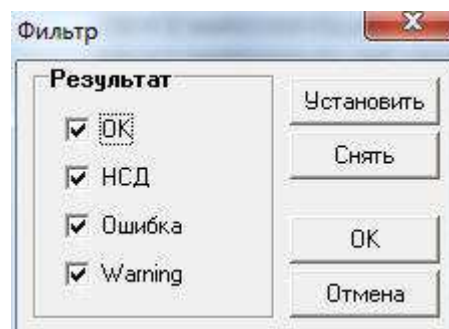


Рис. 4. Установка фильтра по результату операции.

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", 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.

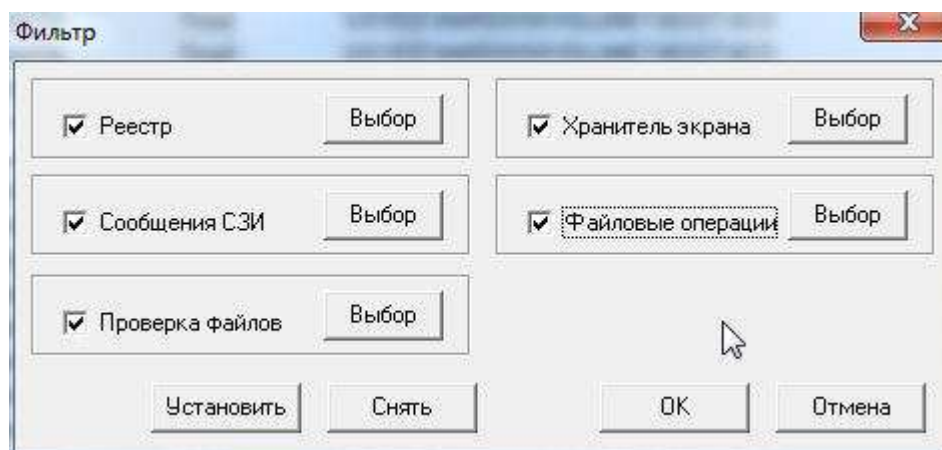


Рис. 5. Установка фильтров кодов событий.

Рассмотрим подробнее регистрируемые события.

Реестр

События данной группы регистрируются только в том случае, когда в опциях СЗИ установлен флаг "Контролировать доступ к реестру". Список событий на Рис. 6.

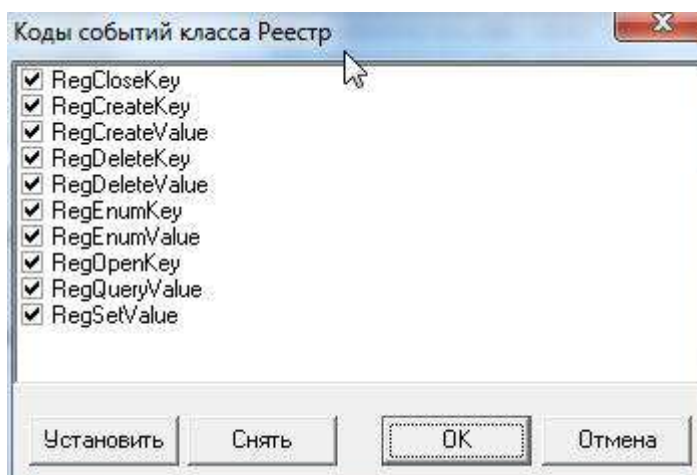


Рис. 6. Установка фильтра для событий класса "Реестр".

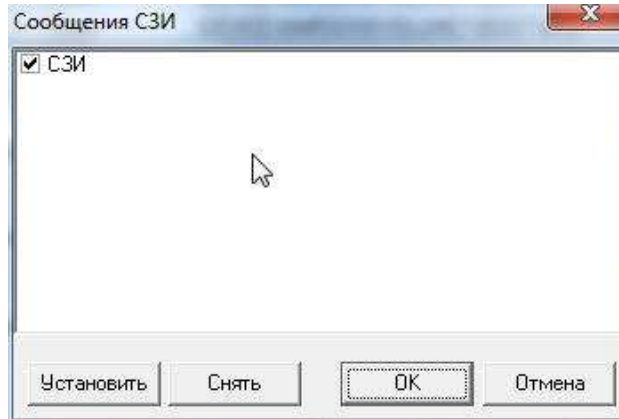
Сообщения СЗИ:

Рис. 7. Установка фильтра для событий класса "Сообщения СЗИ".

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

Проверка файлов

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

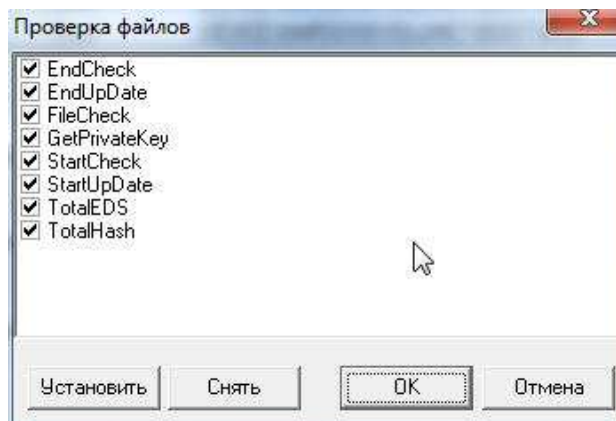


Рис. 8. Установка фильтра для событий класса "Проверка файлов".

Хранитель экрана

В этой группе собраны события, которые относятся к обработке операций блокировки и разблокировки экрана и клавиатуры (Рис. 9.).

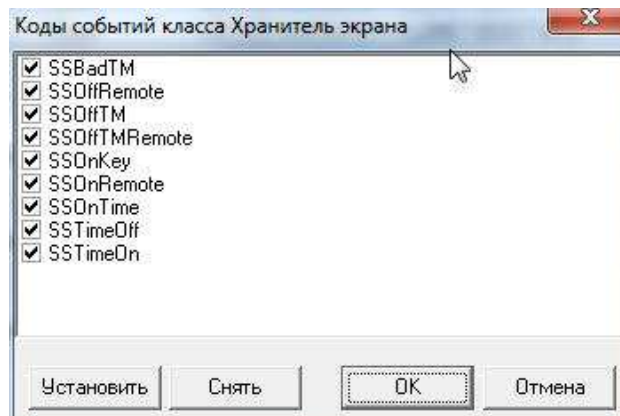


Рис. 9. Установка фильтра для событий класса "Хранитель экрана".

Файловые операции*

Это группа событий, которые относятся к контролю файловых операций (Рис. 10.).

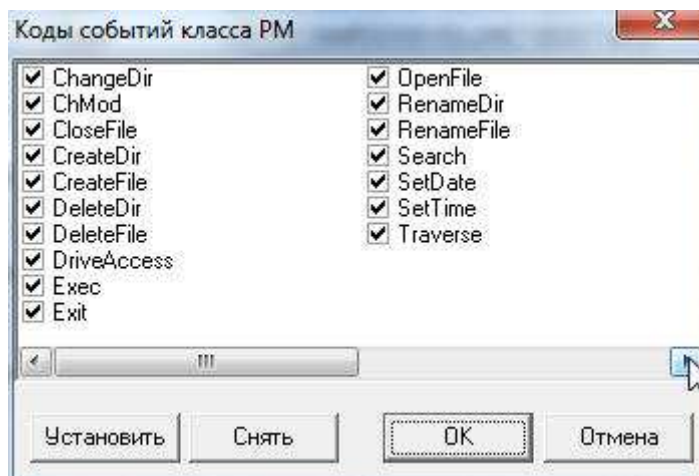


Рис. 10. Установка фильтра для событий класса "PM".

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.).

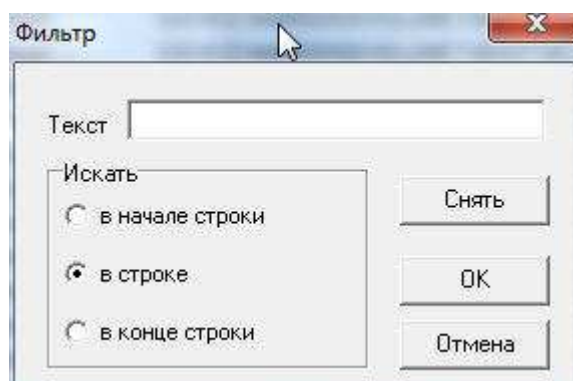


Рис. 11. Установка фильтра по наименованию объекта.

2.3 Вывод на печать

Для вывода на печатающее устройство необходимо левой клавишей "мыши" щелкнуть на кнопке с пиктограммой принтера в верхней строке окна. На печать выводится текущая страница. Такой режим печати предусмотрен потому, что объем журнала, особенно с высоким уровнем детализации, может составлять сотни килобайт. Наиболее рационально выбрать необходимую страницу, или нужный режим фильтрации, а потом производить печать постранично.

2.4 Выход из программы

Для выхода из программы необходимо вернуться в главное окно программы, показанное на Рис. 2. и нажать правую кнопку в верхней панели окна. Также можно завершить работу программы с использованием стандартной комбинации клавиш <Alt>-<F4>.

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

3 ПРЕДВАРИТЕЛЬНАЯ СОРТИРОВКА ЖУРНАЛОВ

Для более эффективной организации работы с журналами регистрации событий следует воспользоваться программой LOGBASE.EXE из каталога C:\ACCORD.NT.

Эта программа выполняет быстрый просмотр всех журналов, расположенных в текущем каталоге и выводит список этих журналов, отсортированный по именам пользователей и дате/времени. Главное окно программы показано на Рис. 12.

С использованием "мыши" следует отметить необходимые для просмотра файлы и нажать кнопку "Просмотр" - программой будут открыты выбранные для просмотра файлы.

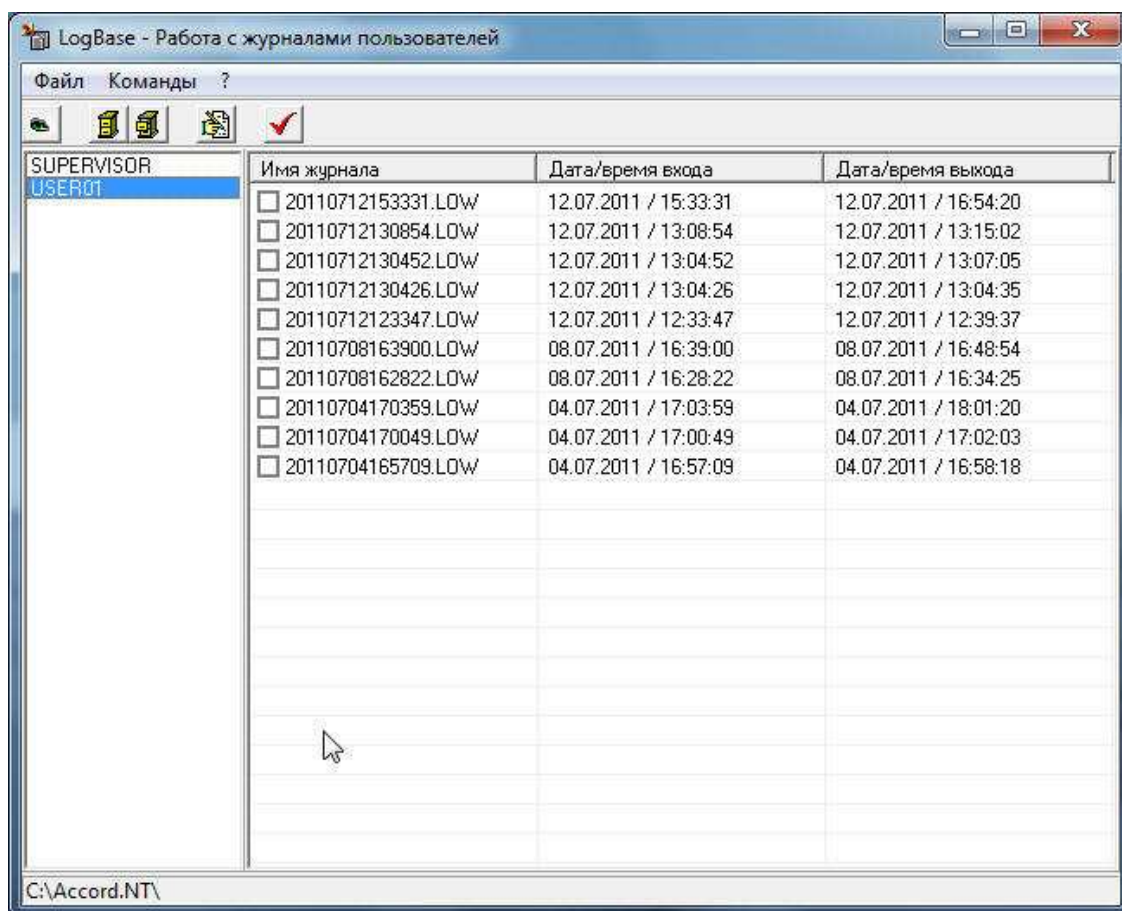


Рис. 12. Предварительная сортировка журналов регистрации.

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.

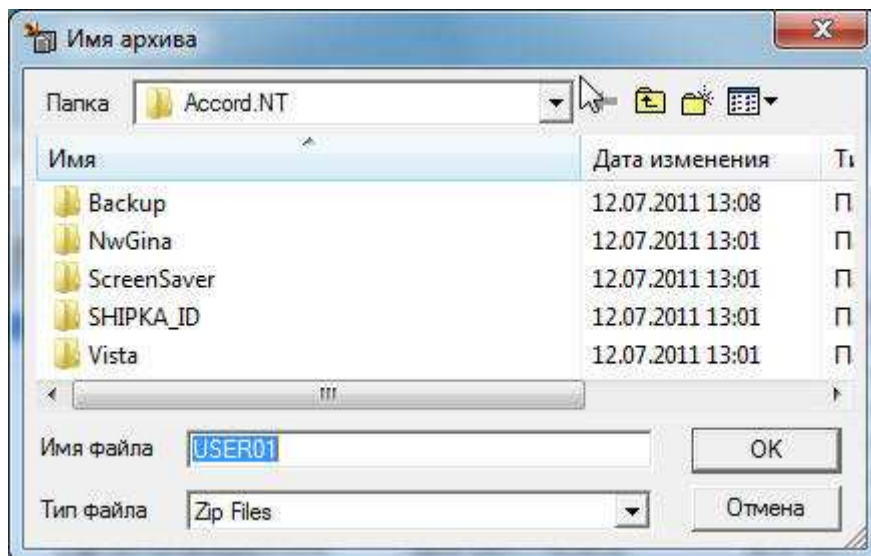


Рис. 13. Окно выбора файла для архивации.

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.

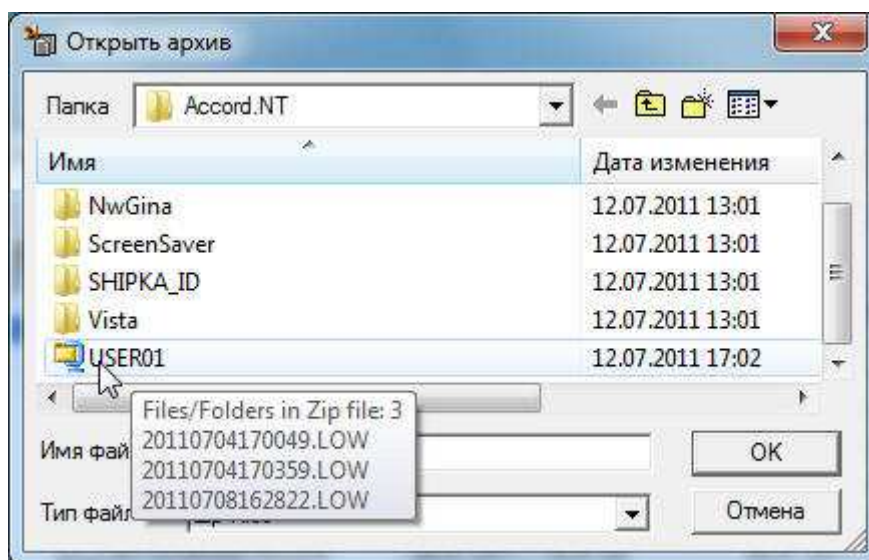


Рис. 14. Окно выбора файла архива для извлечения журнала (разархивации).

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

В состав комплекса "Аккорд" 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.

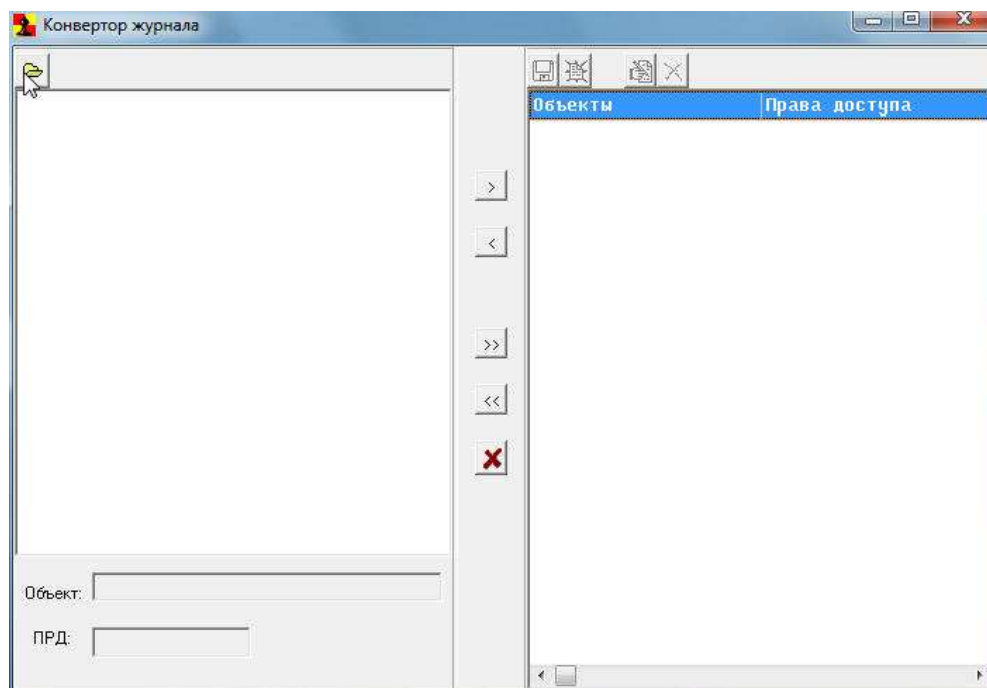


Рис. 15. Главное окно программы.

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

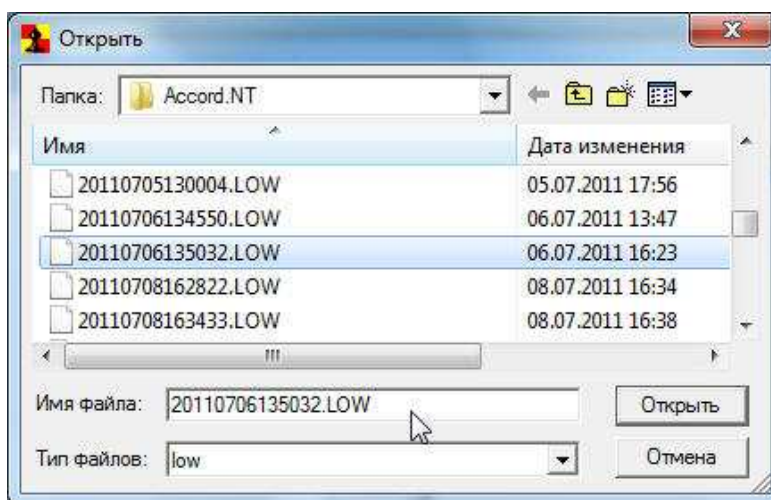


Рис. 16. Выбор журнала для анализа.

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.).

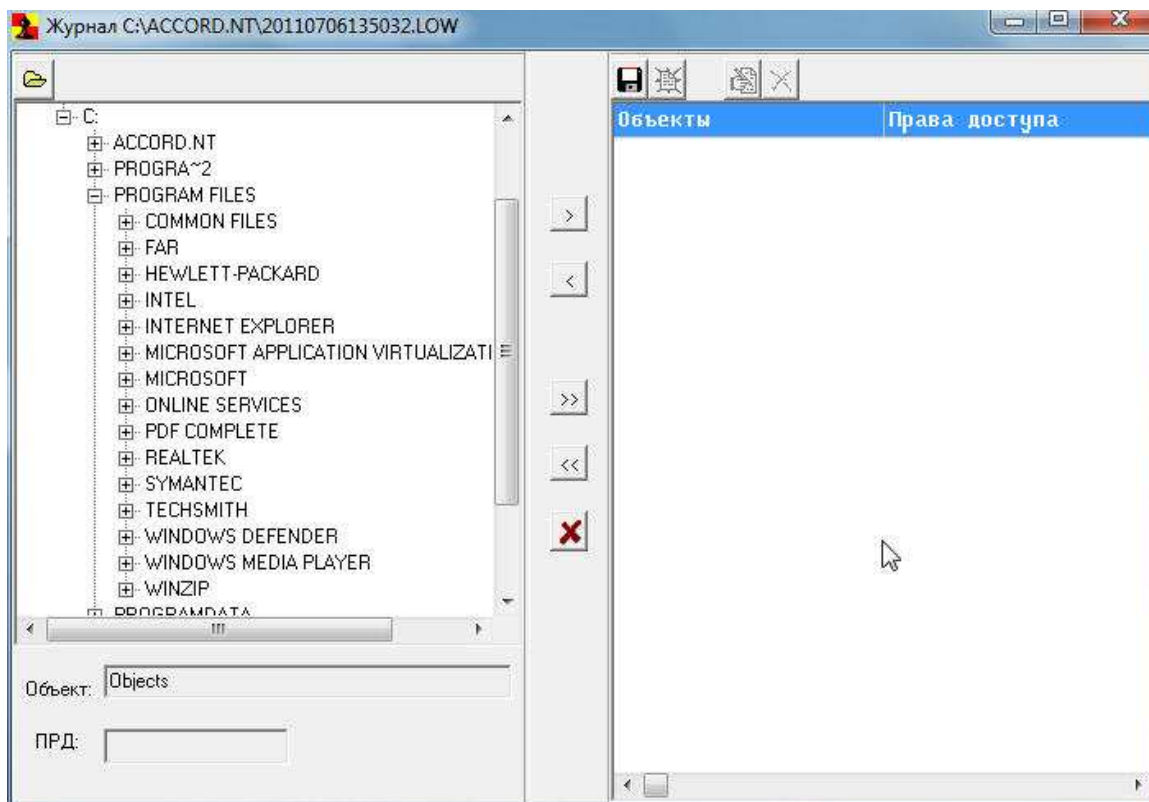


Рис. 17. Список объектов, полученный на основе анализа журнала.

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.).

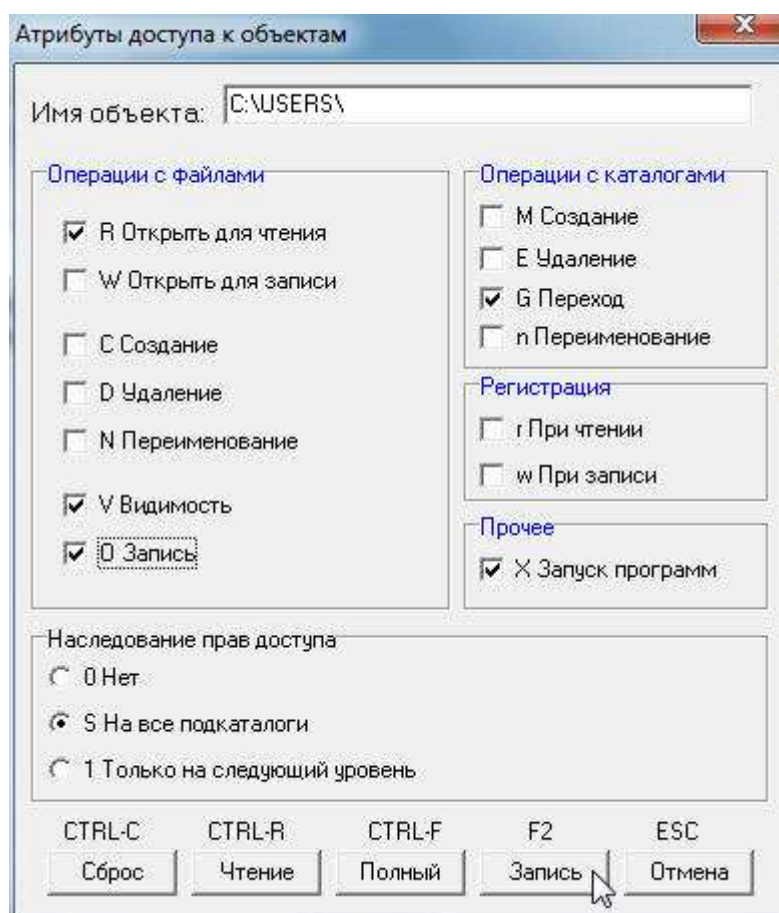


Рис. 18. Окно установки атрибутов доступа.

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.).

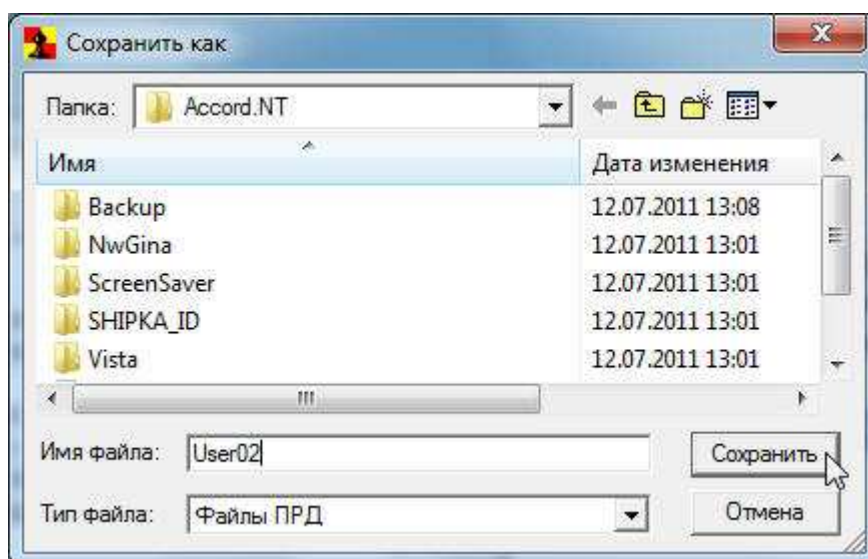


Рис.19. Выбор файла для сохранения ПРД.

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.

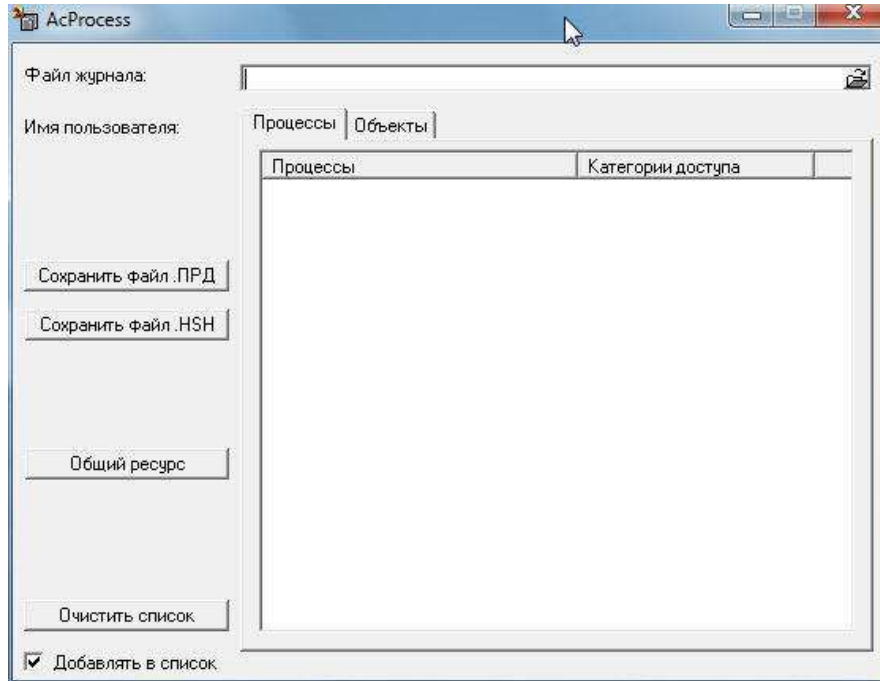


Рис.20. Главное окно программы AcProc.EXE.

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.).

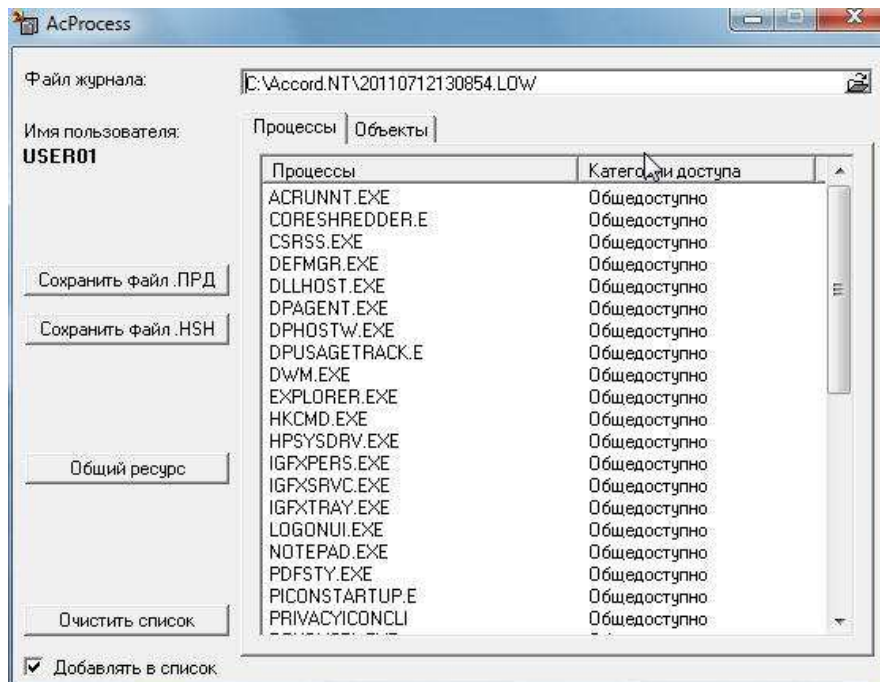


Рис.21. Сформированный список процессов.

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.

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.).

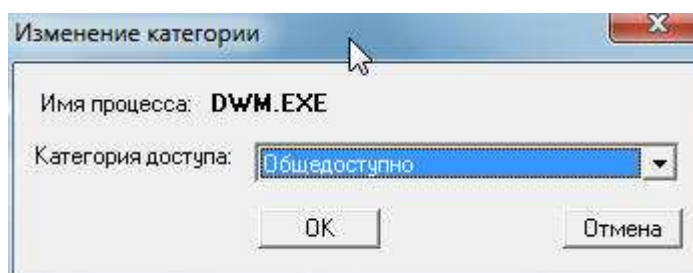


Рис.22. Установка нового уровня доступа.

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.

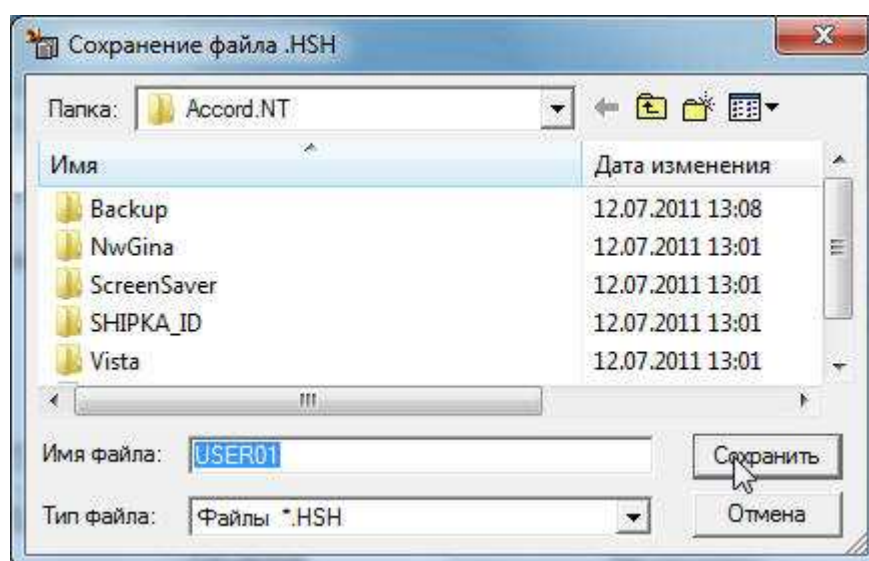


Рис. 23. Сохранение списка файлов для процедуры контроля целостности.

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

Еще одна полезная функция – это анализ работы процесса, запускаемого с разными уровнями доступа с объектами, которые имеют разные метки конфиденциальности. Данная функция помогает сформировать список объектов, которым нужно присвоить метку доступа «ОБЩИЙ_РЕСУРС». Это кнопка «Общий ресурс» в главном окне программы (Рис. 21.).

Для полноценного анализа событий детальность журнала исследуемого пользователя должна быть высокой, а режим работы монитора безопасности «мягкий». Контроль доступа включается дискреционный+мандатный+процессы. Процессы, который должен работать с разными ресурсами администратор устанавливает самый высокий уровень доступа и флаг «может понизить пользователь». После установки соответствующих настроек в программах AcSetup.exe и AcEd32.exe компьютер необходимо перезагрузить и начать работу в сессии того пользователя, которому установлен высокий уровень детальности журнала. Во время работы пользователь запускает программу, выбирая разные уровни доступа, и открывает документы из папок с разными метками конфиденциальности.

После завершения сеанса пользователя идентифицируется администратор и запускает программу AcProc.EXE. Администратора выбирает журнал предыдущего сеанса работы пользователя. После нажатия кнопки «Общий ресурс» открывается окно со списком процессов. Из этого списка следует выбрать тот процесс, работу которого нужно исследовать и нажать кнопку <Ок> (Рис.24.).

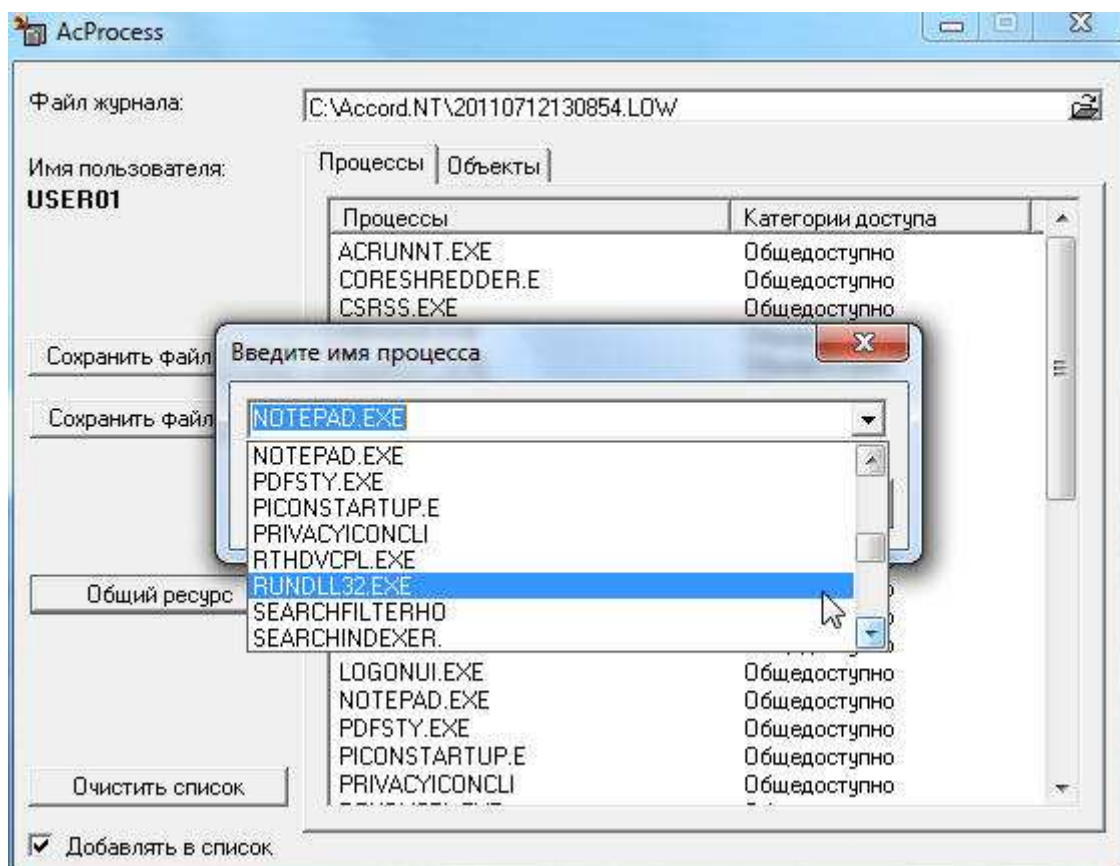


Рис. 24. Выбор процесса для исследования.

Программа выполняет анализ обращений выбранного процесса к ресурсам компьютера. Анализируются операции создания, удаления, переименования файлов и каталогов, открытие файлов на запись и на чтение/запись. Далее программа предлагает выбрать имя файла .PRD для сохранения списка объектов (Рис. 25.).

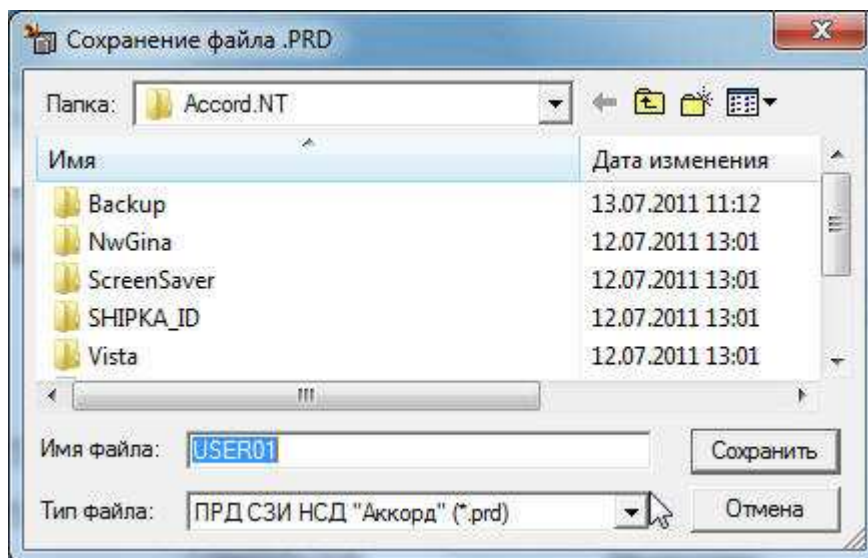


Рис. 25. Выбор имени файла для сохранения ПРД.

Данные из сохраненного файла можно импортировать в список меток мандатного доступа в программе ACED32.EXE. Для этого на панели в главном окне программы нужно нажать кнопку «Команды», далее выбрать пункт «Импорт мандатных меток». В папке Accord.NT выбрать файл <имя_пользователя>.prd с сохраненным списком объектов. В параметрах импорта будет включен только один пункт «Разграничение доступа» «Для объектов». После нажатия кнопки «Импорт» откроется дополнительное окно, в котором содержится список тех объектов, с которыми выбранный в программе AcProc.EXE процесс работал наиболее интенсивно (Рис.26.).

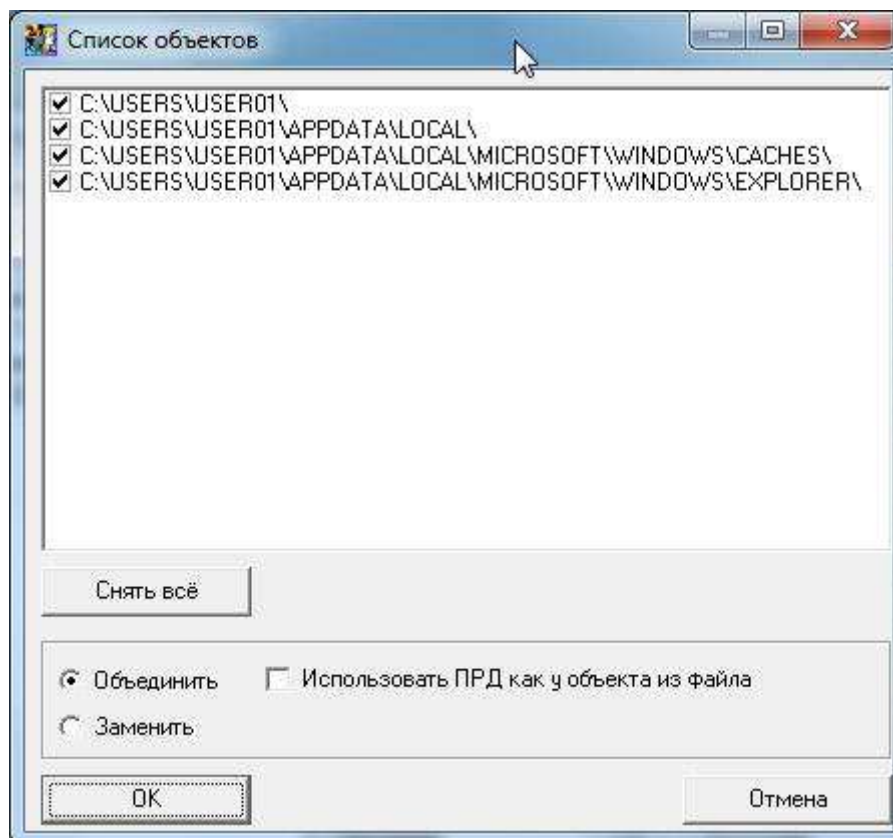


Рис. 26. Список объектов в процедуре импорта.

11443195.4012-036 99

Администратор по кнопке «ОК» может добавить в базу ПРД весь список, а может исключить некоторые объекты, сняв соответствующий флаг в левой колонке списка.

После выполнения процедуры импорта новые объекты появляются в списке мандатного доступа уже с меткой «ОБЩИЙ_РЕСУРС» (Рис. 27).

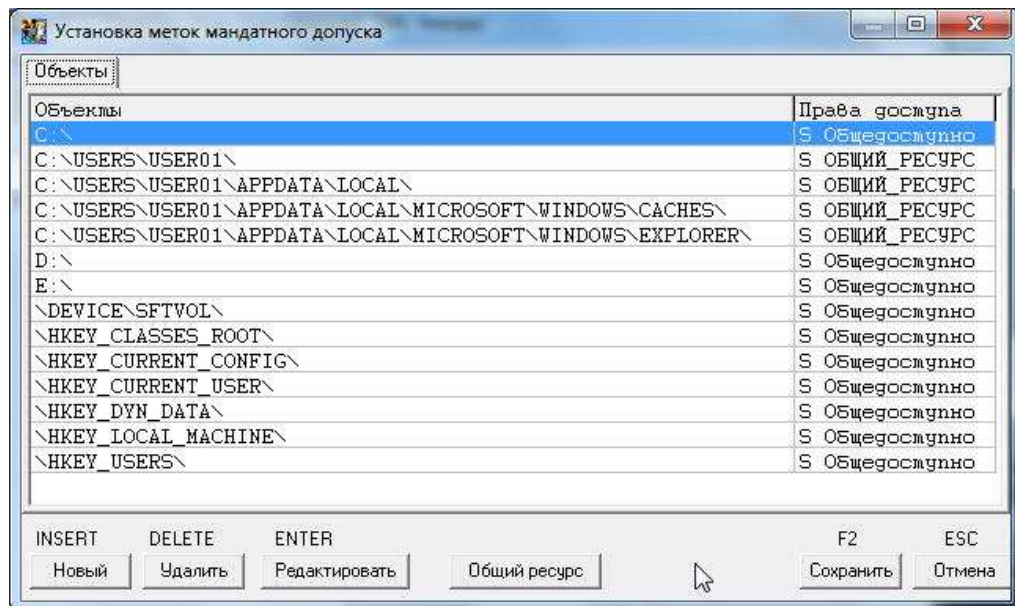


Рис. 27. Список объектов с метками мандатного доступа.

Администратору для эффективной работы необходимо понимать структуру файлов и каталогов ОС и прикладного ПО при установке такой специфической метки, как «ОБЩИЙ_РЕСУРС». В приведенном здесь примере достаточно было добавить в ПРД только первые два объекта, т.к. остальные два являются подкаталогами в папке \APPDATA\LOCAL.

4.3 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.28.

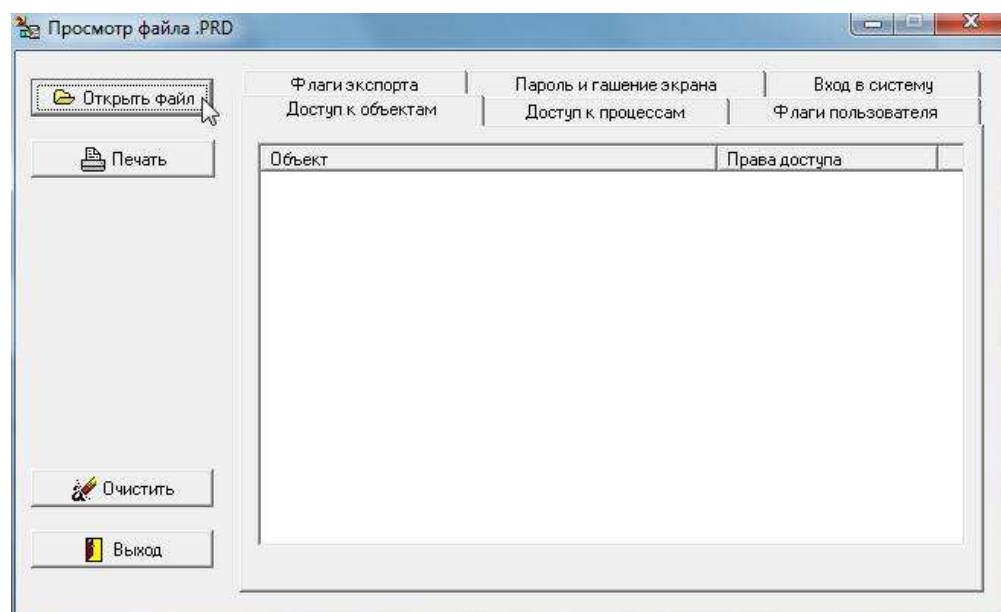


Рис. 28. Главное окно программы ReadPrd.

Описание параметров правил разграничения доступа приведены в документе «Установка правил разграничения доступа. Программа ACED32 (11443195.4012-036 97)»

Для выбора файла нажмите кнопку <Открыть файл> в левом верхнем углу основного окна. На экран выводится окно выбора файла .prd для просмотра. 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.29.).

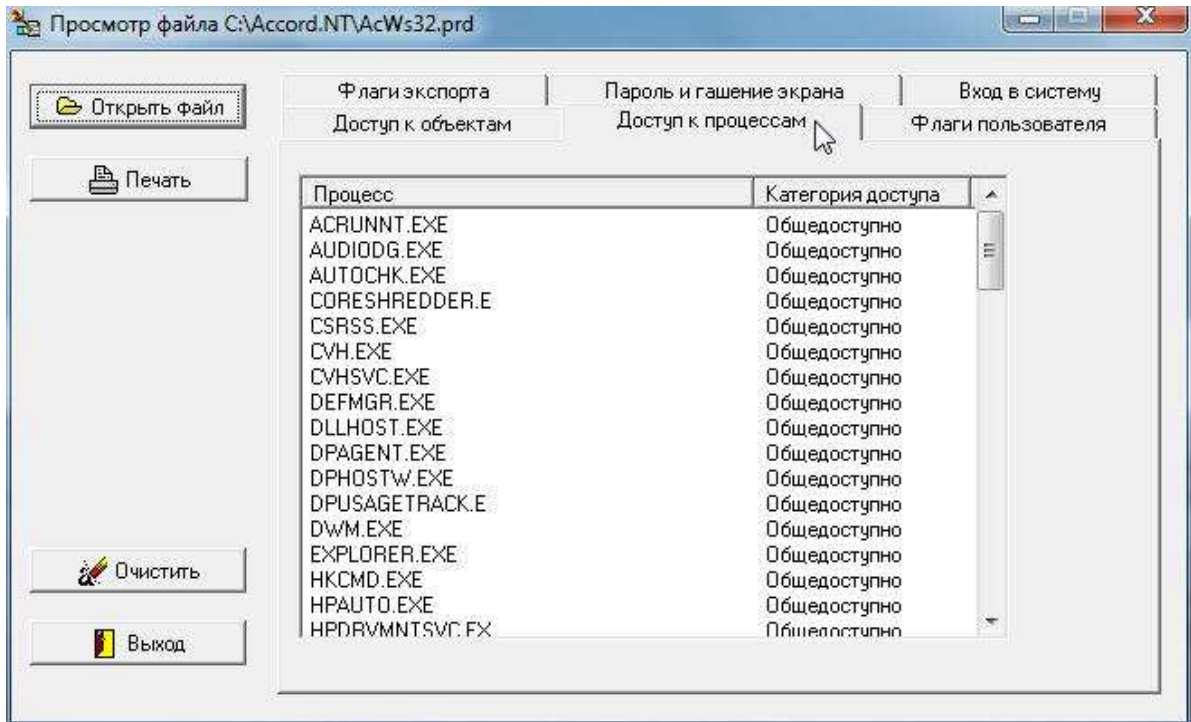


Рис. 29. Данные о правилах доступа и настройках пользователя.

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 пользователя, которые отмечались флагами в процедуре экспорта.