ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
37222406.26.20.40.140.091 99 -ЛУ

Специальное программное обеспечение средств защиты информации от несанкционированного доступа «АККОРД-Win64 К»

ПОДСИСТЕМА РЕГИСТРАЦИИ. ПРОГРАММЫ РАБОТЫ С ЖУРНАЛАМИ РЕГИСТРАЦИИ

37222406.26.20.40.140.091 99

АННОТАЦИЯ

Программа LOGVIEW.EXE предназначена для работы с журналами регистрации, которые создаются в процессе функционирования подсистемы разграничения доступа специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-Win64 K» (ТУ 26.20.40.140-091-37222406-2020) (далее по тексту – СПО «Аккорд-Win64 K», «Аккорд-Win64 K», СПО «Аккорд», «Аккорд»).

Программа используется администратором безопасности информации и входит в состав специального программного обеспечения «Аккорд».

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

Перед эксплуатацией специального программного обеспечения «Аккорд» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые организационные меры защиты, рекомендуемые в документации.

Применение защитных механизмов специального программного обеспечения «Аккорд» должно дополняться общими мерами технической безопасности, а также физической охраной СВТ.

СОДЕРЖАНИЕ

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). Предназначен для временной блокировки экрана СВТ
СПО	специальное программное обеспечение
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 специального программного обеспечения (СПО) «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 СПО «Аккорд» события регистрируются в файлах журнала в упакованном формате (для экономии дискового пространства). Если СПО «Аккорд» используется в сетевой версии, то в журнале фиксируется имя станции.

2.1. Запуск программы LOGVIEW

2.1.1. Общие сведения

Запустите программу LOGVIEW.EXE из каталога C:/ACCORD.X64 (C:/ACCORD.NT – для 32-битных ОС), или Пуск> Программы> Аккорд-Win64 K> Просмотр журнала событий (Пуск> Программы> Аккорд-Win32 K> Просмотр журнала событий – для 32-битных ОС).

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

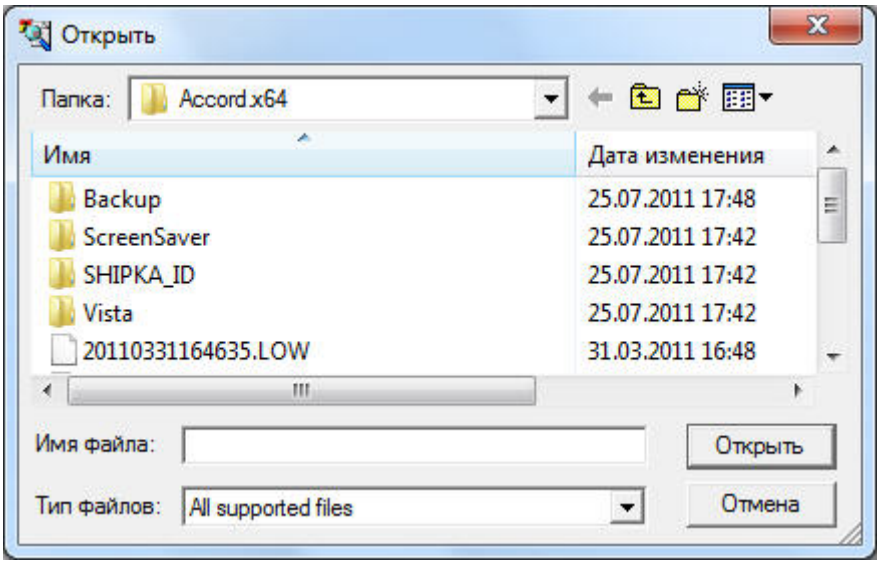

Рисунок 1 - Окно выбора файла журнала

Выбрав левой кнопкой мыши нужный файл, нажмите кнопку <Открыть>. На экран выводится окно просмотра журнала, показанное на рисунке 2.

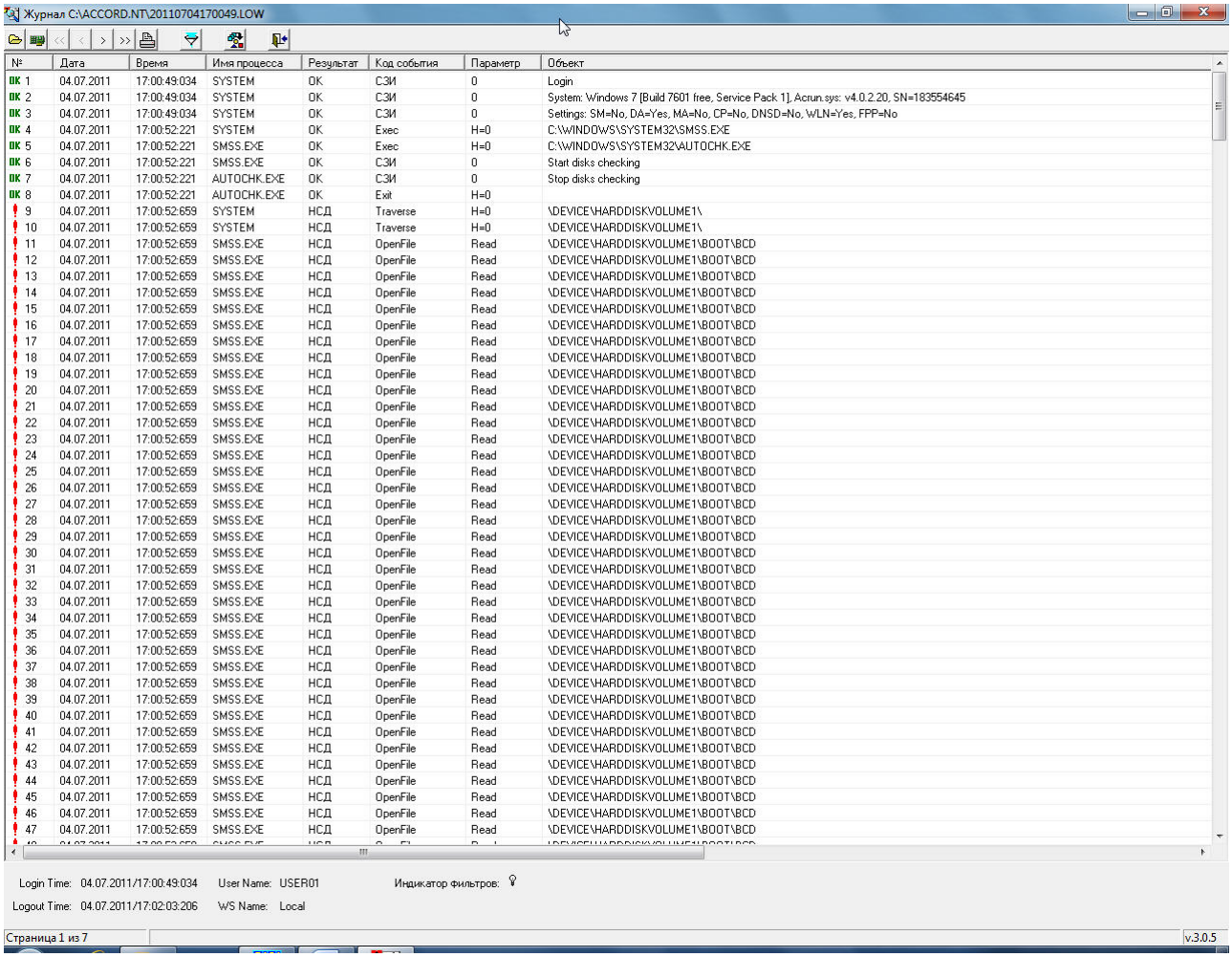

Рисунок 2 - Главное окно программы LOGVIEW

Протоколирование сообщений в журнале событий организовано следующим образом: если длина имени объекта превышает 251 символ, то имя объекта обрезается.

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 (МНД-мандатный[1], ПРЦ-процессы) – 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

[1] В рамках настоящего документа под мандатным принципом контроля доступа понимается принцип контроля доступа на основе иерархических меток

Приложении 2 документа «Руководство администратора» (11443195.509000.056 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 завершен 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;
- 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.

2.1.2. Удаленный запуск программы LOGVIEW

Начиная с версии 5.0.10.51 ПО «Аккорд» имеется возможность запуска программы LOGVIEW с сетевого ресурса или из любого каталога, который имеет доступ на чтение. Для корректной работы программы LOGVIEW в этом случае необходимо наличие в каталоге с программой LogView.exe следующих библиотек:

- TMAttach.dll;
- VCTmDrv.dll (для запуска TmAttach.dll);
- tmdrv32.dll (если на компьютере активирован ПАК «Аккорд», данная библиотека уже содержится в каталоге system32);
- azlog.dll (требуется в случае необходимости чтения журналов контроллеров с расширением azl).

При наличии всех требуемых библиотек может быть осуществлен удаленный запуск программы LogView.

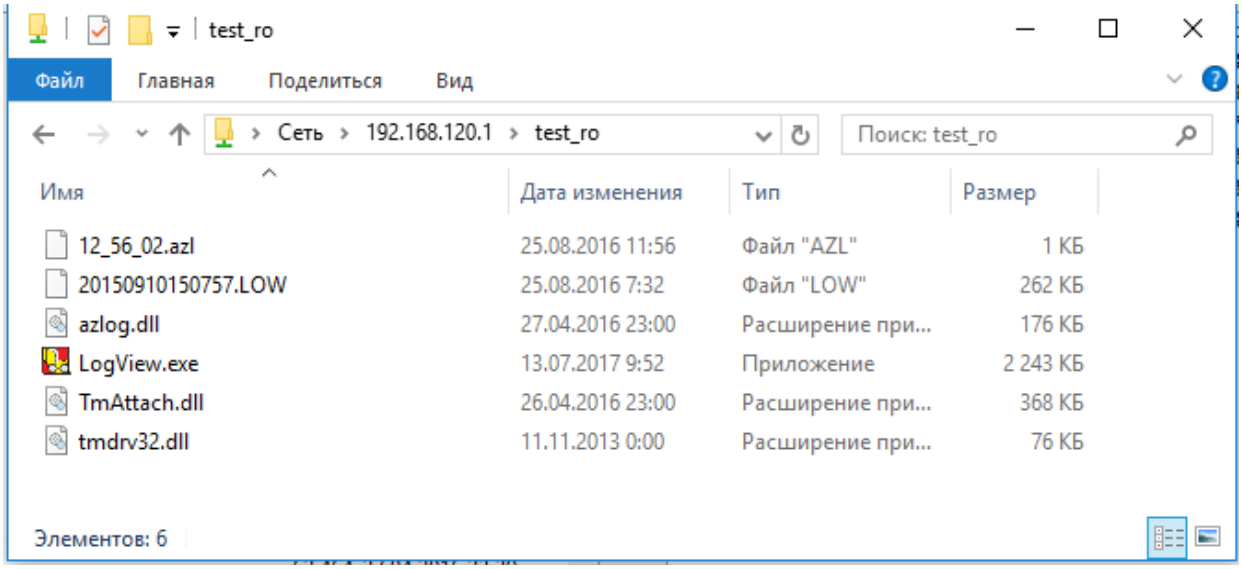

Рисунок 3 - Удаленный запуск программы LogView

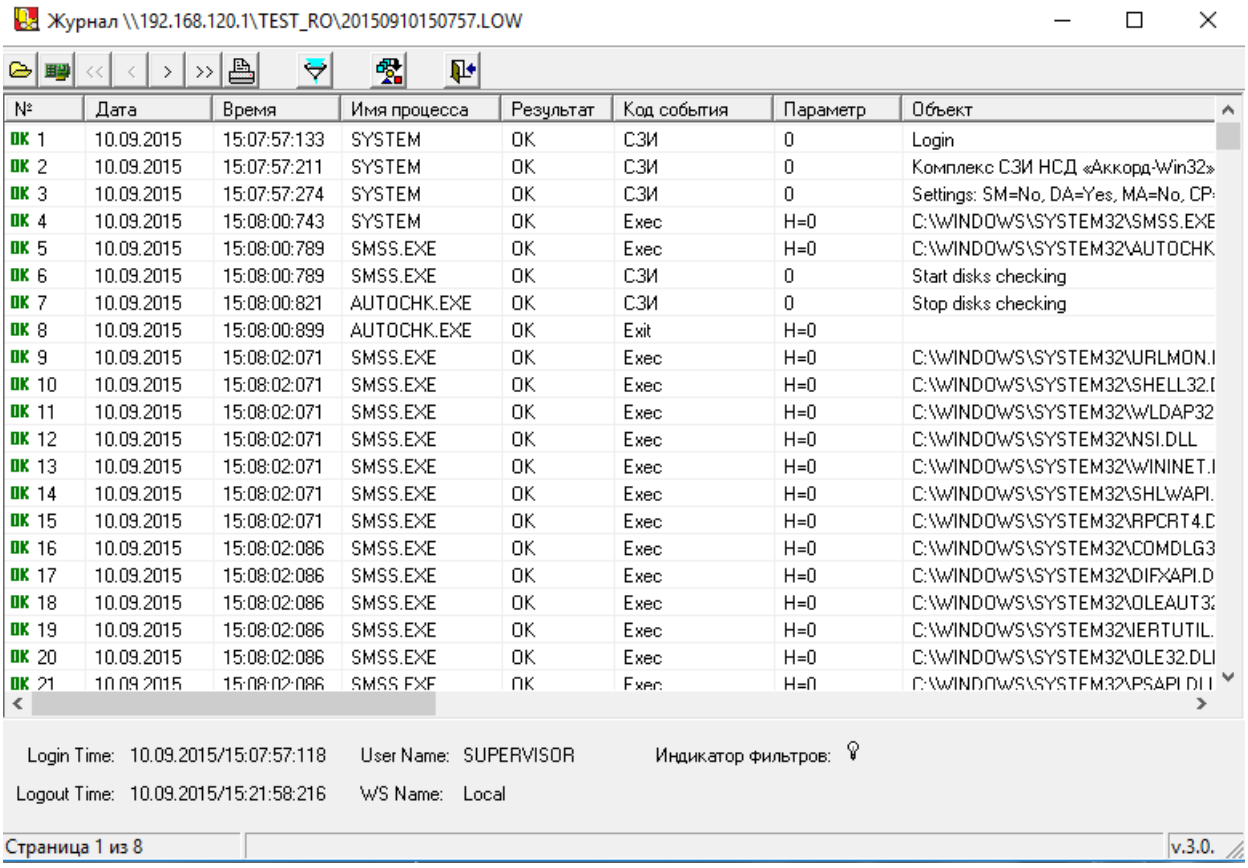

Рисунок 4 - Программа LogView запущена удаленно

При запуске данная утилита создает файл с расширением .idx во временной папке пользователя %userprofile%\appdata\local\temp.

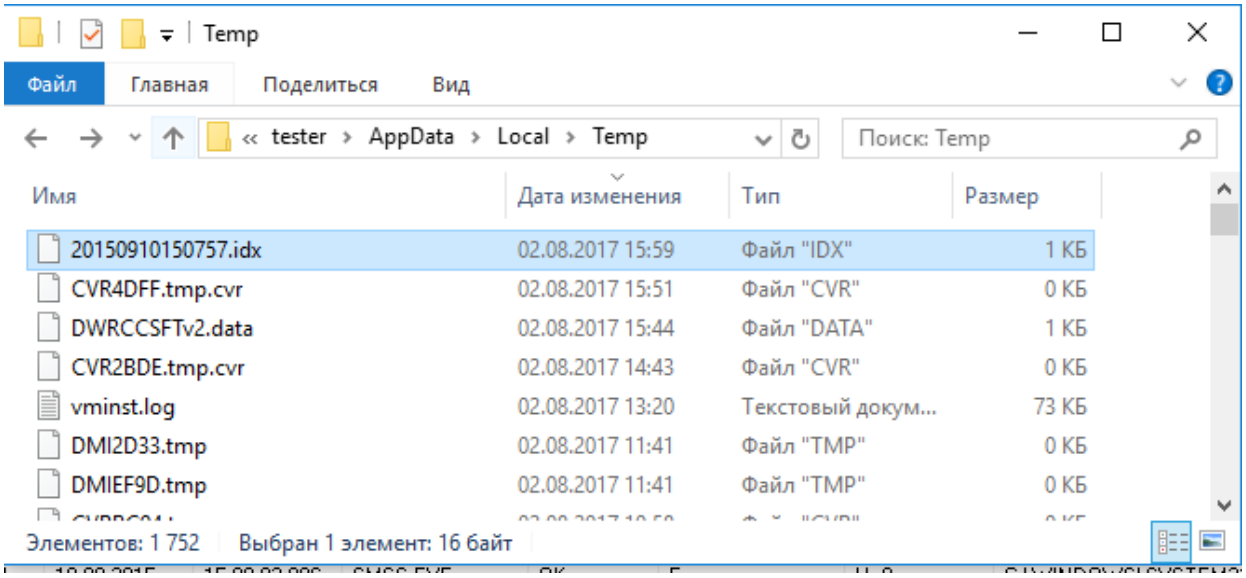

Рисунок 5 - Файл с расширением .idx, созданный во временной папке пользователя

По завершении работы с журналом данный файл будет удален.

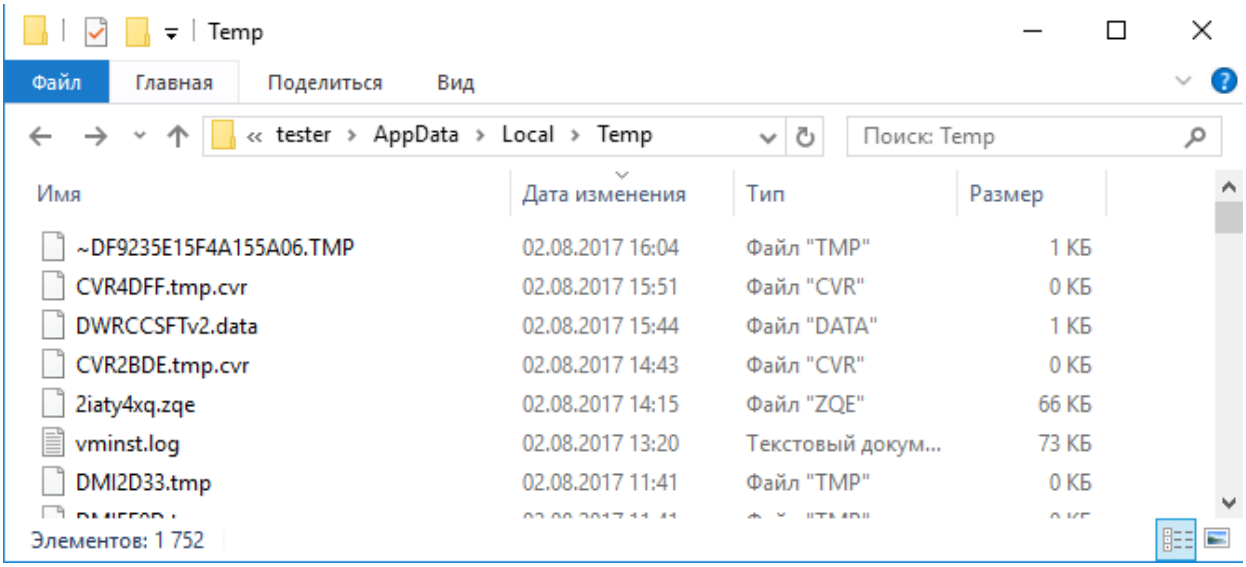

Рисунок 6 - Файл с расширением .idx удален из временной папки пользователя

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 (рисунок 7).

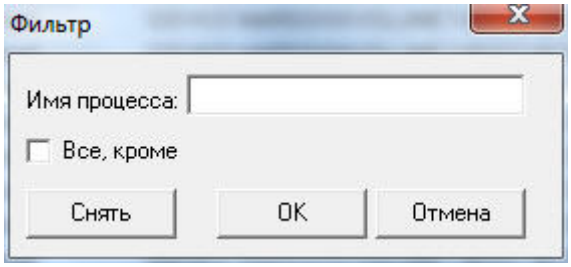

Рисунок 7 - Установка фильтра по имени процесса

Можно ввести как полное имя процесса, так и часть имени. После нажатия на кнопку <OK> 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 рисунке 8.

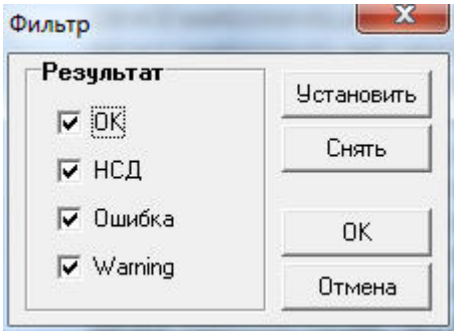

Рисунок 8 - Установка фильтра по результату операции

Нажатием на левую клавишу мыши можно установить/сбросить отметку возле каждой операции. После нажатия кнопки <OK> 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 рисунке 9.

Все события, регистрируемые подсистемой регистрации СПО «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.

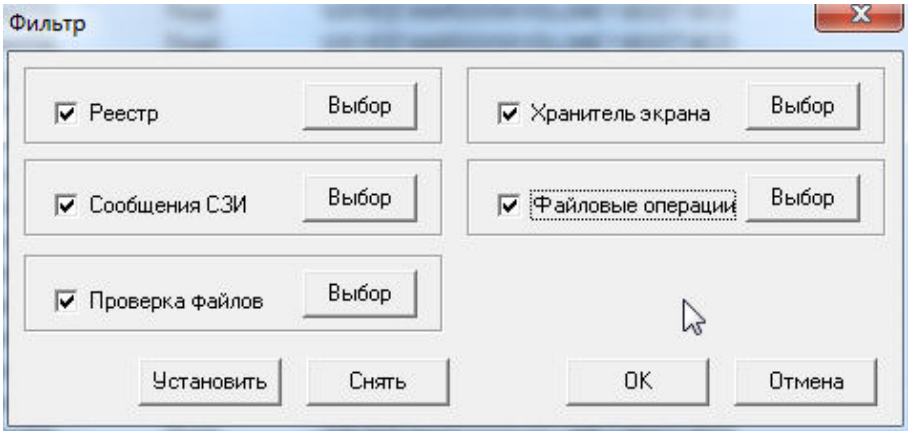

Рисунок 9 - Установка фильтров кодов событий

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 рисунке 10.

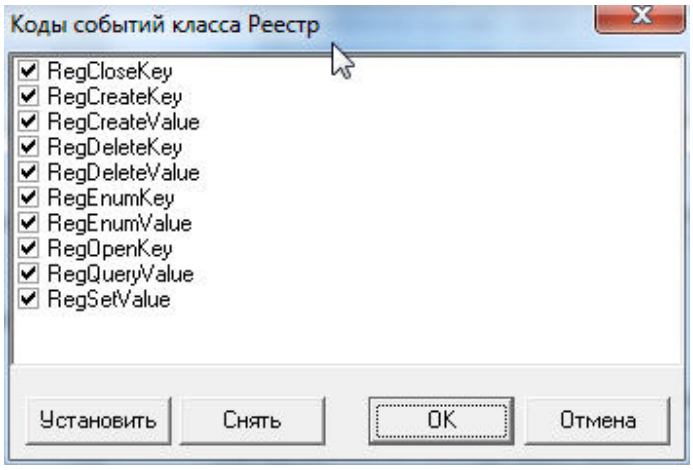

Рисунок 10 - Установка фильтра для событий класса «Реестр»

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» (рисунок 11).

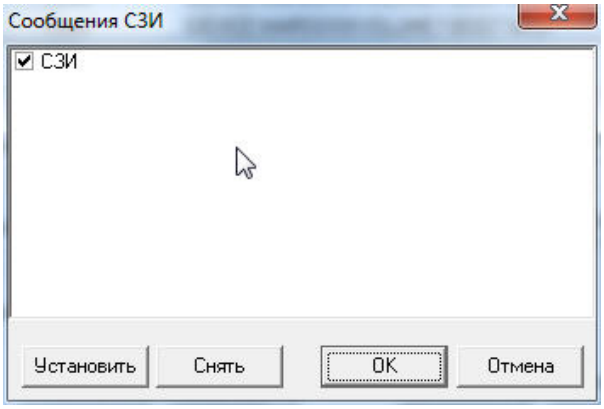

Рисунок 11 - Установка фильтра для событий класса «Сообщения СЗИ»

Хранитель экрана

В этой группе собраны события, которые относятся к обработке операций блокировки и разблокировки экрана и клавиатуры (рисунок 12).

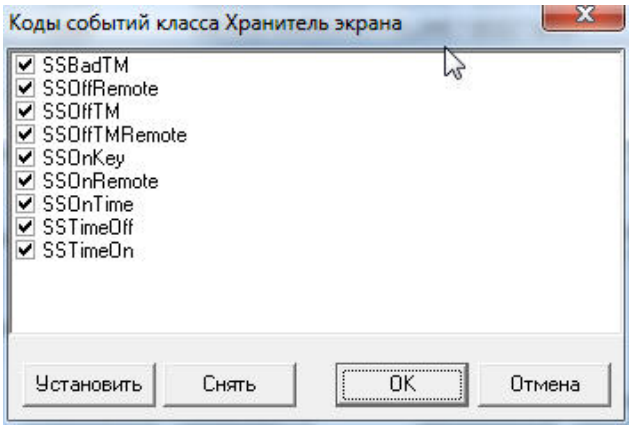

Рисунок 12 - Установка фильтра для событий класса «Хранитель экрана»

Файловые операции*

Это группа событий, которые относятся к контролю файловых операций (рисунок 13).

* 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

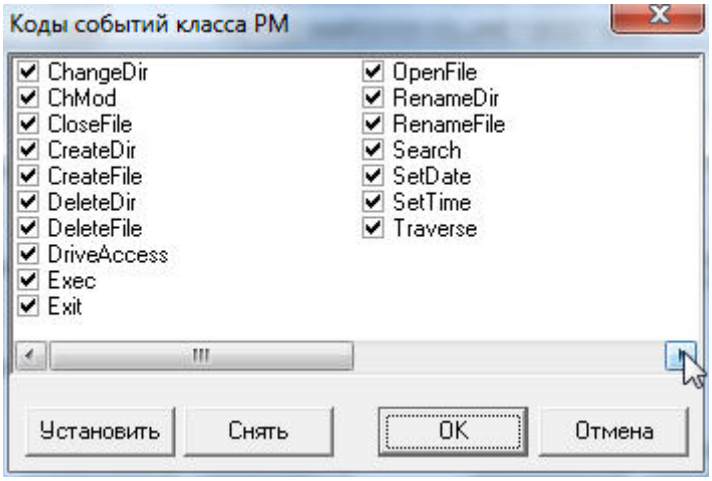

Рисунок 13 - Установка фильтра для событий класса «PM»

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 (рисунок 14).

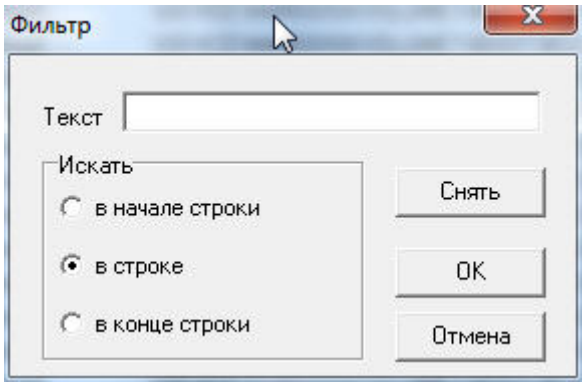

Рисунок 14 - Установка фильтра по наименованию объекта

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 рисунке 2, и нажать правую кнопку в верхней панели окна. Также можно завершить работу программы с использованием стандартной комбинации клавиш <Alt>-<F4>.

3. Предварительная сортировка журналов

Для более эффективной организации работы с журналами регистрации событий следует воспользоваться программой LOGBASE.EXE из каталога C:\ACCORD.X64 (C:\ACCORD.NT – для 32-битных ОС).

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 рисунке 15.

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

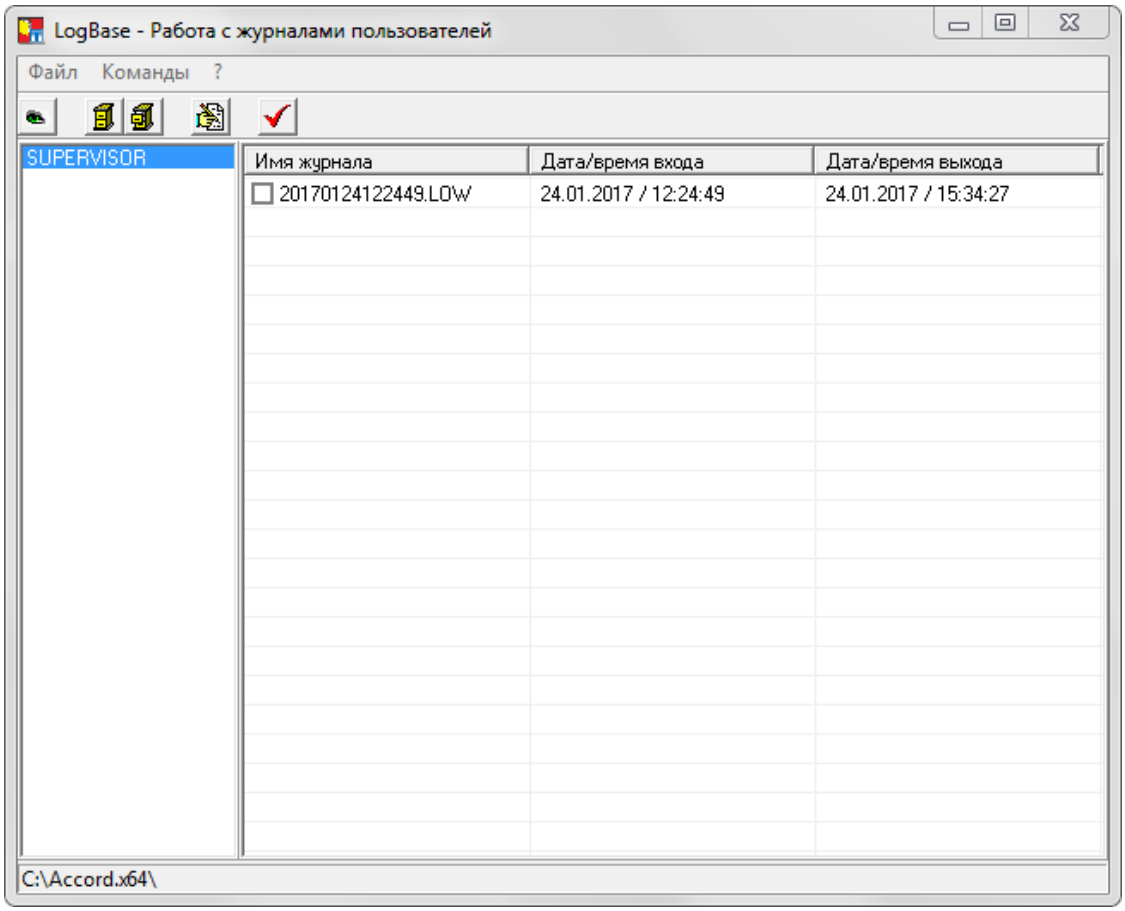

Рисунок 15 - Предварительная сортировка журналов регистрации

3.1. Архивация/Разархивация журналов

С помощью программы LOGBASE.EXE администратором БИ может осуществляться архивация/разархивация журналов. В архив помещаются файлы журнала без полного пути.

Чтобы поместить файлы журнала в архив, следует отметить соответствующие файлы журнала в главном окне программы LOGBASE.EXE и

нажать кнопку <Поместить в архив>(рисунок 15). В появившемся окне следует задать имя архива (рисунок 16).

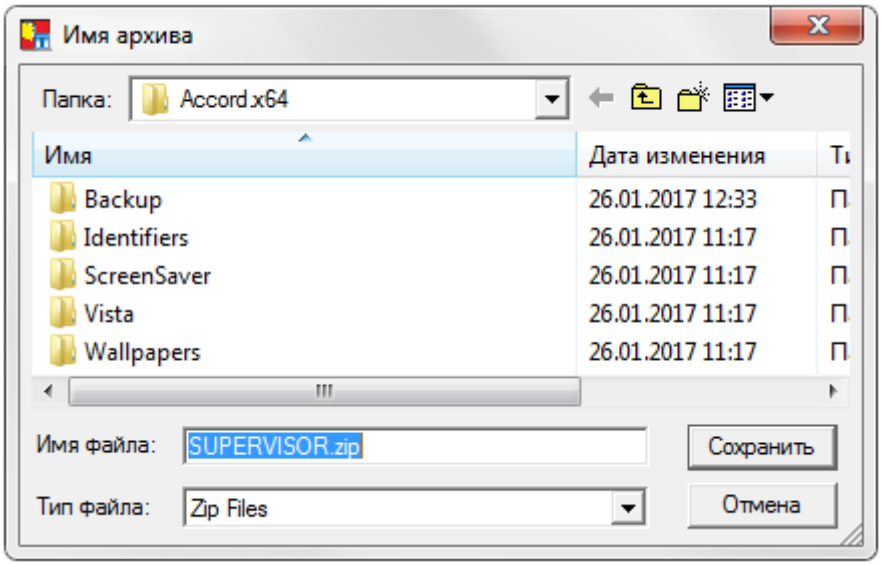

Рисунок 16 - Окно выбора файла для архивации

При нажатии кнопки <OK> (рисунок 16) выполняется проверка имени архива. Если архив с таким именем уже существует, то выдается запрос на его перезапись:

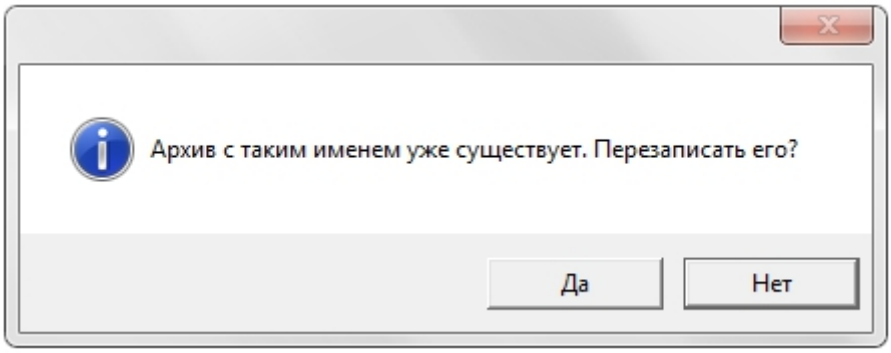

Рисунок 17 – Запрос на перезапись архива

При нажатии кнопки <Извлечь из архива> главного меню программы (рисунок 15) выводится окно выбора архива, показанное на рисунке 18. Файл архива можно выбрать мышью, или в строке «Имя файла» ввести имя архива.

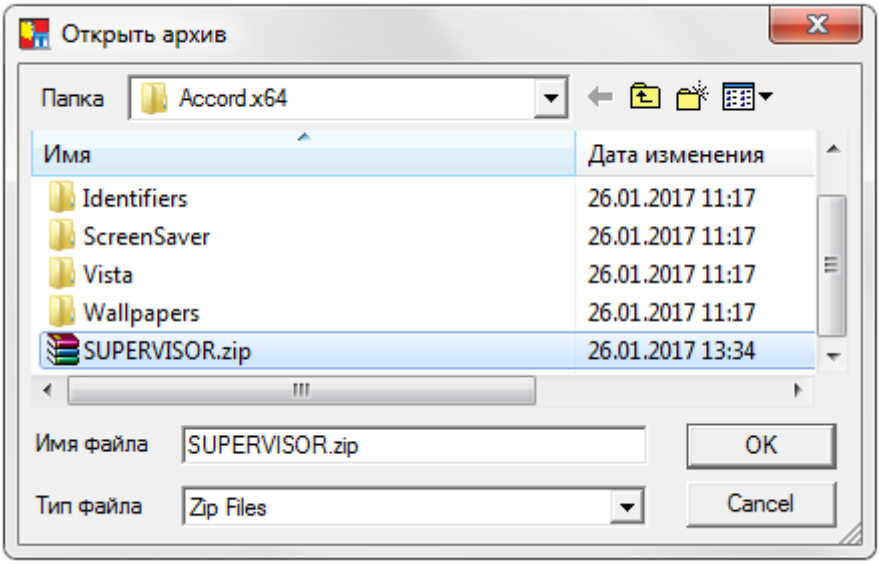

Рисунок 18 - Окно выбора файла архива для извлечения журнала (разархивации)

При нажатии кнопки <OK> (рисунок 18) на экране появляется окно выбора каталога, в который будут помещены разархивированные файлы журнала.

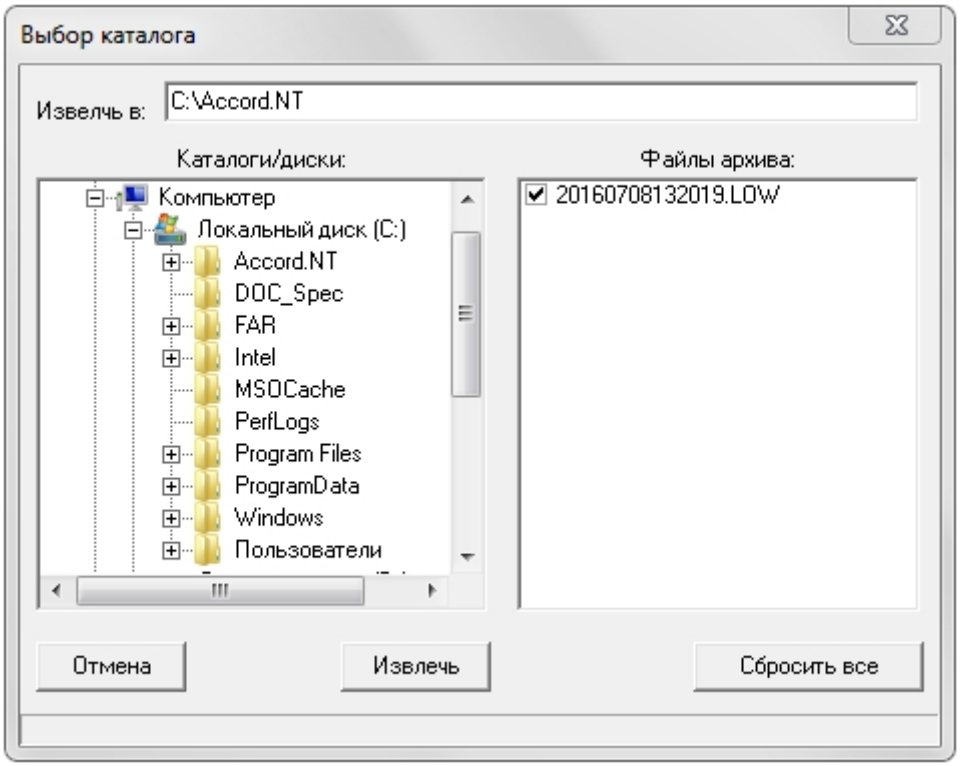

Рисунок 19 – Выбор каталога для извлечение файлов из выбранного архива

При выполнении операции разархивирования происходит извлечение всех файлов из выбранного архива в указанный каталог.

4. Формирование правил разграничения доступа на основе информации в журнале регистрации событий

В состав СПО «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 (подробнее см. документ «Установка правил разграничения доступа. Программа ACED32» п.6.10). 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 (рисунок 20). Левое поле предназначено для списка объектов, сформированного на основе анализа журнала. Правое поле – это предназначенный для сохранения список выбранных объектов с установленными атрибутами доступа.

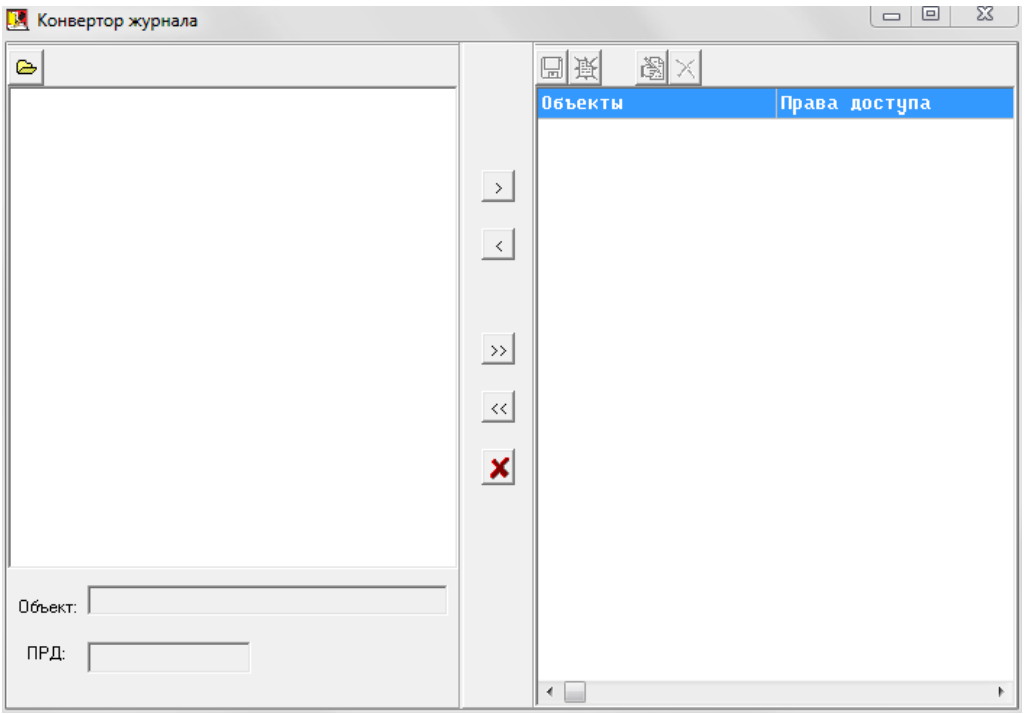

Рисунок 20 - Главное окно программы

Для выбора анализируемого журнала нажмите кнопку с изображением папки в левом верхнем углу. Открывается окно выбора файла журнала (рисунок 21).

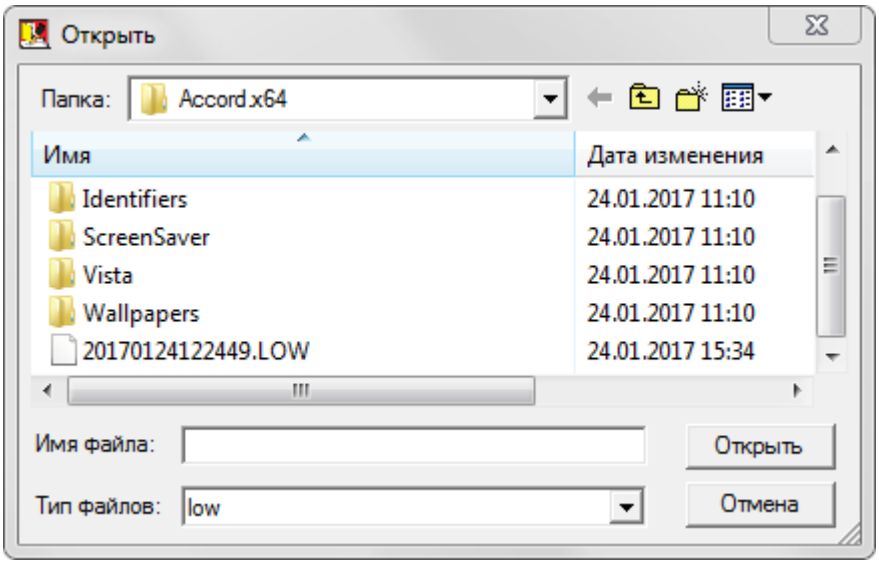

Рисунок 21 - Выбор журнала для анализа

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 (рисунок 22).

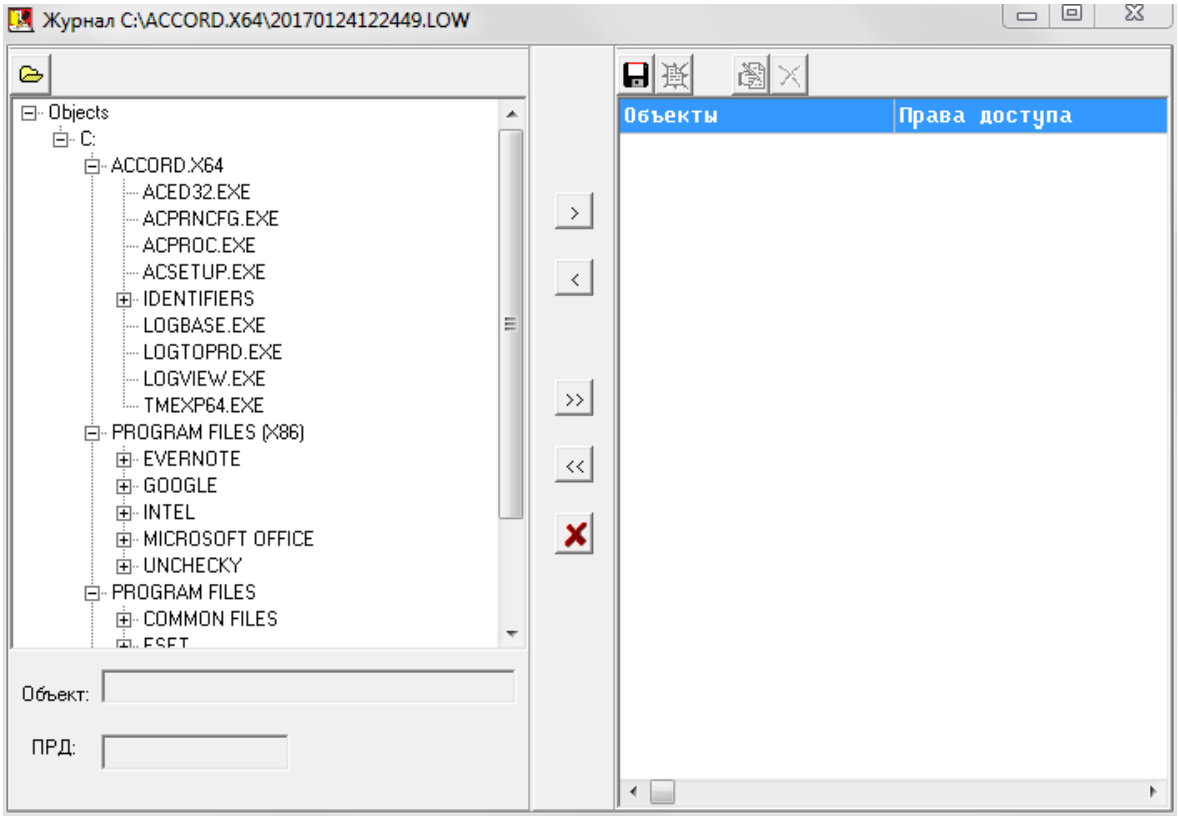

Рисунок 22 - Список объектов, полученный на основе анализа журнала

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> (рисунок 23).

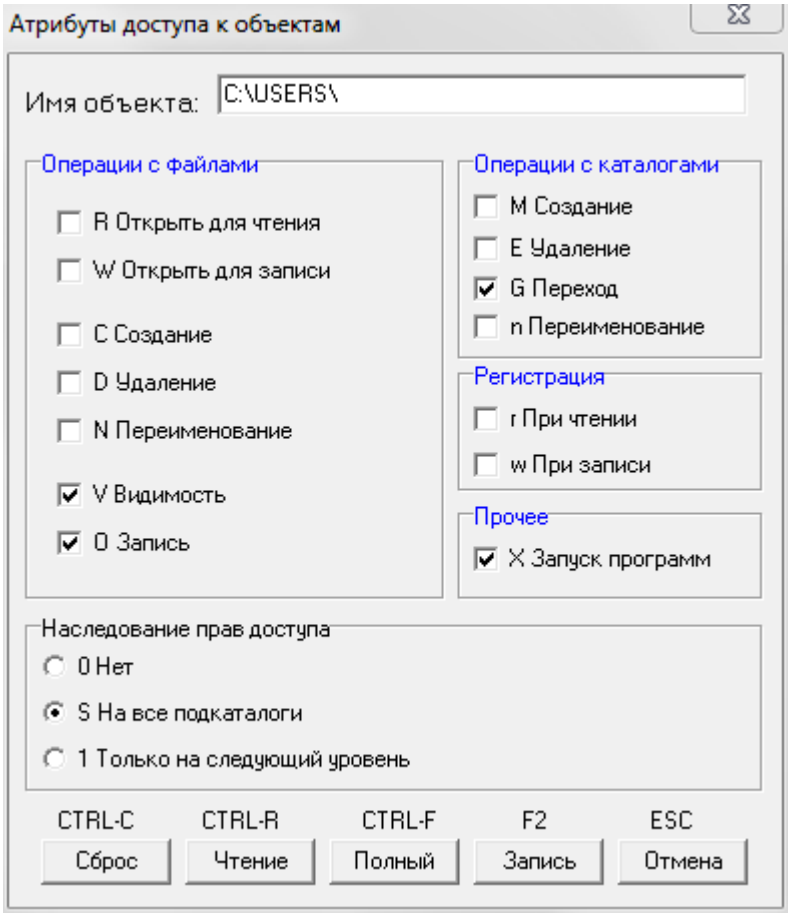

Рисунок 23 - Окно установки атрибутов доступа

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 (рисунок 24).

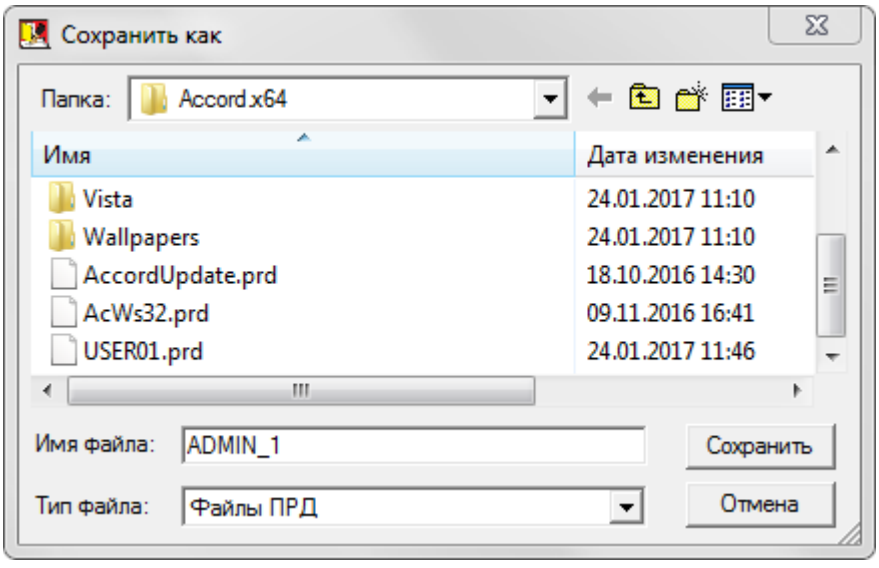

Рисунок 24 - Выбор файла для сохранения ПРД

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 рисунке 25.

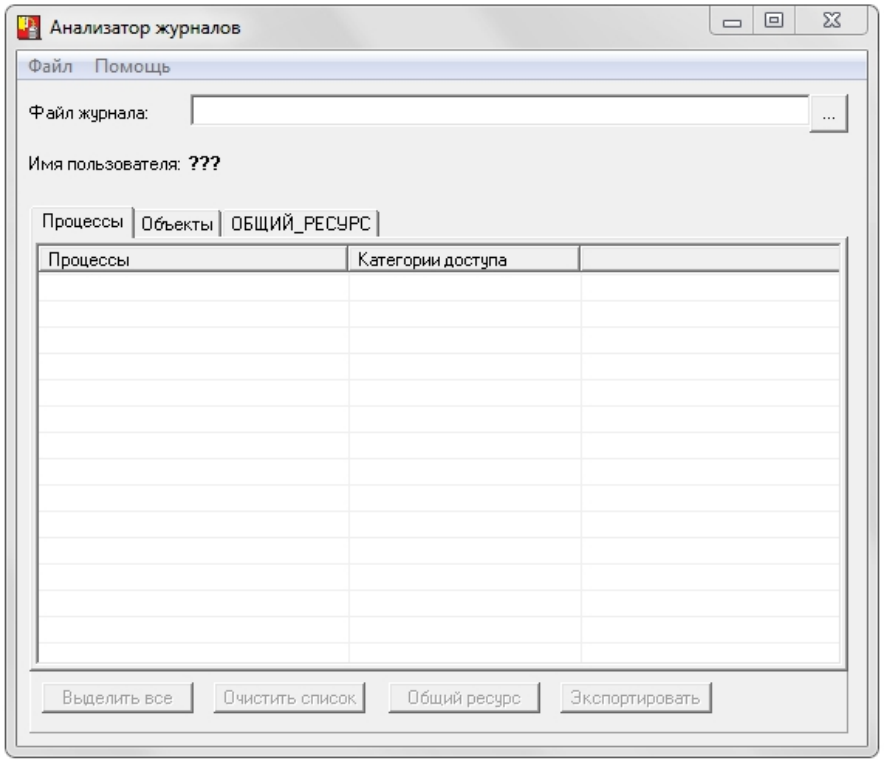

Рисунок 25 - Главное окно программы AcProc.EXE

Поле «Файл журнала» предназначено для выбора анализируемого журнала регистрации. Необходимо нажать на раскрывающийся список в правой части поля. Открывается окно выбора журнала (рисунок 21). Выбрав нужный файл (или несколько файлов), нажмите кнопку <Открыть>. Программа сканирует журнал и выводит в окне список процессов с указанием уровня доступа (рисунок 26).

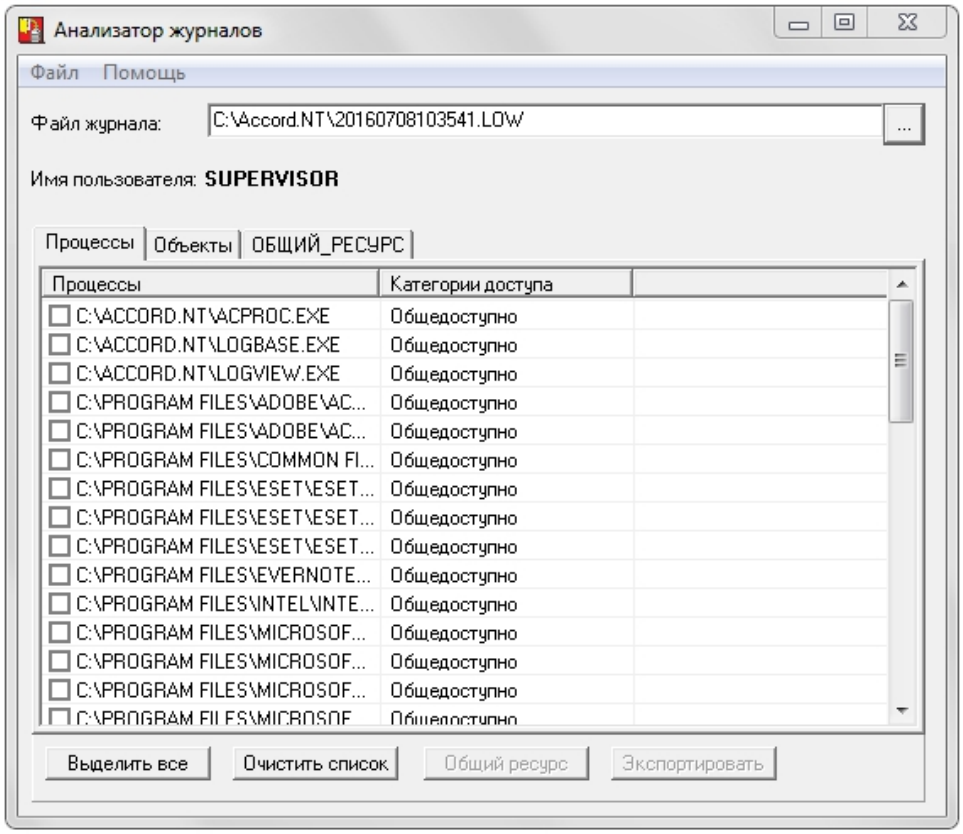

Рисунок 26 - Сформированный список процессов

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 (рисунок 27).

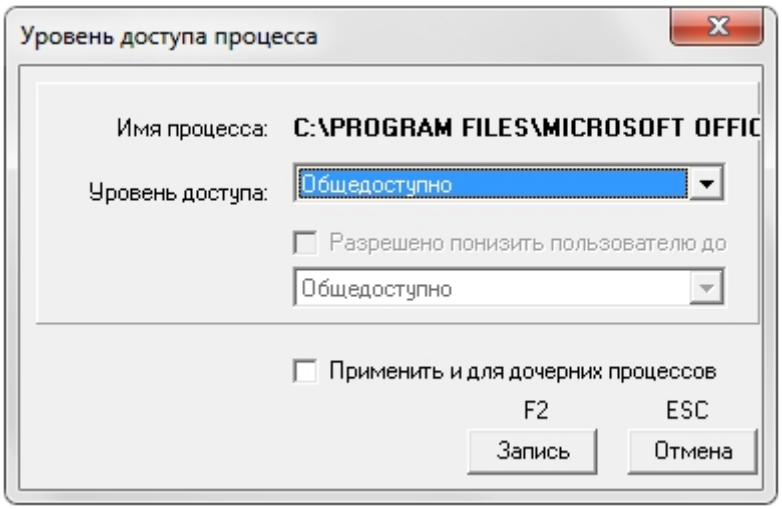

Рисунок 27 - Установка нового уровня доступа

Нажатие кнопки со стрелкой в поле «Уровень доступа» выводит список установленных в СЗИ уровней доступа, которые можно присвоить данному процессу.

После того как список процессов полностью скорректирован, необходимо выполнить сохранение настроек в файле правил доступа. Нажмите кнопку <Экспортировать> (рисунок 26).

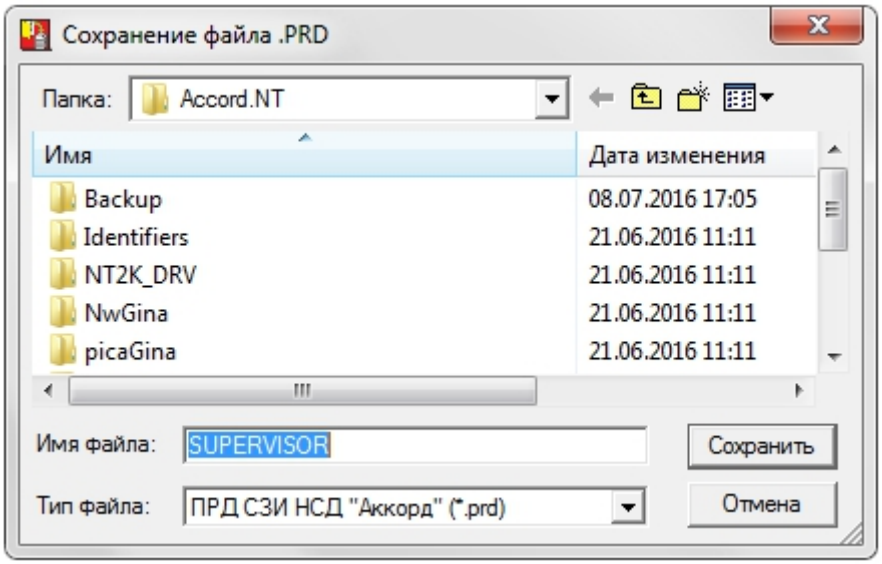

Рисунок 28 – Сохранение списка процессов

В окне сохранения (рисунок 28) введите имя файла и нажмите кнопку <Сохранить>. Данные из сохраненного файла можно импортировать пользователю или группе пользователей в программе ACED32.EXE.

Список исполняемых файлов (рисунок 29) 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.

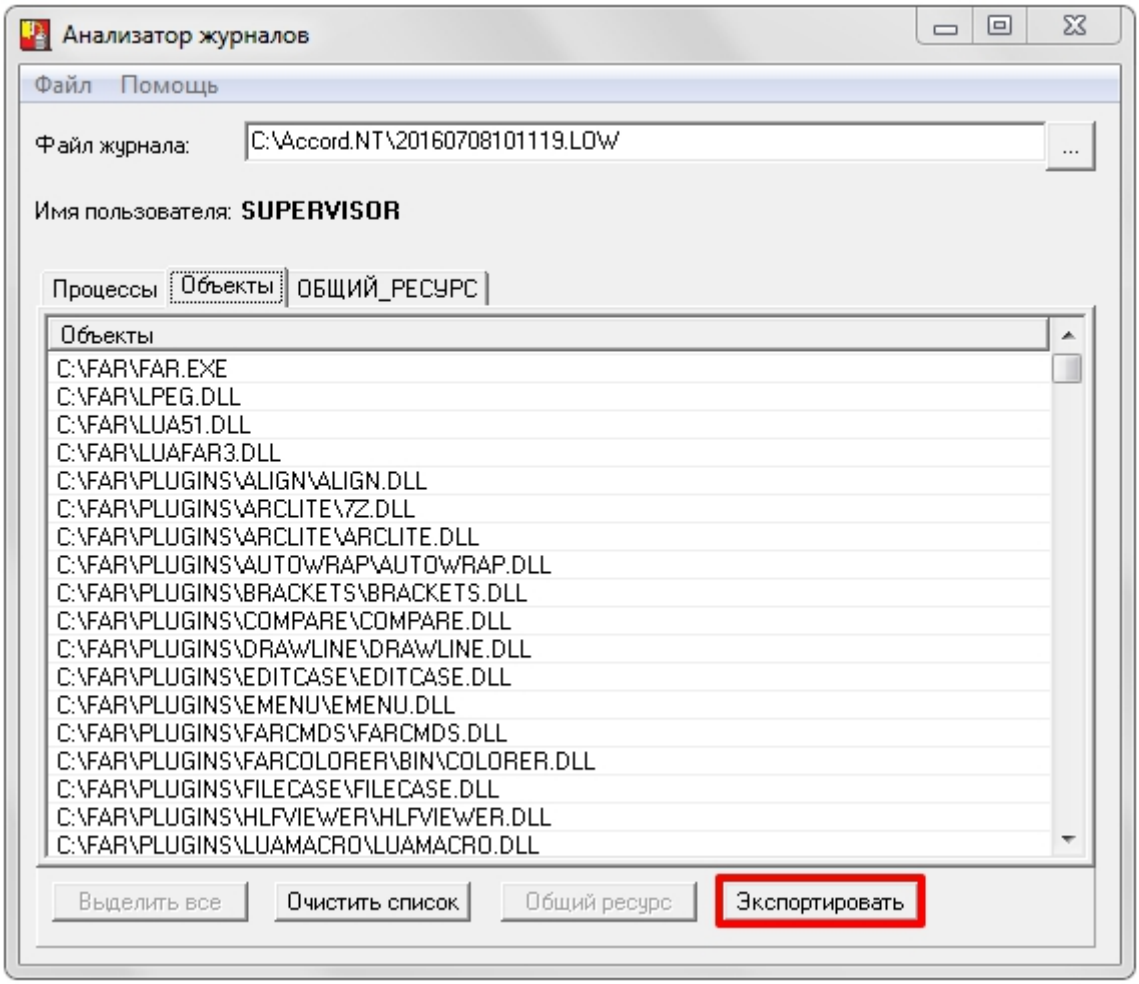

Рисунок 29 – Список исполняемых файлов

Для сохранения списка нажмите кнопку <Экспортировать> (рисунок 29). В окне сохранения (рисунок 30) введите имя файла и нажмите кнопку <Сохранить>. Данные из сохраненного файла можно импортировать пользователю в программе ACED32.EXE.

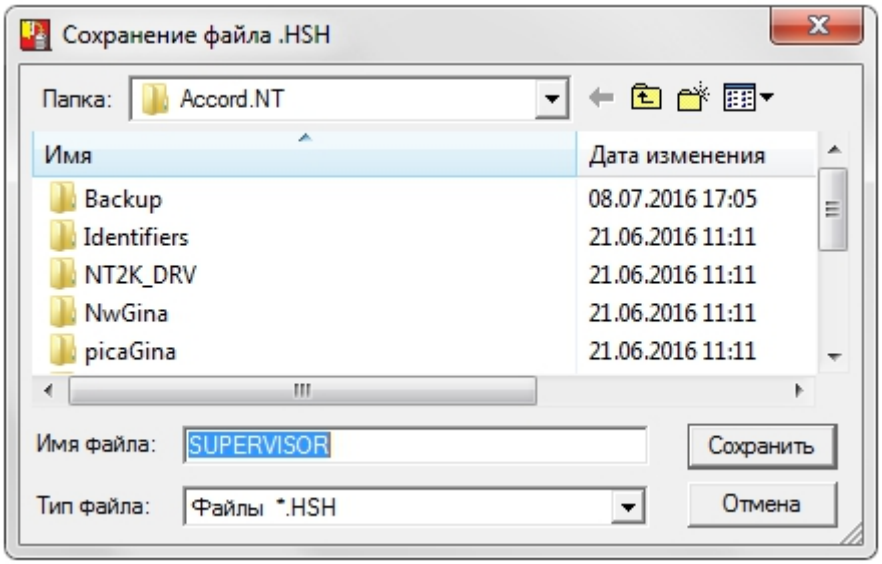

Рисунок 30 - Сохранение списка файлов для процедуры контроля целостности

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 (рисунок 26).

Для полноценного анализа событий детальность журнала исследуемого пользователя должна быть высокой, а режим работы монитора безопасности «мягкий». Контроль доступа включается дискреционный + мандатный + процессы. Процессу, 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. Администратор выбирает файл журнала (или несколько файлов) предыдущего сеанса работы пользователя. В появившемся на экране окне отметить необходимый процесс и нажать кнопку <Общий ресурс>. Далее по выбранным файлам журнала происходит поиск объектов, к которым выбранный процесс обращался с запросом на создание, удаление, переименование файлов и каталогов, открытие файлов на запись и на чтение/запись. Если поиск завершается успешно, то во вкладке «Общий ресурс» появляются соответствующие объекты (рисунок 31).

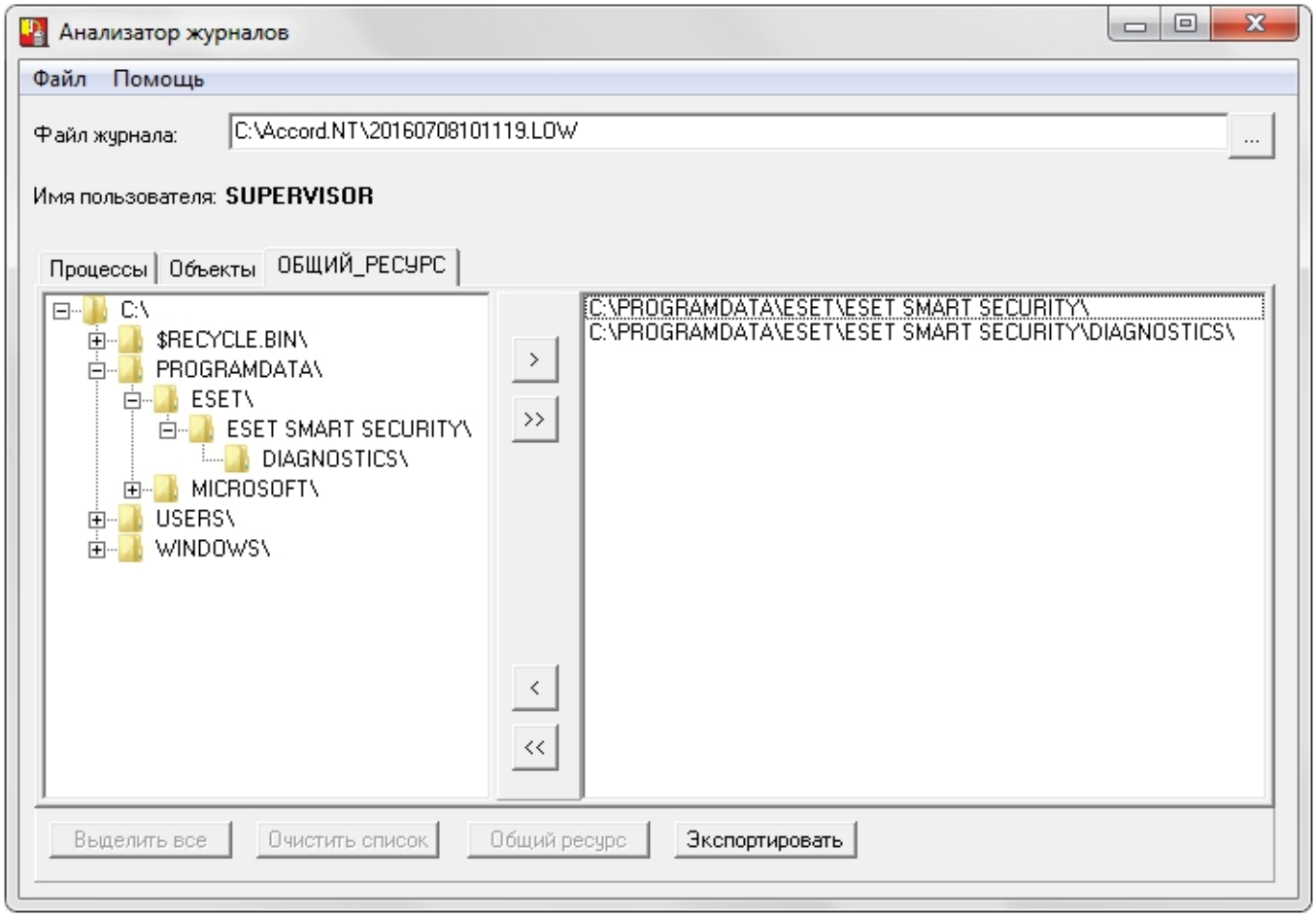

Рисунок 31 - Выбор процесса для исследования

Необходимо сохранить объекты, к которым обращался выбранный процесс. Для этого нужно нажать кнопку <Экспортировать> (рисунок 29). При нажатии кнопки на экране появляется окно, в котором нужно указать путь, имя файла (например, «TEST_USER.PRD») и нажать кнопку <Сохранить> (рисунок 32).

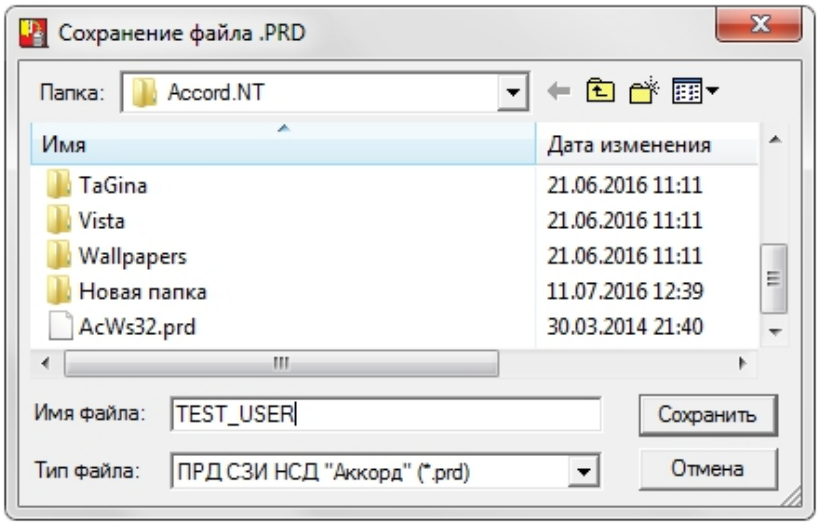

Рисунок 32 - Выбор имени файла для сохранения ПРД

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 «Импортировать мандатные метки». В появившемся на экране окне 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 (рисунок 33).

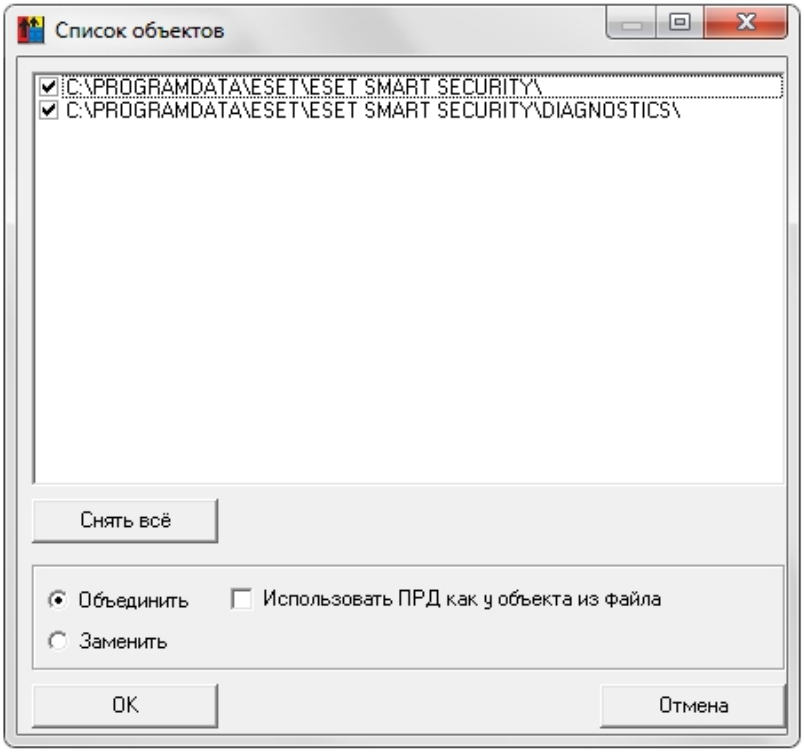

Рисунок 33 - Список объектов в процедуре импорта

Администратор по кнопке <OK> 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» (рисунок 34).

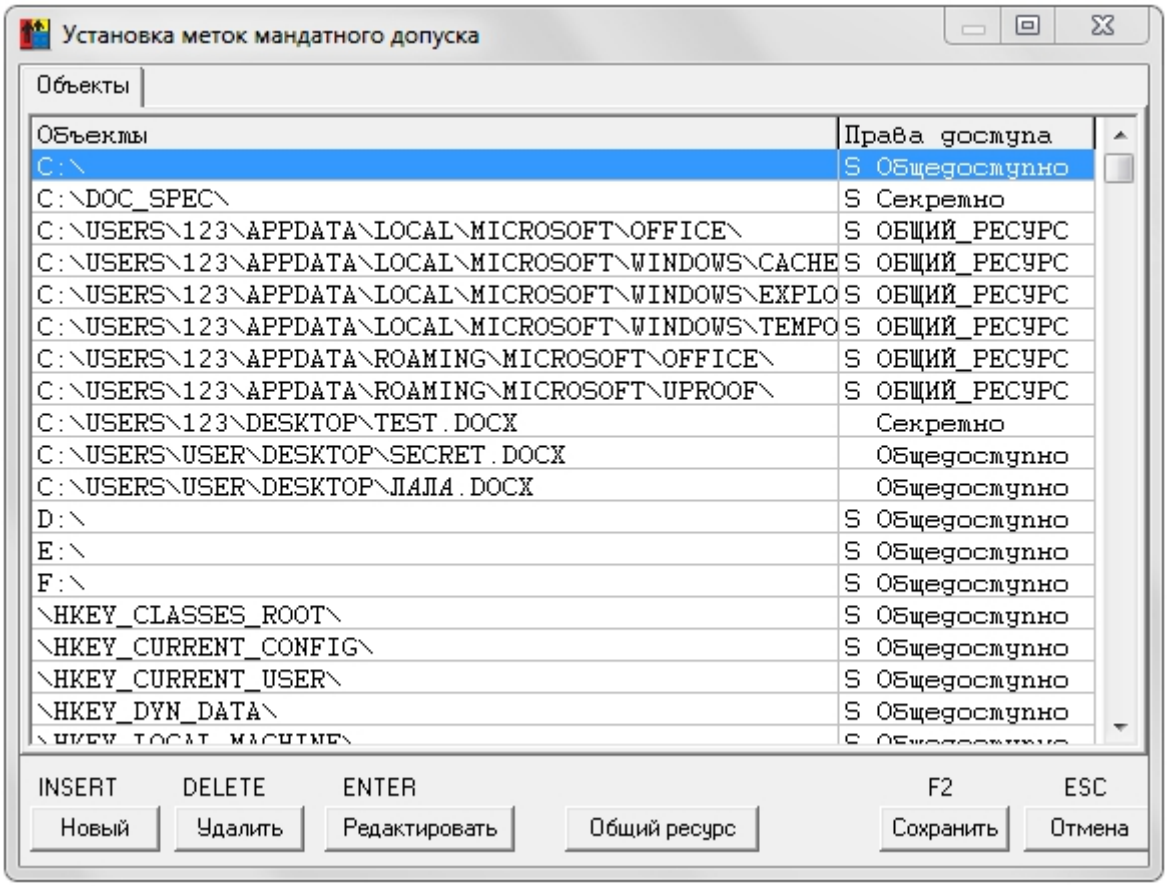

Рисунок 34 - Список объектов с метками мандатного доступа

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 рисунке 35.

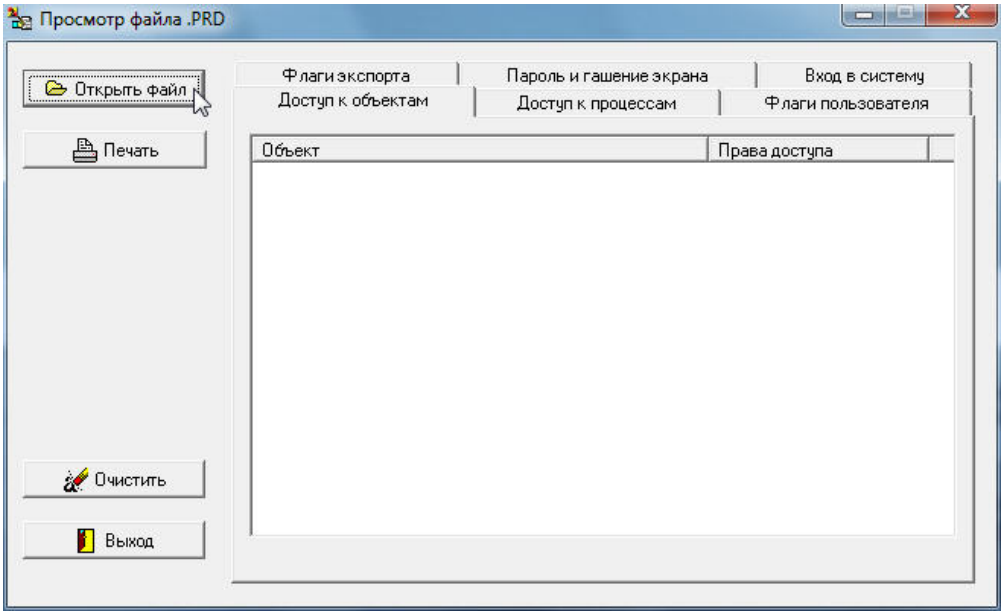

Рисунок 35 - Главное окно программы ReadPrd

Описание параметров правил разграничения доступа приведены в документе «Установка правил разграничения доступа. Программа ACED32 (37222406.26.20.40.140.091 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 (рисунок 36).

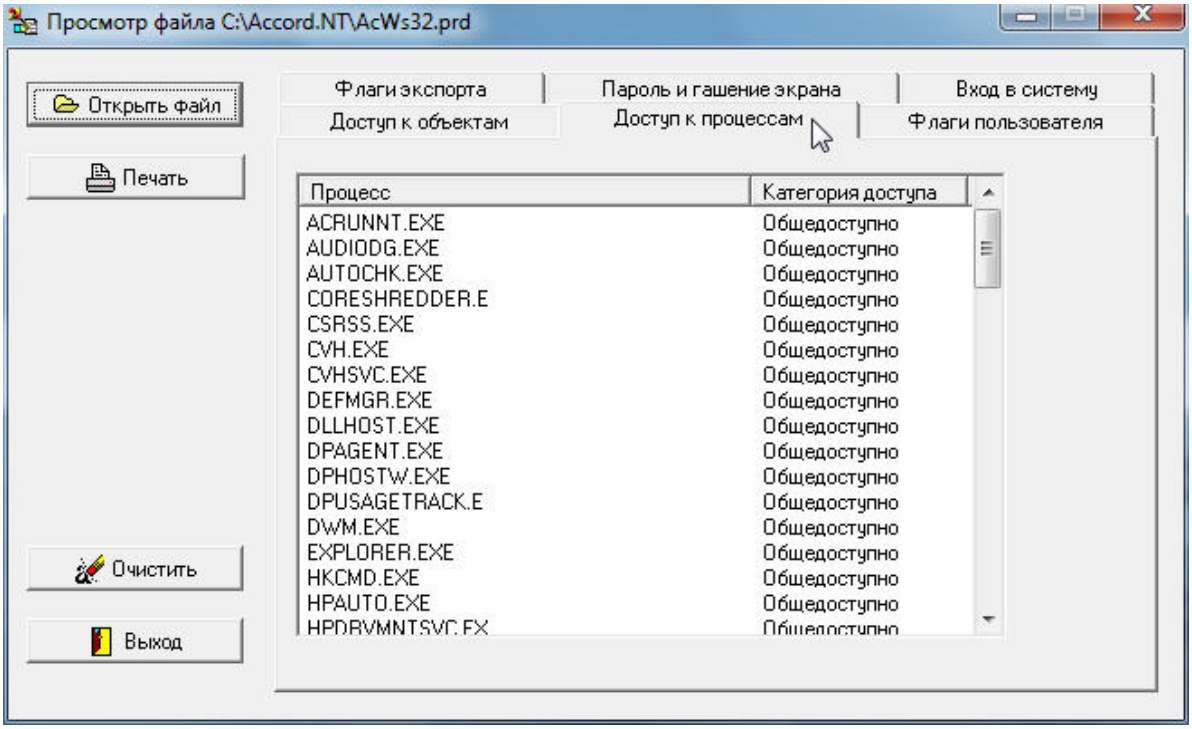

Рисунок 36 - Данные о правилах доступа и настройках пользователя

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.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№	Содержание изменения (обновления)	Дата	Примечание
1			
2			
3			
4			
5			
6			