ОКБ ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
37222406.26.20.40.140.091 97-ЛУ

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

Установка правил разграничения доступа Программа ACED32

37222406.26.20.40.140.091 97

АННОТАЦИЯ

Программа ACED32.EXE – редактор параметров (атрибутов) доступа пользователей к объектам доступа СВТ или АС - предназначена для описания (установки) правил разграничения доступа (ПРД) пользователей в соответствии с их полномочиями.

Программа используется администратором БИ 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») при настройке подсистемы разграничения доступа СПО «Аккорд-Win64 K» в соответствии с принятыми ПРД и входит в состав СПО «Аккорд-Win64 K».

Настоящее руководство предназначено для конкретизации действий администратора БИ (либо субъектов доступа, наделенных правами администратора) и содержит описание программы ACED32.EXE и порядок ее применения при установке СПО «Аккорд-Win64 K».

Перед эксплуатацией СПО «Аккорд-Win64 K» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые организационные меры защиты, рекомендуемые в документации.

Применение защитных механизмов СПО «Аккорд-Win64 K» должно дополняться общими мерами технической безопасности, а также физической охраной СВТ.

СОДЕРЖАНИЕ

1. Назначение программы 6
2. Запуск редактора прав доступа 7
2.1. Порядок запуска программы ACED32 7
2.2. Сохранение выполненных настроек 12
2.3. Выход из программы 12
3. Информация о программе 15
4. Регистрация новой группы пользователей 16
5. Редактирование параметров пользователей (прав доступа) 18
5.1. Регистрация нового пользователя 18
5.2. Печать параметров пользователя 24
5.3. Удаление пользователя из списка 24
5.4. Переименование пользователя в списке 25
5.5. Перемещение пользователя в другую группу 26
5.6. Поиск пользователя по идентификатору 26
6. Синхронизация параметров пользователя с параметрами группы 27
7. Администрирование подсистемы разграничения доступа 29
7.1. Задание имени пользователя 31
7.2. Регистрация идентификатора пользователя 31
7.3. Установка параметров пароля 34
7.4. Задание пароля пользователя 36
7.5. Установка детальности протокола работы пользователей 37
7.6. Установка режима блокировки экрана 41
7.7. Установка временных ограничений для сеанса работы пользователя 45
7.8. Блокировка пользователя 47
7.9. Установка стартовой задачи пользователя 47
7.10. Контроль целостности файлов 57
7.10.1. «Статический» контроль целостности файлов 57
7.10.2. «Динамический» контроль целостности файлов 61
7.11. Установка правил разграничения доступа (ПРД) к объектам доступа 64
7.11.1. Установка доступа к объектам с использованием дискреционного метода ПРД 65
7.11.2. Установка доступа к объектам с использованием мандатного метода контроля ПРД 77
7.12. Контроль процессов с использованием мандатного и/или дискреционного механизмов разграничения доступа 80

7.12.1. Общие сведения 80
7.12.2. Особенности настройки контроля процессов с использованием мандатного механизма разграничения доступа 81
7.12.3. Создание «белого» списка процессов с помощью мандатного и/или дискреционного механизма разграничения доступа с контролем процессов и динамического контроля целостности файлов из этого списка 92
7.13. Установка опций настройки 108
7.14. Установка фиксированных сетевых имен ресурсов общего пользования 109
7.15. Экспорт/импорт базы данных пользователей и правил разграничения доступа 111
7.15.1. Сохранение/загрузка базы данных пользователей 111
7.15.2. Экспорт/импорт правил разграничения доступа 113
7.16. Формирование списка разрешенных USB-устройств и SD-карт 116
7.17. Формирование правил доступа для отдельных программ (процессов) 119
7.18. Групповая политика и особенности установки ПРД на контроллере домена Windows 122
8. Заключение 125
Приложение 1. Файл ACCORD.INI – файл конфигурации СПО «Аккорд» 126
Лист регистрации изменений 131

ПРИНЯТЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

Администратор	– администратор службы безопасности информации
Имя_пользователя	– имя, под которым пользователь зарегистрирован в системе
Идентификатор	- специальное устройство, содержащее уникальный признак пользователя, с которым зарегистрированный пользователь входит в систему и который используется системой для определения его прав, а также для регистрации факта доступа и характера выполняемых им работ или предоставляемых ему услуг
Объект доступа	– под объектом доступа понимается один из перечисленных ресурсов СВТ: диск, каталог, файл, раздел или ключ реестра, процесс (задача), драйвер устройства
Параметры пользователя	– идентифицирующие признаки пользователя (имя, номер идентификатора, пароль) и его права по доступу к ресурсам СВТ в соответствии с его полномочиями
Пользователь	– субъект доступа к объектам (ресурсам) СВТ
ПРД	– правила разграничения доступа
Предъявить идентификатор	- приложить идентификатор к контактному устройству съемника информации, либо вставить идентификатор в USB-порт компьютера (в зависимости от типа используемого идентификатора)
Удаление пользователя	- удаление имени, под которым пользователь зарегистрирован в системе, из списка зарегистрированных пользователей в СПО «Аккорд»
СВТ	- средство вычислительной техники
Синхронизация параметров пользователя	- сопоставление БД пользователей подсистемы разграничения доступа с учетными записями пользователей Windows
Создать пользователя	– зарегистрировать пользователя в подсистеме разграничения доступа
Сообщения	– информация, выводимая на дисплей, которая сообщает о действиях пользователя, о состоянии программы и нормально завершенных действиях, сбоях в системе и др.
ТМ-идентификатор (или ТМ)	- персональный идентификатор DS-199x («Touch-memory» – «Память касания») пользователя
Число проходов при удалении	– количество записи случайной последовательности по содержимому файла при его удалении с очисткой

1. Назначение программы

Программа ACED32.EXE – редактор параметров (атрибутов) доступа пользователей при использовании в СПО «Аккорд-Win64 K» дискреционного и мандатного[1] механизмов к объектам СВТ или АС – предназначена для администрирования подсистемы разграничения доступа СПО «Аккорд».

Программа используется администратором БИ системы защиты информации (или субъектами доступа, наделенными правами администратора) при установке и эксплуатации СПО «Аккорд» для описания (определения) принятых в организации (учреждении и т.п.) правил разграничения доступа (ПРД) в соответствии с полномочиями пользователей.

Программа ACED32.EXE входит в состав СПО «Аккорд», инсталлируется на жесткий диск СВТ (PC) при его установке.

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

2. Запуск редактора прав доступа

ВНИМАНИЕ! Доступ к редактору прав доступа обеспечивается только Администратору БИ

2.1. Порядок запуска программы ACED32

Для запуска редактора параметров (атрибутов) доступа пользователей СПО «Аккорд» необходимо запустить программу C:\ACCORD.X64\ACED32.EXE (C:\ACCORD.NT\ACED32.EXE –для 32-битных ОС), выбрав мышью Пуск -> Все программы -> Аккорд-Win64 -> Редактор прав доступа (Пуск -> Все программы -> Аккорд-Win32 -> Редактор прав доступа). При первом запуске программы на экране появляется сообщение (рисунок 1):

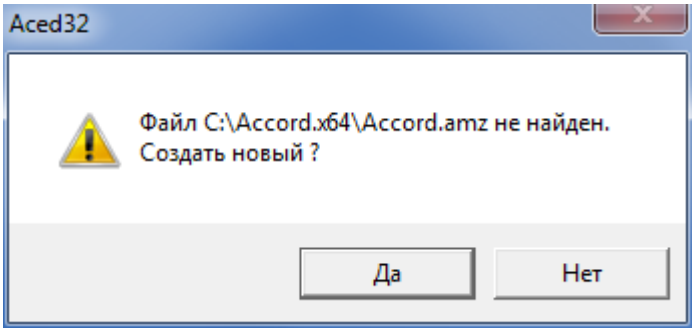

Рисунок 1 – Сообщение о создании новой базы пользователей

При нажатии кнопки <Да> в этом сообщении появляется главное окно программы, показанное на рисунке 2.

Главное окно программы состоит из следующих разделов:

- меню команд;
- управляющие кнопки, дублирующие действия меню команд;
- список пользователей (левая половина окна);

информация о выделенном пользователе (правая половина окна).

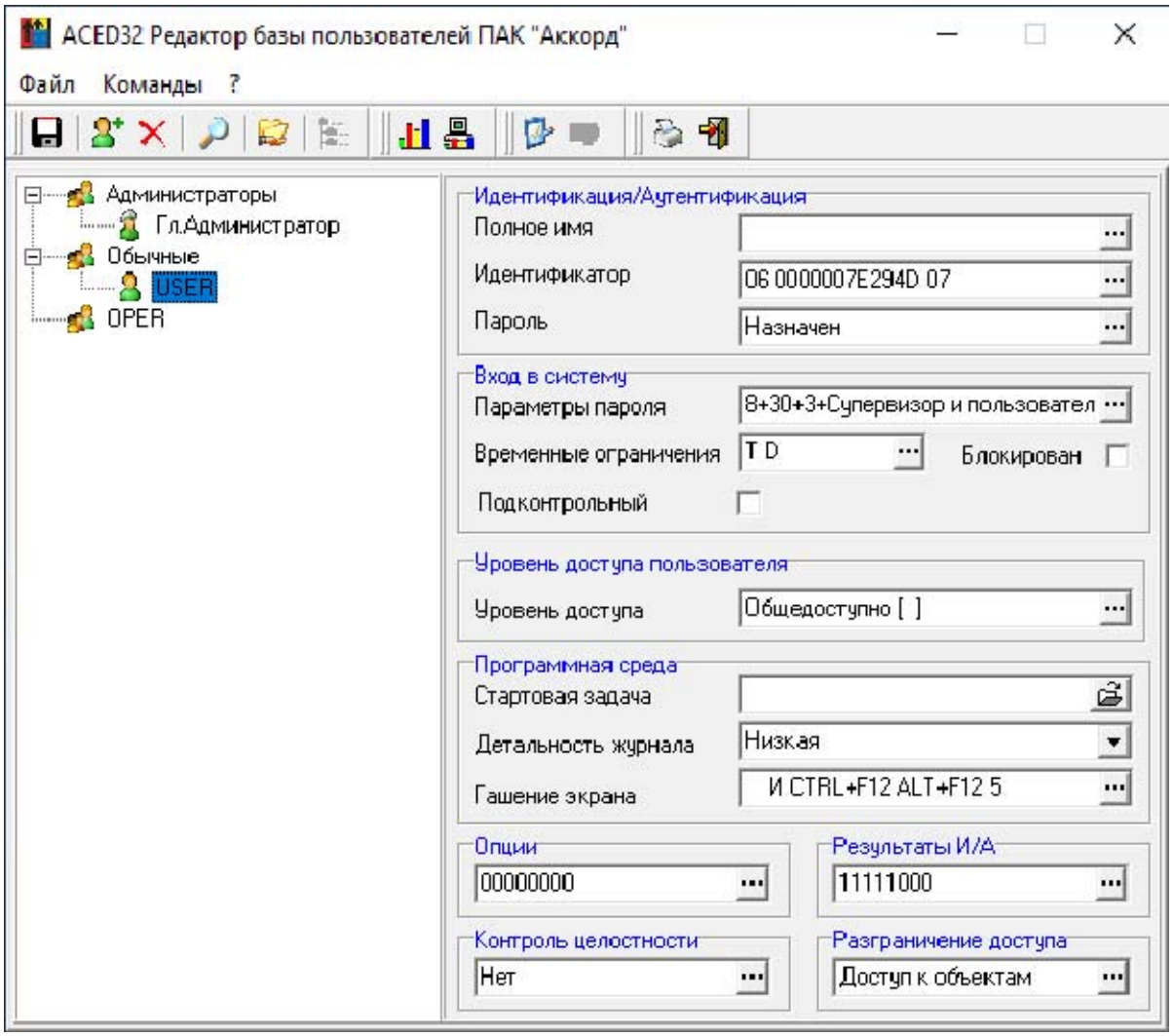

Рисунок 2 - Главное окно программы

Таблица 1 - Сообщения, выдаваемые программой при ее запуске, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Неверный идентификатор или пароль»	Введен пароль, не соответствующий данным идентификации	Введите правильный пароль
«Редактор может использовать только Администратор»	Попытка запуска редактора лицом, не являющимся администратором.	Используйте зарегистрированные данные для идентификации администратора или введите правильный пароль
Выход из ACED32 без предупреждения	Истекло время для использования данных для идентификации или ввода пароля	Перезапустите программу ACED32. Используйте данные для идентификации в течение времени, отведенного для этой операции

В случае если Администратор БИ не является Администратором ОС Windows, он может запустить редактор прав доступа. При этом:

1)если в программе настройки СПО «Аккорд» не установлены флаги «Синхронизация с базой пользователей NT» и «Мандатный + процессы», то запуск редактора прав доступа происходит так же, как и для Администратора ОС (см. п.2.1);

2)если в программе настройки СПО «Аккорд» установлены флаги «Синхронизация с базой пользователей NT» и флаг «Мандатный + процессы», то при запуске редактора прав доступа на экране появляется сообщение, показанное на рисунке 3.

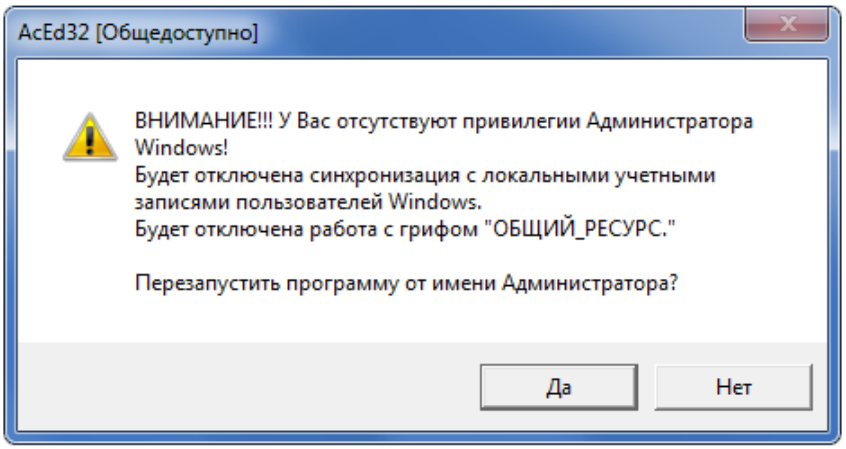

Рисунок 3 – Сообщение при запуске редактора прав доступа в случае если в настройке СПО «Аккорд» установлены флаги «Синхронизация с базой пользователей NT», «Контроль процессов»

3)если в программе настройки СПО «Аккорд» установлен флаг «Синхронизация с базой пользователей NT», но не установлен флаг «Мандатный + процессы», то при запуске редактора прав доступа на экране появляется сообщение, показанное на рисунке 4.

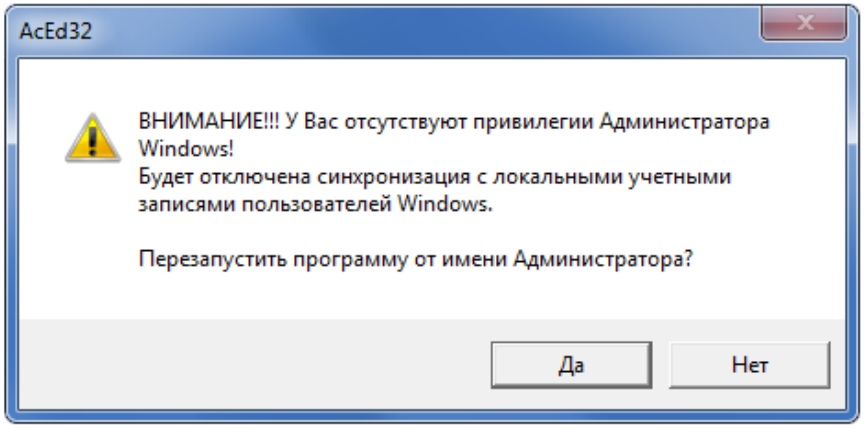

Рисунок 4 - Сообщение при запуске редактора прав доступа в случае если в настройке СПО «Аккорд» установлен флаг «Синхронизация с базой пользователей NT» и не установлен флаг «Контроль процессов»

4)если в программе настройки СПО «Аккорд» не установлен флаг «Синхронизация с базой пользователей NT», но установлен флаг «Мандатный + процессы», то при запуске редактора прав доступа на экране появляется сообщение, показанное на рисунке 5.

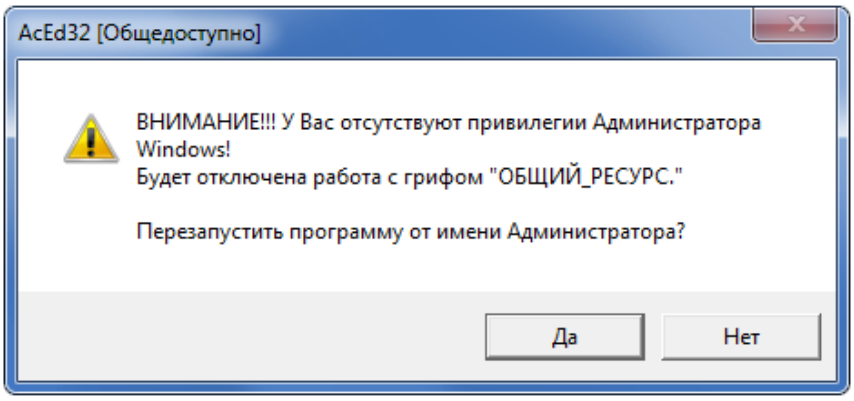

Рисунок 5 – Сообщение при запуске редактора прав доступа в случае если в настройке СПО «Аккорд» не установлен флаг «Синхронизация с базой пользователей NT», но установлен флаг «Контроль процессов»

Если в описанных сообщениях (рисунки 3-5) выбрать кнопку <Да> (т.е. выбрать перезапуск программы от имени Администратора ОС Windows), то появляется окно (рисунок 6), в котором предлагается ввести имя и пароль Администратора ОС Windows.

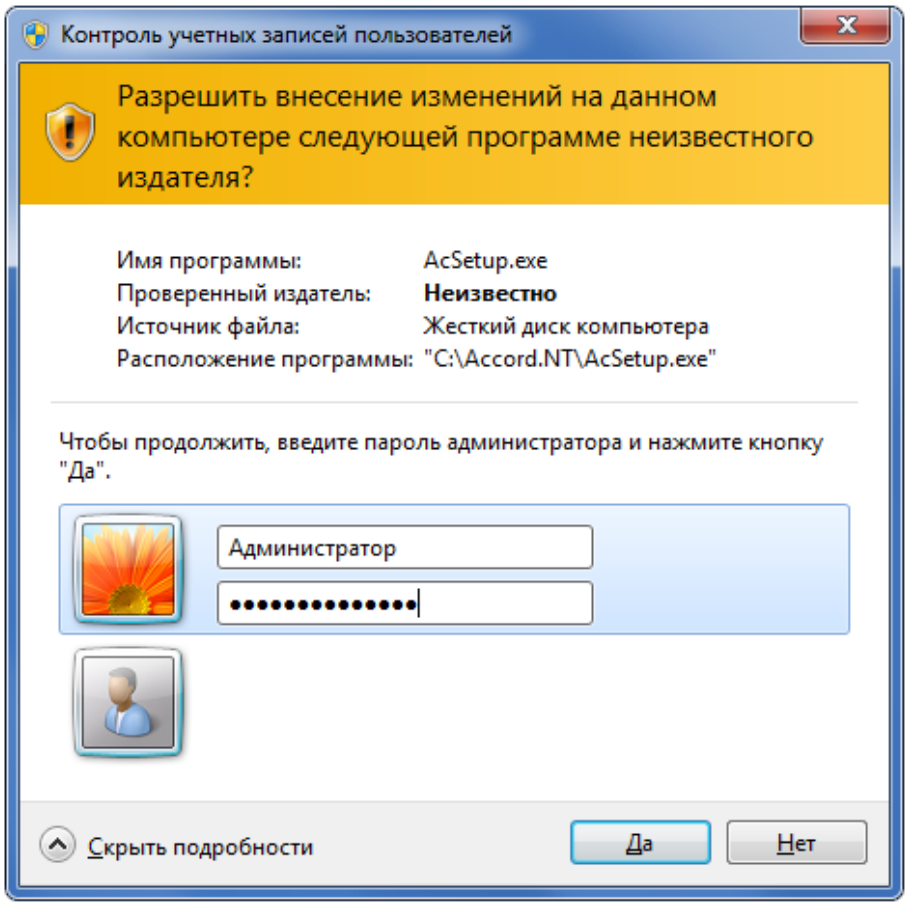

Рисунок 6 – Окно ввода пароля Администратора ОС Windows

После этого появляется главное окно программы ACED32 (рисунок 2), все функции которой доступны (так же, как и для Администратора ОС, см. п.2.1).

Если в описанных сообщениях (рисунки 3-5) выбрать кнопку <Нет> (т.е. продолжить запуск программы ACED32.EXE), то появляется главное окно

программы ACED32, две (или одна из двух)[2] функции которой заблокированы: синхронизация с локальными учетными записями ОС Windows, работа с грифом «ОБЩИЙ_РЕСУРС» (рисунок 7).

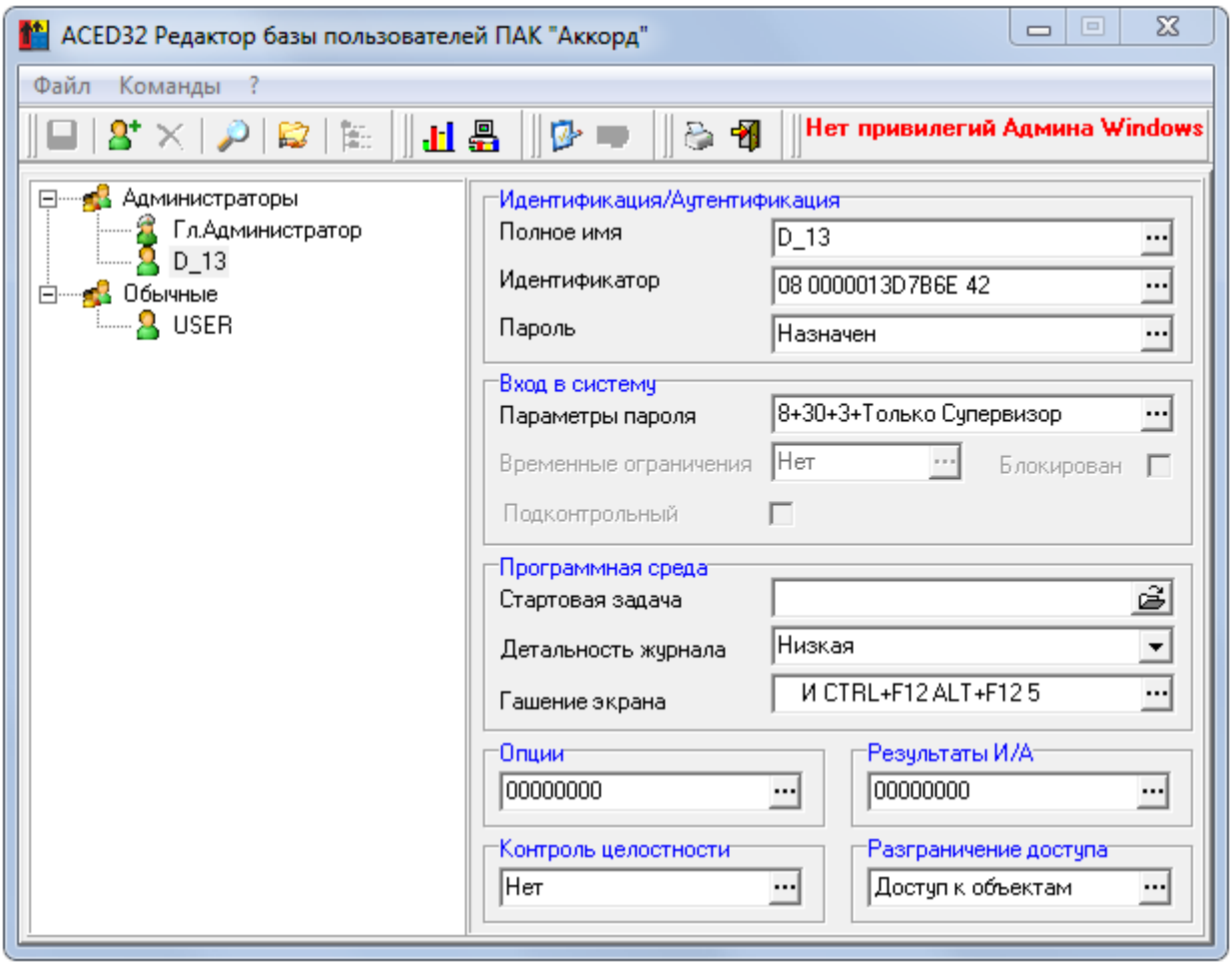

Рисунок 7 - Главное окно программы ACED32 с заблокированными функциями

В случае если Администратор БИ не является Главным Администратором СПО «Аккорд» и не является Администратором ОС Windows, то он может запустить редактор прав доступа. При этом в зависимости от выбранных настроек (см. п. 2.1) появляются сообщения 3-5.

Если в описанных сообщениях 3-5 выбрать кнопку <Да>, то после ввода имени и пароля Администратора ОС Windows (рисунок 6) программа ACED32 запускается в рамках новой сессии. При этом если в предыдущей сессии в ПРД пользователей был разрешен доступ к сетевым ресурсам, то в рамках новой сессии доступ к сетевым ресурсам отсутствует. В таком случае в список ПРД необходимо включить (ввести с клавиатуры) полные сетевые имена необходимых ресурсов.

Если в описанных сообщениях (рисунки 3-5) выбрать кнопку <Нет>, то появляется главное окно программы ACED32, две (или одна из двух)[3] функции

[2)] Зависит от того, какие флаги («Синхронизация с базой пользователей NT» и/или «Мандатный + процессы») установлены в программе настройки СПО «Аккорд» (см. п. 2.1)

[3)] Зависит от того, какие флаги («Синхронизация с базой пользователей NT» и/или «Мандатный + процессы») установлены в программе настройки СПО «Аккорд» (см. п.2.1)

которой заблокированы (рисунок 7). При этом доступ к сетевым ресурсам сохраняется. Кроме того, к ресурсам применяются такие же ПРД, как и к томам физического HDD.

ВНИМАНИЕ! В случае возникновения затруднений в работе с программой ACED32.EXE следует обратиться к справке (\Accord.x64\ACED32.html или (\Accord.NT\ACED32.html – в случае 32-битной ОС).

2.2. Сохранение выполненных настроек

Чтобы сохранить выполненные настройки, необходимо выбрать команду Файл\Сохранить или нажать кнопку <Сохранить базу> на панели инструментов в главном окне программы (рисунок 8).

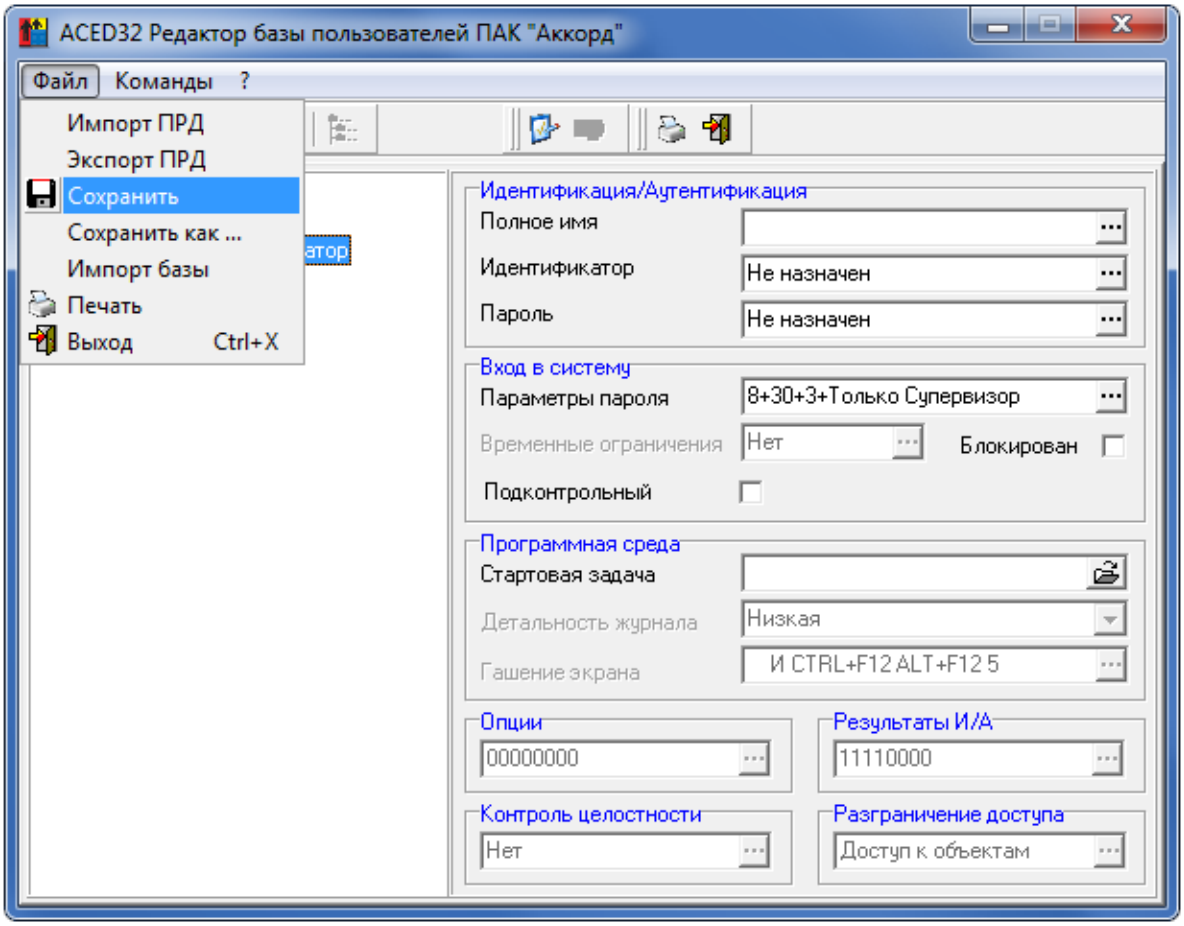

Рисунок 8 – Сохранение настроек

2.3. Выход из программы

В подменю «Файл» (рисунок 2) выберите команду «Выход»[4] или на панели инструментов нажмите кнопку <Выход из программы>.

[4)] Команде <Выход> в подменю <Файл> соответствуют клавиши <Ctrl+X>.

Если были внесены изменения в ПРД любого пользователя, то выводится запрос на подтверждение сохранения изменений. При выборе кнопки <ДА> все изменения базы пользователей будут сохранены. Если в программе настройки СПО «Аккорд» установлен флаг «Синхронизация с базой пользователей NT», то в процессе сохранения настроек может выводиться окно с требованием повторно ввести пароль пользователя. Связано это с тем, что формат хранения учетных записей пользователей в системе «Аккорд» кардинально отличается от ОС Windows, и программа ACED32 не хранит пароли в открытом виде в процессе работы. Некоторое неудобство, связанное с повторным вводом пароля, компенсируется высокой стойкостью защитных процедур к попыткам перехвата парольной информации. Если выбрать кнопку <Отмена>, то произойдет выход из программы без сохранения изменений в списке пользователей.

Если редактор прав доступа запущен не Администратором ОС, и в программе настройки СПО «Аккорд» установлен флаг «Синхронизация с базой пользователей NT», то при выходе из программы ACED32 появляется предупреждение (рисунок 9).

Таблица 2 - Сообщения, выдаваемые программой при выходе из нее, и порядок действий по ним:

Сообщение	**Причина**	**Порядок действий**
«Назначьте пользователю (*имя_пользователя)* пароль!»	Для пользователя зарегистрированы данные для идентификации, но не назначен пароль	Назначить пользователю (*имя_пользователя)* пароль, или отменить использование пароля: в поле «Параметры пароля» (установить минимальную длину пароля - 0)

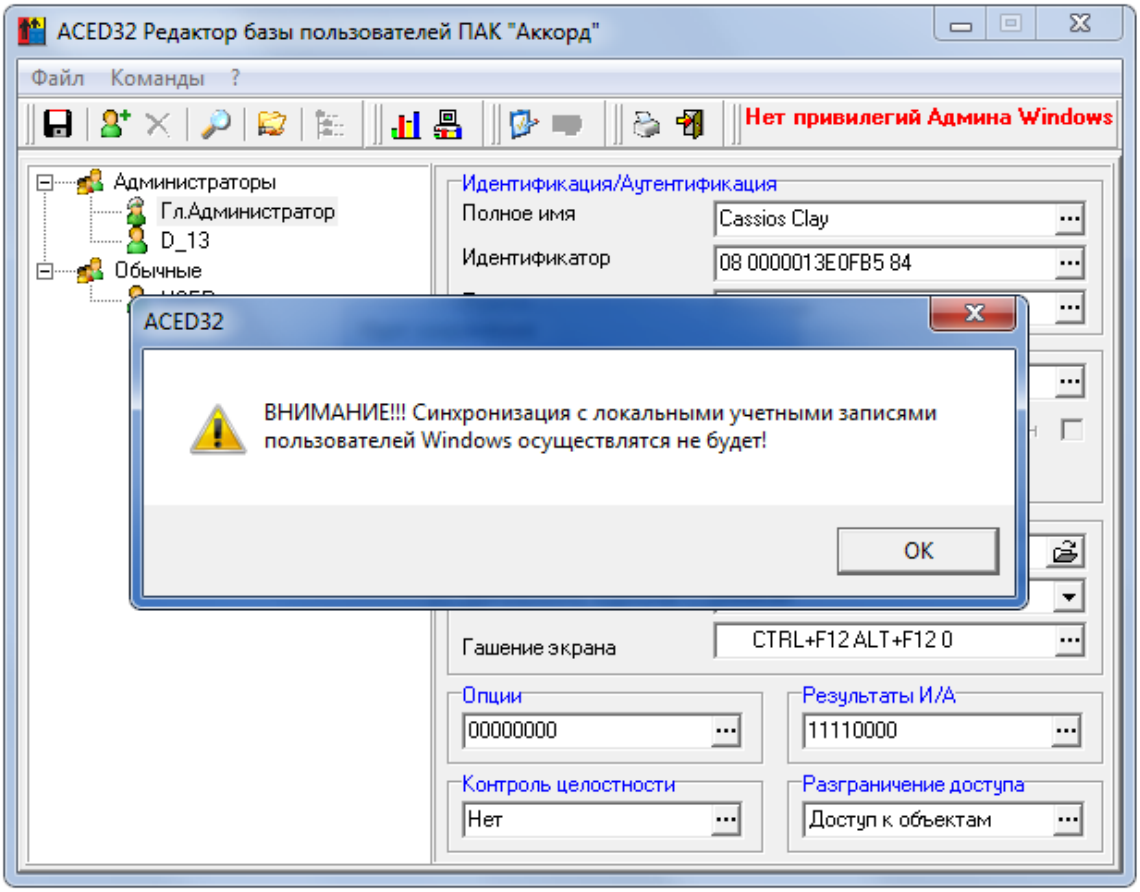

Рисунок 9 - Предупреждение, возникающее при выходе из программы

3. Информация о программе

Выберите команду <?> в меню главного окна программы (рисунок 2). В подменю <?> выберите команду <О программе>. На экран выводится окно, в котором отображена информация о программе, содержащая сведения о версии программы, типе ПРД (см. приложение accord.ini); максимальном количестве пользователей, которые могут быть зарегистрированы; типе БД СПО «Аккорд», разработчике программы. Для продолжения работы нажмите кнопку <ОК> или клавишу <Enter>.

4. Регистрация новой группы пользователей

В подменю «Команды» выберите команду «Создать» или нажмите кнопку <Создать> в главном окне программы (рисунок 10). На экран выводится окно, предлагающее выбрать тип создаваемого объекта. Установите отметку на строке «NT Группа» и введите имя новой группы пользователей. После этого следует выбрать кнопку <OK>. В главном окне программы появится новая группа.

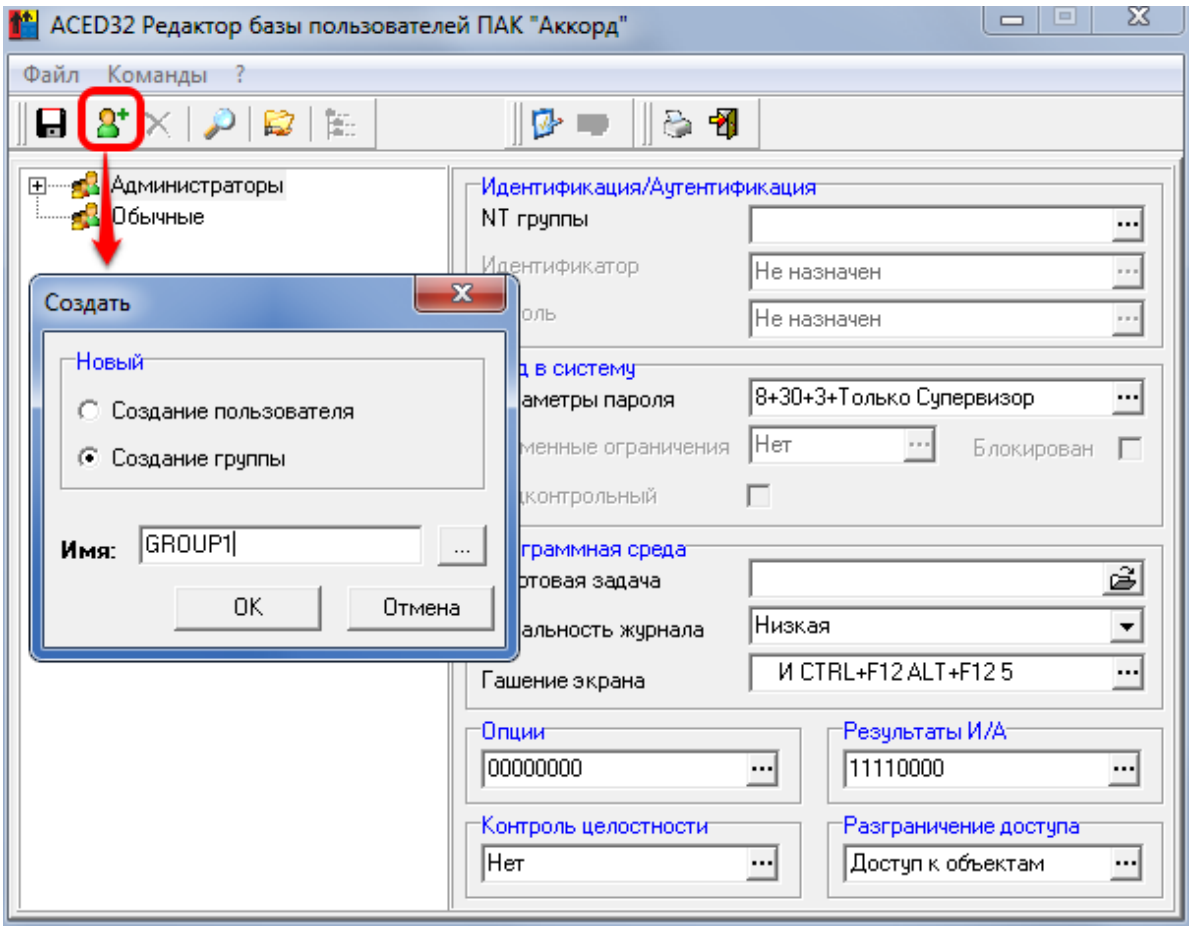

Рисунок 10 – Создание группы пользователей

Для группы можно задать параметры доступа к ресурсам СВТ.

Также для группы пользователей можно установить флаг «Коллективная работа». Данный флаг определяет режим работы, при котором пользователи соответствующей группы могут разблокировать компьютеры друг друга. Например, в группе с установленным флагом «Коллективная работа» состоят пользователи USER1 и USER2. Если USER1 заблокировал свой компьютер, то USER2 может разблокировать компьютер пользователя USER1[5]. При этом в СПО Аккорд» будет начата новая сессия для USER2. Однако в ОС Windows сессия останется прежней.

[5)] При этом пользователи должны знать пароли друг друга в ОС Windows

Для корректной работы опции «Коллективная работа» необходимо, чтобы в параметрах «Гашения экрана» был установлен флаг «Защита паролем» (рисунок 34).

Разблокировать компьютер пользователей из группы с установленным флагом «Коллективная работа» может также пользователь с привилегией «Оператор НШР».

Параметры, заданные для группы, автоматически присваиваются всем пользователям, которые в дальнейшем будут в ней созданы, но для каждого пользователя их можно изменить в индивидуальном порядке.

ВНИМАНИЕ! Если в группе ранее уже были созданы пользователи, то для применения к ним (всем или определенным) новых параметров группы необходимо выполнить процедуру синхронизации.

Подробнее об особенностях синхронизации параметров пользователей с параметрами группы см. в разделе 6.

5. Редактирование параметров пользователей (прав доступа)

5.1. Регистрация нового пользователя

Для создания нового пользователя в группе нужно выделить мышью группу, а затем в подменю «Команды» (рисунок 2) выбрать команду «Создать». На экран выводится окно, предлагающее выбрать тип создаваемого объекта. Установите отметку на строке «Пользователь» и введите имя нового пользователя (рисунок 11). Нажмите кнопку <OK> - в главном окне программы появится новый пользователь.

Примечание: если список пользователей активен, то при нажатии клавиши <Insert> также можно «создать» нового пользователя.

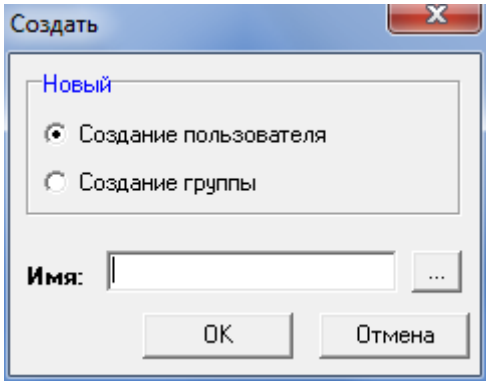

Рисунок 11 - Окно регистрации нового пользователя

Имя пользователя можно ввести с клавиатуры или выбрать из состава пользователей, уже зарегистрированных в ОС. Для этого достаточно нажать кнопку справа от поля ввода имени пользователя - открывается окно списка существующих пользователей (рисунок 12).

Если новый пользователь зарегистрирован в AD на контроллере домена, и администратор безопасности взаимодействует с администратором домена, то в поле «Сервер» следует задать имя или IP-адрес компьютера, на котором находится база данных пользователей.

При нажатии кнопки <OK> запрашиваются имя и пароль администратора контроллера домена, и если информация введена правильно, можно выбрать пользователя из списка.

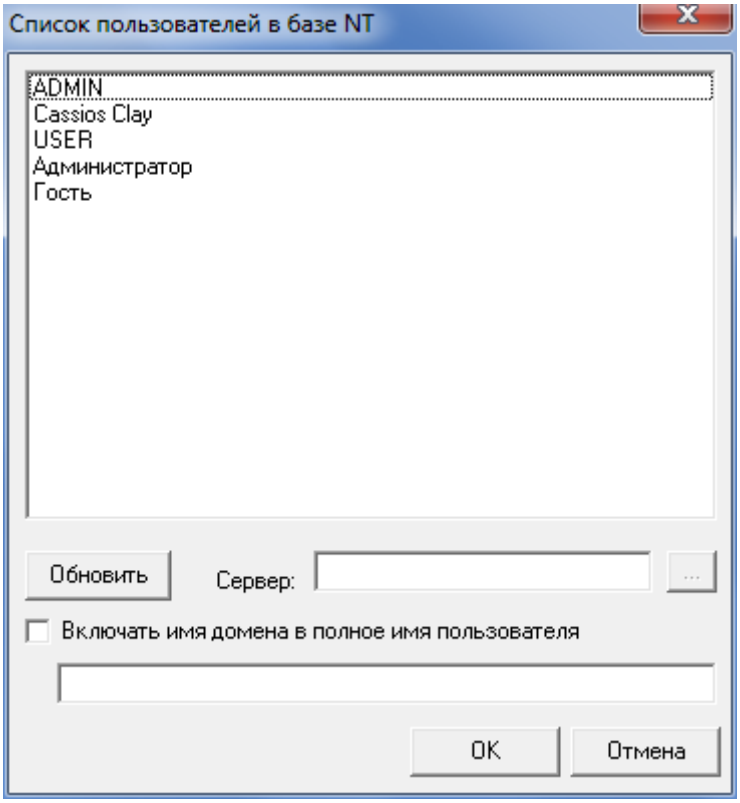

Рисунок 12 - Окно выбора нового пользователя

Если в настройке СПО «Аккорд» установлен флаг «Использовать полное имя в учетных записях NT», то в нижней части окна становятся доступными флаг «Включать имя домена в полное имя пользователя» и поле для ввода имени домена. В этом случае в качестве основного используются первые 12 символов имени, а в поле «Полное имя» заносится <имя_пользователя>@ <имя_домена> (либо <имя домена> \ <имя пользователя>).

В качестве основного имени пользователя можно использовать заглавные латинские буквы, цифры и _ (символ подчеркивания).

ВНИМАНИЕ! При создании пользователей необходимо учитывать, что если:

– в настройках комплекса не установлен флаг «Синхронизация с базой пользователей NT», пользователи домена не заносятся в локальную базу NT;

– в настройках комплекса установлен флаг «Синхронизация с базой пользователей NT», пользователи домена заносятся в локальную базу NT;

– в настройках комплекса установлен флаг «Синхронизация с базой пользователей NT» и не установлен флаг «Использовать полное имя в учетных записях NT», пользователи домена заносятся в локальную базу NT;

– в настройках комплекса установлен флаг «Синхронизация с базой пользователей NT», не установлен флаг «Использовать полное имя в учетных записях NT», но имена пользователей содержат имена домена, пользователи домена не заносятся в локальную базу NT.

Более подробно варианты работы с доменными пользователями описаны в п.7.18.

При нажатии кнопки <Отмена> регистрация нового пользователя производиться не будет.

Таблица 3 - Сообщения, выдаваемые при регистрации пользователей, и порядок действий по ним

Сообщение	Причина	Порядок действий
«Пользователь с таким именем уже есть»	Пользователь с таким именем уже есть в списке пользователей	Назначьте новому пользователю уникальное имя
«Задайте имя, пожалуйста»	Имя пользователя не задано	Назначьте новому пользователю имя

Встречаются случаи, когда возможность выполнить регистрацию пользователей непосредственно на терминальном сервере отсутствует. Например, когда пользователи находятся территориально удаленно от терминального сервера.

В этом случае необходимо копировать информацию о пользователях (данные для идентификации пользователей, хэш-функцию от ключа пользователя, служебные данные) в файл *.atf посредством утилиты AcTmReg.EXE (см. п.2.5.2 документа «Инструкция по установке» 37222406.26.20.40.140.091 98).

Далее этот файл необходимо переслать администратору безопасности информации терминального сервера любым способом (например, по электронной почте).

Затем на терминальном сервере информацию из файла *.atf следует добавить в базу пользователей СПО «Аккорд» (файл *.amz). Для этого необходимо выполнить следующие действия:

1) запустить программу ACED32.EXE;

2) в главном меню ACED32.EXE выбрать Команды\Создать;

3) в появившемся окне выбрать флаг «Создание группы», в поле «Имя» ввести имя группы. Далее нажать кнопку <Импорт пользователей из *.atf файлов> (рисунок 13);

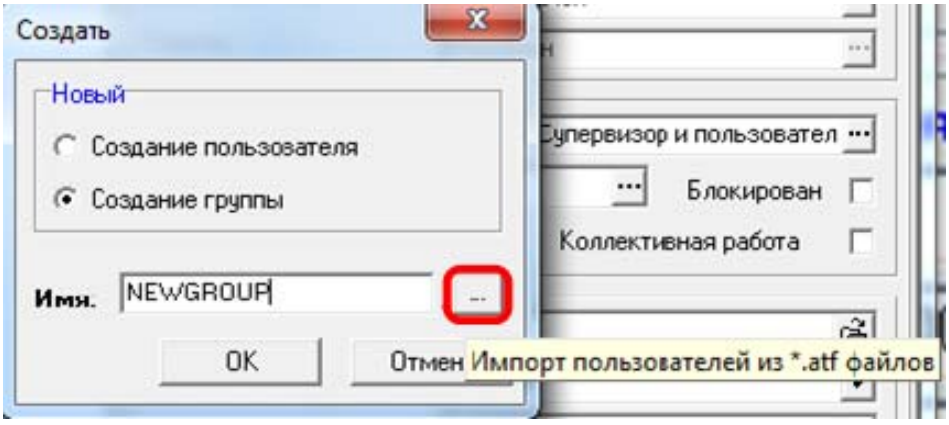

Рисунок 13 – Импортирование пользователей из файла .atf

4) при нажатии кнопки <Импорт пользователей из *.atf файлов> (рисунок 13) появляется окно, в котором нужно выбрать один или несколько файлов формата *.atf и нажать кнопку <Открыть> (рисунок 14);

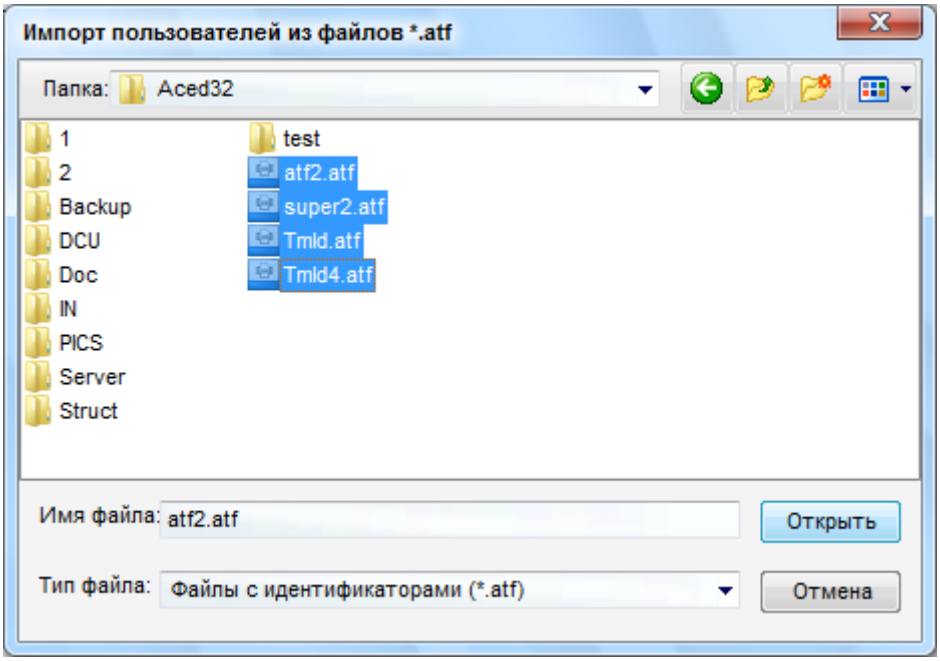

Рисунок 14 – Выбор файлов формата .atf

5)при выполнении процедуры импорта пользователей из файла *.atf в базу пользователей СПО «Аккорд» (accord.amz) в качестве основного имени пользователя записываются первые 12 символов значения поля «Описание» утилиты AcTmReg.EXE. При этом в поле «Полное имя» в ACED32.EXE записываются все символы поля «Описание» утилиты AcTmReg.EXE. Имеется возможность редактирования полного имени (рисунок 15, при редактировании следует помнить, что количество символов в поле «Полное имя» ограничено 34 символами);

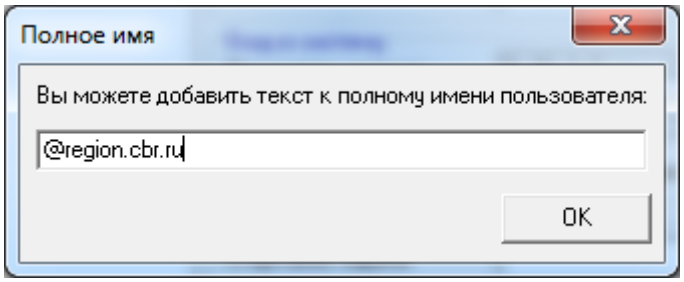

Рисунок 15 – Редактирование полного имени пользователя

6)для сохранения изменений нажать кнопку <OK> (рисунок 15). При нажатии кнопки выполняется проверка корректности полного имени пользователя (имя пользователя должно состоять из английских букв, цифр и символа «_»), а также проверка наличия пользователя с таким именем в базе ПАК «Аккорд». Если пользователь с полным именем «NAME» существует в базе, то к его имени добавляется сквозная нумерация, при этом возможно урезание имени (из-за ограничения его 12 символами). В журнале импорта пользователей в этом случае появляется запись «Пользователь NAME создан под именем ATF_XXX»;

7) после выполнения проверки выполняется импортирование пользователей из *.atf файлов в базу пользователей СПО «Аккорд». Если процедура импорта выполняется успешно, появляется сообщение:

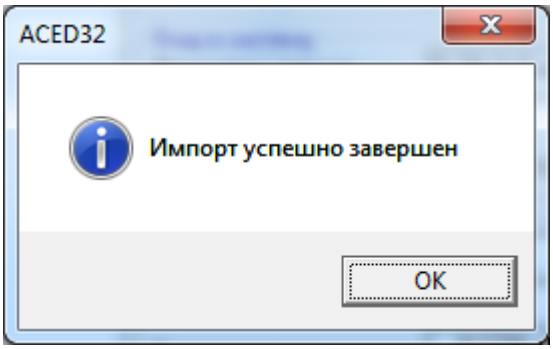

Рисунок 16 – Сообщение об успешном выполнении процедуры импорта пользователей из файлов *.atf в файл *.amz

После успешного импорта в базу СПО «Аккорд» добавляются пользователи с присвоенными им идентификаторами и открытыми ключами. Пароли пользователей сбрасываются. Выполняется синхронизация параметров пользователей, импортированных из файла *.atf, с параметрами группы, в которую они импортированы.

Если процедура импорта выполняется с ошибками, то появляется следующее сообщение:

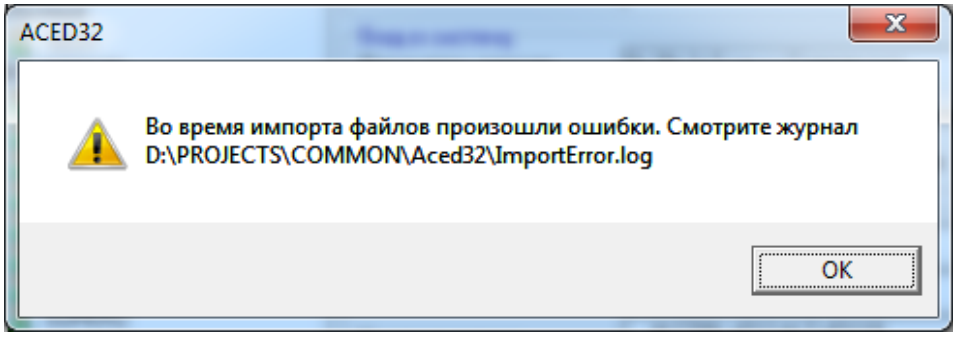

Рисунок 17 – Сообщение об ошибках во время выполнения процедуры импорта пользователей из файлов *.atf в файл *.amz

Для получения подробного описания ошибок, которые произошли при выполнении процедуры импорта пользователей из файлов *.atf в файл *.amz, необходимо просмотреть журнал событий ImportError.log.

Импортирование пользователей из файлов *.atf можно осуществить с помощью командной строки. Переход на работу с командной строкой осуществляется, если есть хотя бы один ключ. Информация выводится на консоль. Все сообщения пропадают через 5 секунд.

Для импорта используются следующие ключи:

-d Задать каталог с atf-файлами для импорта. Путь к каталогу указывается сразу после ключа, без пробела или в кавычках. Если ключ не задан, то поиск будет выполняться в каталоге, из которого запущено приложение.

Примеры: -dC:\ATF_IMPORT\ , "-d C:\ATF_IMPORT\"

-r Задать каталог, в который будут перемещены обработанные atf-файлы. Путь к каталогу указывается сразу после ключа, без пробела или в кавычках. Если ключ не задан, то файлы будут перемещены в подкаталог ..\ATF_END.

Примеры: -rC:\ATF_OUT\ , "-r C:\ATF_OUT\"

-z Задать файл базы Аккорд-Win32/64. Путь к файлу указывается сразу после ключа, без пробела или в кавычках. Если ключ не задан, то будет выполнен поиск файла accord.amz в каталоге из которого запущено приложение.

Примеры: -zC:\AMZ\accord.amz , "-z C:\AMZ\accord.amz"

-l Задать файл для записи журнала. Путь к файлу указывается сразу после ключа, без пробела или в кавычках. Если ключ не задан, то журнал будет писаться в файл ..\ATF_END\AtfImport.log

Примеры: -lC:\logs\atfimport.log , "-l C:\AMZ\accord.amz"

-g Задать имя группы пользователей, в которую будет выполнен импорт. Имя группы должно состоять из латинских букв, цифр. Длина имени не должна превышать 12 символов. Если ключ не задан, то импорт будет выполнен в группу «Обычные».

Примеры: -gOPERATOR "-g OPERATOR"

Также с помощью командной строки можно базу пользователей «Аккорд», содержащуюся в файле *.amz, экспортировать в файл *.lst. Для этого используются следующие ключи (порядок и регистр ключей не важен):

/convert:filename
/base:basename MPH username

Если указано просто filename, то создается файл в текущем каталоге. Если filename указано с путем, то создается файл по указанному пути. Если filename не имеет расширения, то добавляется расширение .lst.

Если поле filename пусто, то создается файл users.lst в текущем каталоге.

Если поле basename пусто, то используется файл accord.amz из текущего каталога.

Если basename указано с путем, то используется файл accord.amz по указанному пути.

Параметр MPH определяет следующие значения вывода:

M – вывод основных параметров;

P – вывод ПРД;

H – вывод КЦ.

Параметр username используется опционально: при его отсутствии выведется информация обо всех пользователях базы, при указании в этом поле имени отдельного пользователя или группы будет выведена информация, соответствующая заданному значению (имени).

Пример1: AcEd32.exe /convert:c:\users.txt /base:c:\accord.x64\accord.amz MPH Обычные

База из каталога c:\accord.x64 экспортируется в файл c:\users.txt с выводом основных параметров, ПРД и КЦ группы «Обычные».

Пример2: AcEd32.exe /convert

База accord.amz из текущего каталога экспортируется в файл users.lst в текущем каталоге.

5.2. Печать параметров пользователя

Для хранения и учета параметров пользователей необходимо выбрать Файл -> Печать (рисунок 2).

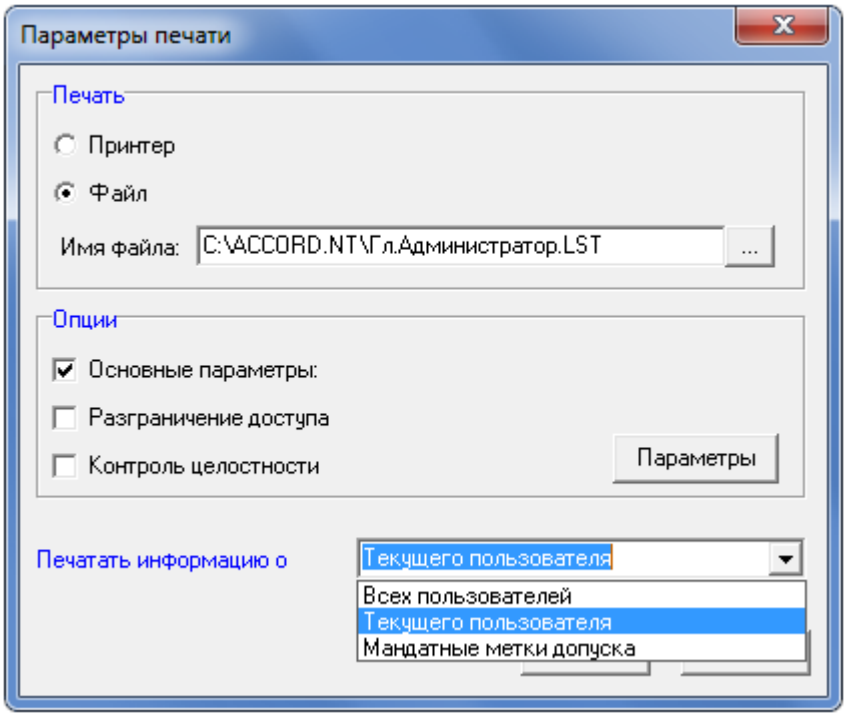

Рисунок 18 - Окно для выбора параметров пользователя и устройства печати

Команда «Печать» предназначена для вывода списка параметров пользователя на твердый носитель (принтер) или в файл (магнитный носитель).

В подменю «Команды» главного меню программы выберите команду «Печать» или на панели инструментов нажмите кнопку <Печать информации> - выводится окно «Параметры печати», показанное на рисунке 18.

Выберите параметры пользователя, необходимые для вывода, и устройство, на которое они будут записаны. Далее нажмите кнопку <ОК> или клавишу <F2>, для отмены операции следует нажать кнопку <Отмена> или <Esc>.

Примечание: если осуществляется запись параметров пользователя в файл, то по умолчанию создается файл <имя_пользователя>.LST в рабочем каталоге.

5.3. Удаление пользователя из списка

С помощью мыши или клавиатуры выделите пользователя, которого следует удалить. Выберите Команды -> Удалить или на панели инструментов

нажмите кнопку <Удалить пользователя>. Программа выдает запрос «Вы действительно хотите удалить пользователя *<имя_пользователя>*?» Подтвердите или отмените удаление.

Примечание: если список пользователей активен, то можно удалить выделенного пользователя, нажав на клавишу <Delete>.

Можно удалить нескольких пользователей из группы, выделив ее и выбрав во всплывающем меню пункт «Удалить пользователей». При этом появится окно «Выбор пользователей» с полным списком пользователей выделенной группы. Все отмеченные в этом окне пользователи будут удалены.

Также можно удалить группу целиком, выбрав Команды -> Удалить или на панели инструментов нажав кнопку <Удалить группу>. Программа выдает запрос «Вы действительно хотите удалить группу *<имя_группы>*?», при подтверждении которого группа будет удалена вместе с учетными записями всех входящих в нее пользователей.

ВНИМАНИЕ! Нельзя удалить группы «Администраторы» и «Обычные», а также пользователя «Гл.Администратор».

5.4. Переименование пользователя в списке

С помощью мыши или клавиатуры выделите пользователя, которого Вы хотите переименовать. В подменю «Команды» выберите «Переименовать» или щелкните правой кнопкой мыши на выделенном пользователе и выберите из всплывающего меню команду <Переименование>.

Выводится окно (рисунок 19), предлагающее ввести новое имя пользователя.

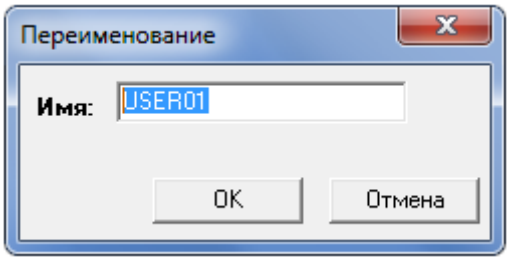

Рисунок 19 - Переименование пользователя

<OK> или <Enter> - изменение имени, «Отмена» – отмена операции переименования.

Примечание: если список пользователей активен, то можно переименовать выделенного пользователя, нажав на клавишу <F2>.

Таблица 4 - Сообщения, выдаваемые программой при регистрации пользователей, и порядок действий по ним

Сообщение	Причина	Порядок действий
«Пользователь с таким именем уже есть»	Пользователь с таким именем уже есть в списке	Назначьте пользователю новое уникальное имя
«Задайте имя, пожалуйста»	Имя пользователя не задано	Назначьте пользователю имя

5.5. Перемещение пользователя в другую группу

Пользователей можно переместить в другую группу. Для этого следует выделить группу, в которой находятся эти пользователи, и выбрать во всплывающем меню пункт «Переместить пользователей». При этом появится окно «Выбор пользователей» с полным списком пользователей выделенной группы. В этом окне следует отметить необходимых пользователей и нажать <Далее>. Появится следующее окно – «Выберите группу», в котором предлагается из списка имеющихся групп выбрать ту, в которую будут помещены отмеченные ранее пользователи. Обратите внимание, что при перемещении в другую группу флаги синхронизации с группой у этих пользователей будут сброшены.

5.6. Поиск пользователя по идентификатору

По идентификатору можно найти соответствующего ему пользователя. Для этого необходимо выбрать в подменю «Команды» пункт «Поиск» или на панели инструментов нажать кнопку <Поиск пользователя по идентификатору> - на экран выводится окно (рисунок 20) с запросом идентификатора.

Если присоединить идентификатор к контактному устройству (считывателю) в отведенный интервал времени, то в списке выделяется пользователь, которому принадлежит данный идентификатор.

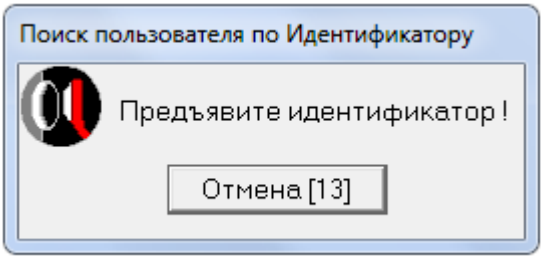

Рисунок 20 - Запрос идентификатора для поиска

Таблица 5 - Сообщения, выдаваемые программой и порядок действий по ним

Сообщение	Причина	Порядок действий
«Пользователь не найден»	Идентификатор не принадлежит ни одному из пользователей	Попробуйте предъявить другой идентификатор

6. Синхронизация параметров пользователя с параметрами группы

Синхронизация может понадобиться при изменении параметров группы и последующем присвоении этих параметров одному или нескольким пользователям.

Синхронизация параметров может быть выполнена двумя способами:

1. Синхронизация параметров одного пользователя с параметрами группы.

В списке пользователей с помощью мыши выделите пользователя, параметры которого Вы хотите синхронизировать. Правой кнопкой мыши щелкните на имени выделенного пользователя, на экране появится всплывающее меню. Выберите из него пункт «Синхронизировать».

Процедура синхронизации параметров выбранного пользователя с параметрами группы также может быть запущена с использованием команды главного меню программы ACED32: Файл -> Команды -> Синхронизировать.

Выводится окно «Выбор параметров синхронизации», показанное на рисунке 21. Установите те параметры пользователя, которые будут синхронизированы. Для выполнения синхронизации нажмите кнопку <Синхронизация> или клавишу <F2>, для отмены - <Отмена> или <Esc>.

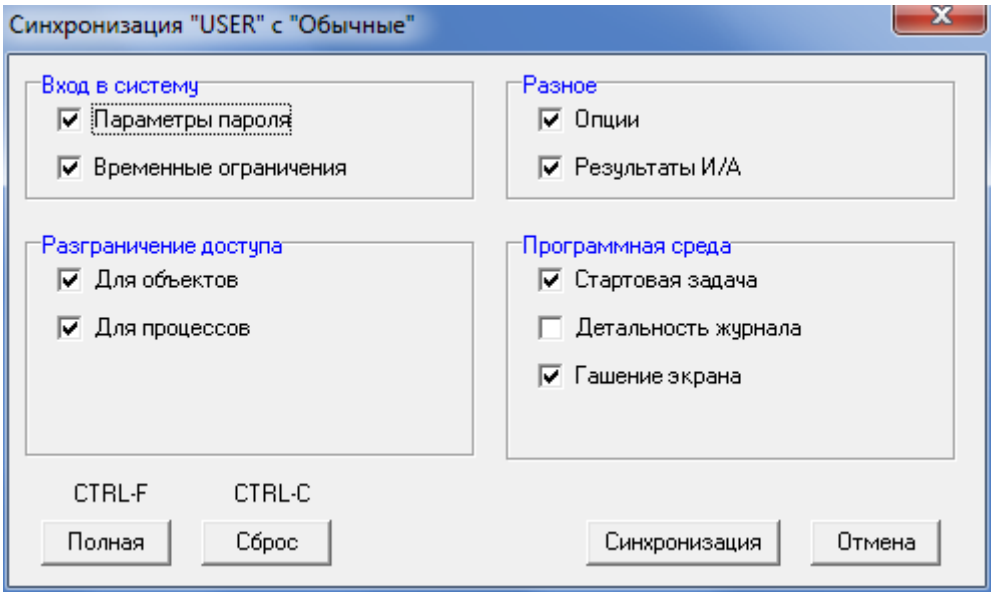

Рисунок 21 - Параметры синхронизации

Примечание: для группового манипулирования параметрами синхронизации пользуйтесь кнопками <Полная> или клавишами <Ctrl+F> - устанавливает все параметры; и <Сброс> или <Ctrl+C>- сбрасывает все параметры.

2. Синхронизация параметров группы с параметрами одного или нескольких пользователей.

В списке групп с помощью мыши выделите группу, параметры которой Вы хотите синхронизировать. Правой кнопкой мыши щелкните на названии выделенной группы - появится всплывающее меню. Выберите из него пункт «Синхронизировать».

Процедура синхронизации параметров выбранной группы с параметрами пользователей также может быть запущена с использованием команды главного меню программы ACED32: Файл -> Команды -> Синхронизировать.

В появившемся окне следует выбрать из списка пользователей, с параметрами которых необходимо синхронизировать параметры группы, и нажать кнопку <Далее>.

Выводится окно «Выбор параметров синхронизации», показанное на рисунке 21. Установите те параметры группы, которые будут синхронизированы для выбранных пользователей. Для выполнения синхронизации нажмите кнопку <Синхронизация> или клавишу <F2>, для отмены - <Отмена> или <Esc>.

Таблица 6 - Сообщения, выдаваемые программой при синхронизации параметров пользователей, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Выберите, пожалуйста, объект для синхронизации»	Не выбран объект для синхронизации	Выберите объект для синхронизации, щелкнув левой кнопкой мыши на его имени

7. Администрирование подсистемы разграничения доступа

Администратор БИ может производить изменение параметров доступа субъектов к объектам СЗИ. Для этого в списке пользователей выберите имя пользователя, параметры которого необходимо отредактировать.

Примечание: некоторые «Параметры пользователя» являются обязательными, без которых невозможен ввод остальных (например, «Идентификатор» и «Пароль»). Группы «Администраторы» и «Обычные» создаются при инициализации БД пользователей СПО «Аккорд», и их нельзя переименовать или удалить. Параметры группы являются универсальным шаблоном для задания «Параметров пользователя» и присваиваются по умолчанию каждому создаваемому пользователю.

Пользователям из группы «Администраторы» по умолчанию разрешен доступ ко всем локальным ресурсам компьютера. Доступ к сетевым ресурсам определяется настройками сети.

Все пользователи из группы «Администраторы» по умолчанию обладают привилегиями, изменять которые может только главный Администратор (рисунок 22):

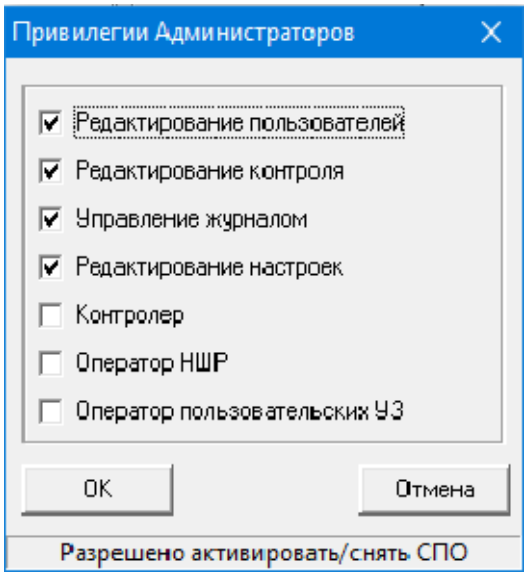

Рисунок 22 – Привилегии Администраторов

Привилегии Администраторов включают следующие поля:

- «Редактирование пользователей» – позволяет создавать и удалять пользователей и группы пользователей, а также редактировать параметры пользователей (имя пользователя, идентификатор, пароль, параметры пароля, см. рисунок 2);
- «Редактирование контроля» - позволяет устанавливать списки аппаратуры, файлов, системных областей диска для контроля целостности ;

- «Управление журналом» – позволяет выполнять процедуры архивирования и разархивирования журналов, формировать правила разграничения доступа на основе информации в журнале регистрации событий;
- «Редактирование настроек» – позволяет устанавливать необходимые настройки с помощью утилиты AcSetup.exe (подробнее см. документ «Руководство по установке» 37222406.26.20.40.140.091 98, п. 2.1).

  При установке верхних четырех флагов (рисунок 22) в строке статуса окна «Привилегии Администраторов» появится запись «Разрешено активировать/снять СПО». В случае отсутствия хотя бы одного из этих флагов запись в строке статуса будет информировать о запрете администратору выполнения команд активации/снятия (рисунок 23).

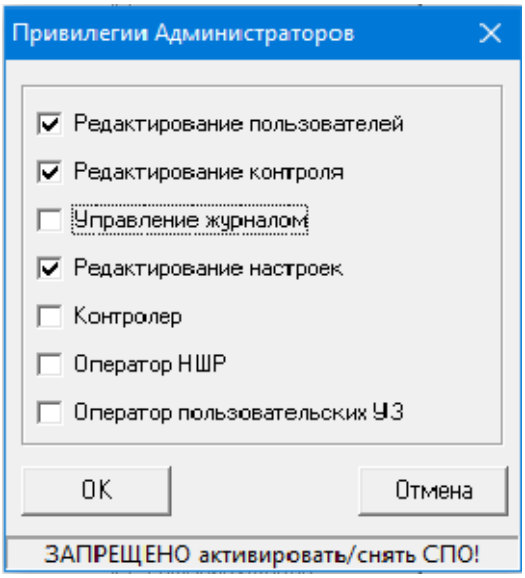

Рисунок 23 - Информирование о запрете выполнения команд активации/снятия СПО

- «Контролер» – позволяет контролировать доступ пользователей к рабочим станциям. Задача пользователя с привилегией «Контролер» – контролировать запуск пользователя с установленным флагом «Подконтрольный»: для входа в учетную запись «подконтрольному» пользователю помимо своего идентификатора и пароля потребуется предъявление идентификатора и пароля пользователя с привилегией «Контролер»;
- «Оператор НШР» - может выполнять выход из Хранителя экрана других пользователей;
- «Оператор пользовательских УЗ» - установка этой привилегии позволяет выделенному Администратору осуществлять просмотр отдельных пользователей базы во всех группах, кроме группы «Администраторы», и редактирование следующих параметров: создание/удаление/переименование имени (полного имени) и экспорт/импорт информации о пользователе (группе) в/из файл(а) *.atf.

Если у пользователя группы «Администраторы» в разделе «Привилегии Администраторов» снят флаг:

- «Редактирование пользователей» – запрещено редактирование правил разграничения доступа пользователя (запрещена модификация файлов Accord.amz, *.ACT, Accord.PRC);
- «Управление журналом» – запрещена работа с журналами регистрации (запрещена модификация файлов *.LOW, *.LOG);
- «Редактирование настроек» – запрещена модификация файлов Accord.ini, AcTskMng.ini[6].

Привилегия «Контролер» может быть установлена как для пользователя группы «Администраторы», так и для пользователя группы «Обычные».

Пользователь с привилегией «Контролер» может выполнять вход в операционную систему, если это не запрещено настройками ПРД.

Если в разделе «Привилегии Администраторов» установлен флаг «Контролер», а остальные флаги сняты, то для того, чтобы пользователь мог запустить редактор прав доступа ACED32.EXE, необходимо в политиках операционной системы установить данному пользователю полный доступ к каталогу C:/Accord.x64/ (C:/Accord.NT/ – для 32-битной ОС) (при выбранных настройках пользователь может запустить редактор прав доступа, но не имеет возможности вносить какие-либо изменения).

7.1. Задание имени пользователя

Администратор должен присваивать каждому пользователю уникальное в данной вычислительной среде (отдельный компьютер или локальная сеть) имя. Имя пользователя задается только при регистрации нового пользователя. Параметр «Полное имя» не является обязательным параметром, задается по желанию администратора, и может использоваться для идентификации пользователя в ОС, если в программе настройки СПО «Аккорд» установлен параметр «Использовать полное имя в учетных записях NT» (подробнее п.6.17).

7.2. Регистрация идентификатора пользователя

В поле «Идентификатор» главного окна (рисунок 2) отображается информация об идентификаторе активного (выделенного) пользователя. Пока пользователю не назначен идентификатор, в окне редактирования недоступны для изменения другие параметры. Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «Идентификатор» или клавишу <Enter>. Появится окно «Работа с ключом пользователя» (рисунок 24).

---

[6] Если у пользователя группы «Администраторы» в разделе «Привилегии Администраторов» снят один из флагов: «Редактирование пользователей», «Управление журналом», «Редактирование настроек», то для такого пользователя действуют правила разграничения доступа СЗИ от НСД «Аккорд», и ему нужно прописать полный доступ к дискам и к сети.

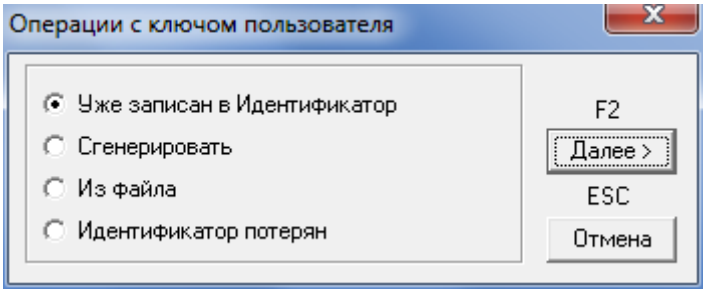

Рисунок 24 - Работа с ключом пользователя

Идентификатор, в котором не записан ключ пользователя, считается недопустимым в СЗИ «Аккорд». По этой причине не допускается использование идентификаторов типа DS-1990 и DS-1991, т.к. они не имеют внутренней памяти.

Возможны четыре варианта работы с ключами пользователей:

1. «Уже записан в Идентификатор»

Ключ пользователя может быть уже записан в идентификаторе, например, при перерегистрации пользователя, который был уже зарегистрирован в составе СПО «Аккорд» на другой ПЭВМ (PC), или ключ уже был сгенерирован при регистрации пользователя.

После выбора кнопки <Далее> или нажатия клавиши <F2> выдается запрос на считывание серийного номера идентификатора. Следует присоединить идентификатор пользователя к контактному устройству считывателя информации - происходит регистрация предъявленного идентификатора.

2. «Сгенерировать»

В этом случае при нажатии кнопки <Далее> или клавиши <F2> генерируется ключ и выдается запрос на считывание идентификатора. Используйте идентификатор пользователя. Происходит регистрация идентификатора и запись в него ключа пользователя.

3. «Из файла»

Данная опция позволяет из указанного файла, который подготовлен на другом компьютере с помощью специальной утилиты, считать номер идентификатора и ключ пользователя. Этот вариант регистрации необходим для системы терминального доступа, когда уже существующие идентификаторы пользователей защищенных рабочих станций нужно зарегистрировать на терминальном сервере (подробнее см. «Руководство по установке» 37222406.26.20.40.140.091 98, п.2.5.2).

4. «Идентификатор потерян»

В этом случае после нажатия кнопки <Далее> или клавиши <F2> поле «Идентификатор» данного пользователя примет значение «Не назначен». Все остальные правила доступа останутся неизменными. Администратор таким способом может временно отключить доступ данного пользователя на время разбора конфликтной ситуации, а потом быстро восстановить его, назначив новый идентификатор.

ВНИМАНИЕ! При регистрации идентификатора «Клавиатура» можно использовать как опцию «Уже записан в идентификатор», так и опцию

«Сгенерировать»; в данном случае эти опции не влияют на конечный результат. После выбора опции и нажатия кнопки <Далее> (рисунок 24) на экран выводится окно ввода идентификатора (рисунок 25), в котором следует ввести ключевое слово, которое в дальнейшем будет использоваться в качестве идентификатора для данной клавиатуры, и нажать кнопку <OK>. **Данное поле чувствительно к регистру!**

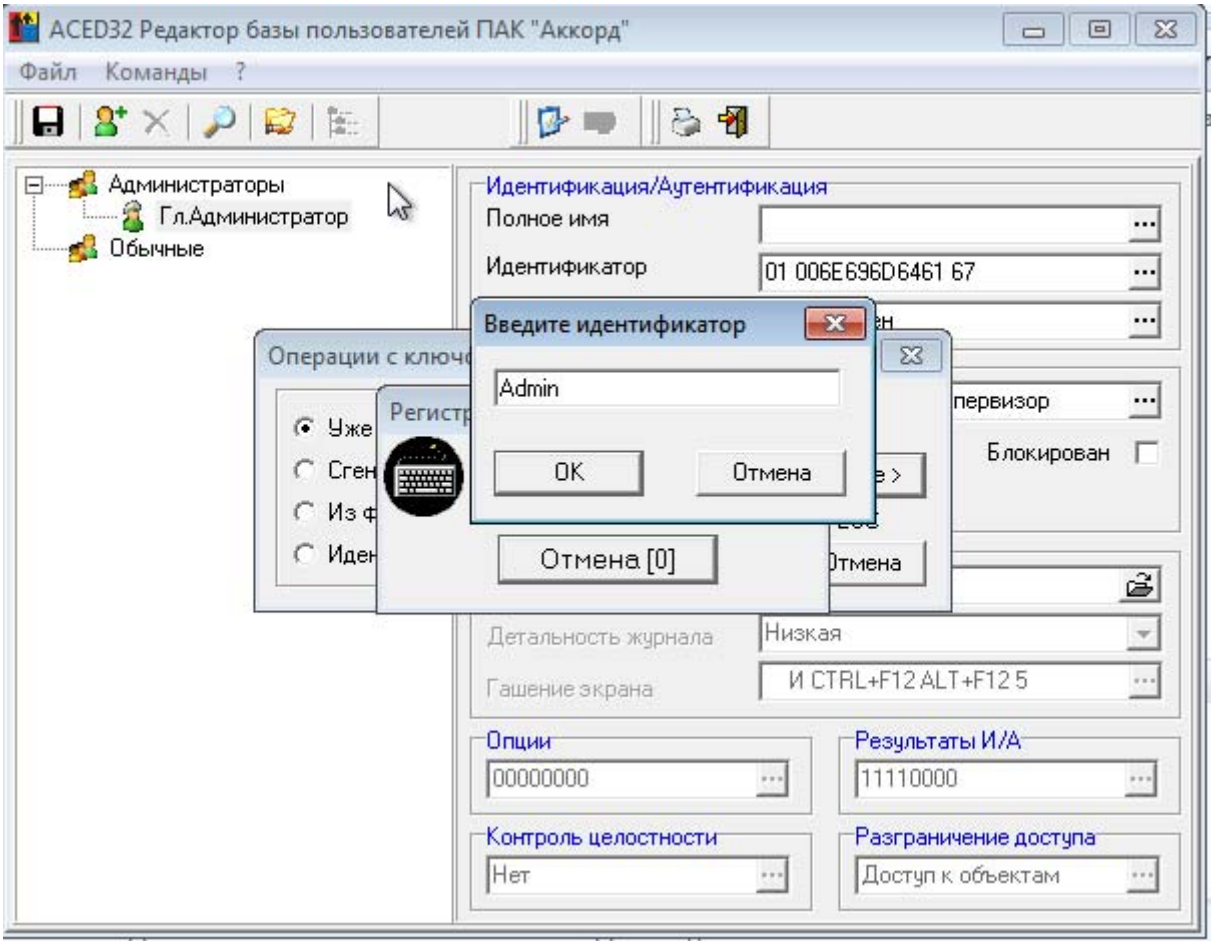

Рисунок 25 - Окно ввода ключевого слова при использовании идентификатора «Клавиатура»

В появившемся далее окне следует установить пароль. Процедура установки пароля для пользователя с идентификатором «Клавиатура» ничем не отличается от установки пароля с любым другим идентификатором.

После установки идентификатора «Клавиатура» для какого-либо пользователя или администратора каждый раз при выполнении процедур его аутентификации следует предъявлять ключевое слово, которое используется в качестве идентификатора для данной клавиатуры:

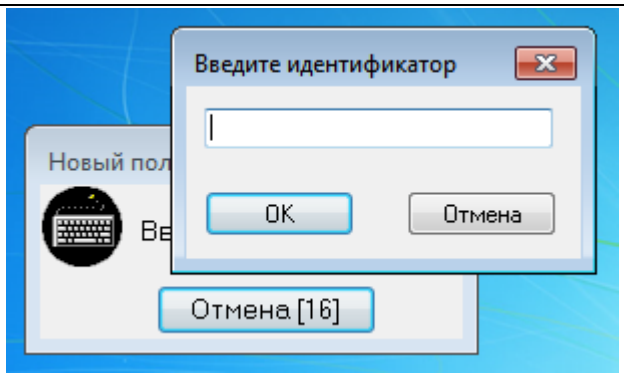

Рисунок 26 - Окно с запросом идентификатора для клавиатуры

Таблица 7 - Сообщения при регистрации идентификатора и порядок действий по ним

Сообщение	Причина	Порядок действий
«Идентификатор принадлежит пользователю: *имя_пользователя* Удалить эту учетную запись?»	Данный идентификатор уже зарегистрирован для пользователя *(указывается имя)*	Нажмите <Да>, если хотите сделать новую учетную запись вместо прежней[1]. Нажмите <Нет> и используйте другой идентификатор
«Ошибка чтения ключа!»	Ошибка чтения данных из идентификатора	Нажмите кнопку <OK>, повторите операцию. Если ошибка повторится, сгенерируйте новый ключ
«Неверный тип идентификатора»	Идентификаторы данного типа не поддерживаются СПО «Аккорд»	Нажмите кнопку <OK>. Предъявите другой идентификатор
«Ошибка создания ключевой пары!»	Ошибка записи в идентификатор	Нажмите кнопку <OK>. Повторите операцию

7.3. Установка параметров пароля

В главном окне (рисунок 2) щелкните левой кнопкой мыши в поле «Параметры пароля». Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «Параметры пароля», или клавишу <Enter>.

[1] Учетную запись пользователя «Гл.Администратор» удалить нельзя

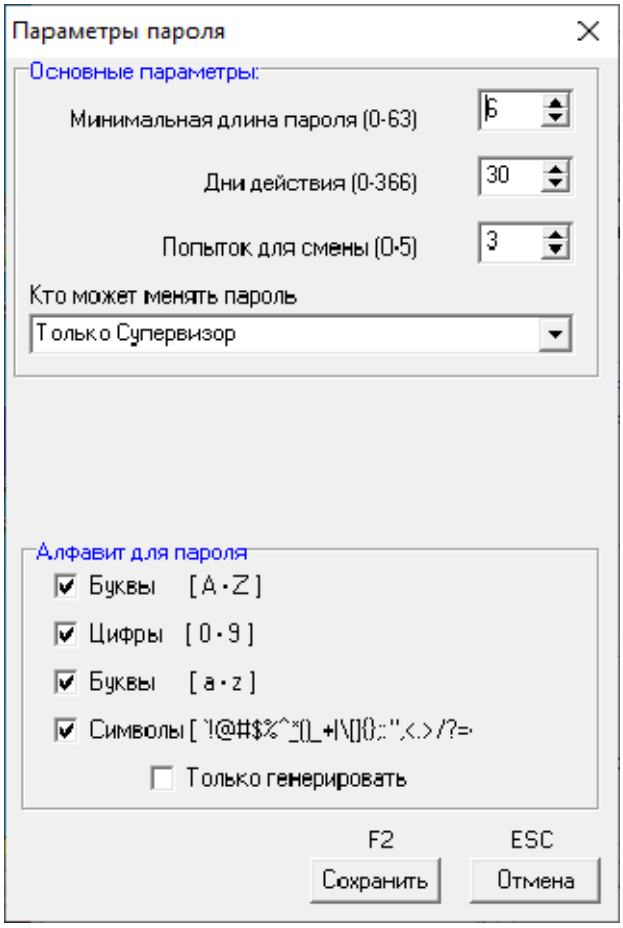

Рисунок 27 – Параметры пароля

На экран выводится окно «Параметры пароля» (рисунок 27), которое включает следующие поля:

- «Длина пароля» - минимальная длина пароля – 0 (пароль задавать не обязательно), максимальная - 63 символа.
- «Время действия» - время действия пароля до смены: от 0 (нет смены пароля) до 366 дней.
- «Попыток для смены» - количество попыток смены пароля: от 0 (бесконечное) до 5.
- «Кто может менять пароль» - установка прав на смену пароля (только администратор или администратор и пользователь).
- «Алфавит для пароля» - определяет набор символов, из которых может состоять пароль пользователя. Если установлен флаг в одном или нескольких полях, то наличие хотя бы одного символа данной последовательности обязательно при вводе пароля. При установке флага «Только генерировать» пароль будет генерироваться случайным образом из символов заданного алфавита при смене пароля пользователя.

ВНИМАНИЕ! Если пароль уже задан, то изменения его параметров вступят в силу только при смене пароля.

Для выхода из режима редактирования с сохранением измененных параметров нажмите кнопку <Сохранить> или клавишу <F2>, без сохранения – <Отмена> или <Esc>.

7.4. Задание пароля пользователя

В поле «Пароль» главного окна (рисунок 2) отображается информация о том, назначен или нет пароль выделенному пользователю. Выберите режим редактирования, нажав на кнопку справа в поле «Пароль» или клавишу <Enter>. Появится окно «Ввод пароля» (рисунок 28).

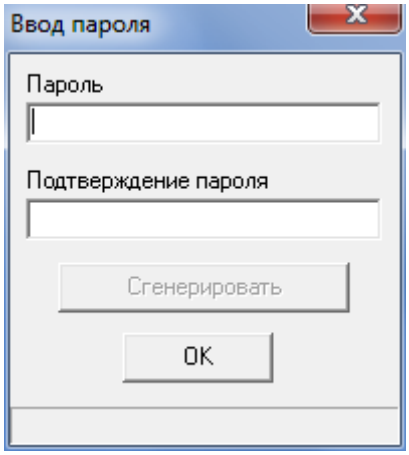

Рисунок 28 - Задание пароля пользователя

Введите пароль и повторите ввод пароля для подтверждения. Нажмите клавишу <Ok>. При использовании кнопки <Сгенерировать> полученная последовательность символов автоматически вводится в первое поле пароля, а в нижней части окна выводится значение пароля и требуется его повторный ввод для подтверждения (рисунок 29).

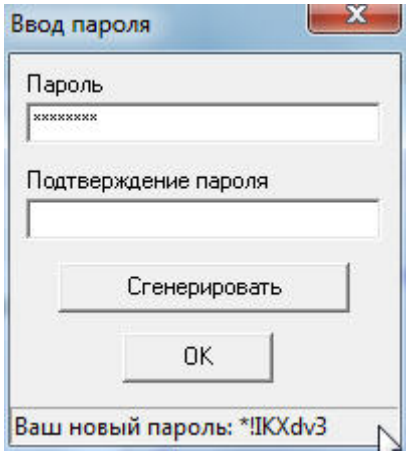

Рисунок 29 - Ввод пароля с использованием процедуры генерации

Таблица 8 - Сообщения при вводе пароля пользователя и порядок действий по ним

Сообщение	Причина	Порядок действий
«Такую комбинацию символов недопустимо	При вводе пароля контролируется нажатие	Используйте другой пароль

использовать в качестве пароля»	последовательно расположенных клавиш	
«Не следует в качестве пароля использовать имя пользователя или его часть»	В пароле использовано имя пользователя	Используйте другой пароль
«Не следует в качестве пароля использовать старый пароль или его часть»	При смене пароля в качестве нового введен опять старый пароль	Используйте другой пароль
«Длина пароля должна быть не менее (указывается число) символов»	Количество введенных символов меньше установленной минимальной длины пароля	Введите пароль из большего количества символов, или уменьшите минимальную длину в параметрах пароля
«Вы ошиблись - начинаем все сначала»	Ошибка при повторном вводе пароля	Повторите процедуру ввода пароля заново
«Использован не весь алфавит пароля»	При назначении пароля использованы не все символы алфавита пароля, установленные в окне «Параметры пароля» (рисунок 27)	Повторите процедуру ввода пароля, используя все символы алфавита пароля, установленные в окне «Параметры пароля» (рисунок 27)

7.5. Установка детальности протокола работы пользователей

Во время каждого сеанса работы пользователя ведется журнал регистрации событий, в котором отображаются действия пользователя, прикладного и системного ПО. Администратору рекомендуется в текущей работе использовать низкую детальность ведения журнала. Среднюю и высокую детальность следует использовать при изучении работы вновь используемых задач с целью определения особенностей задачи, а именно: создание новых постоянных и временных каталогов и файлов, используемых устройств и т.д. Выберите команду «Детальность журнала» в окне «Параметры пользователя» (рисунок 30). Значение поля «Детальность журнала» выбирается из списка, который раскрывается при щелчке мышью по кнопке, расположенной справа.

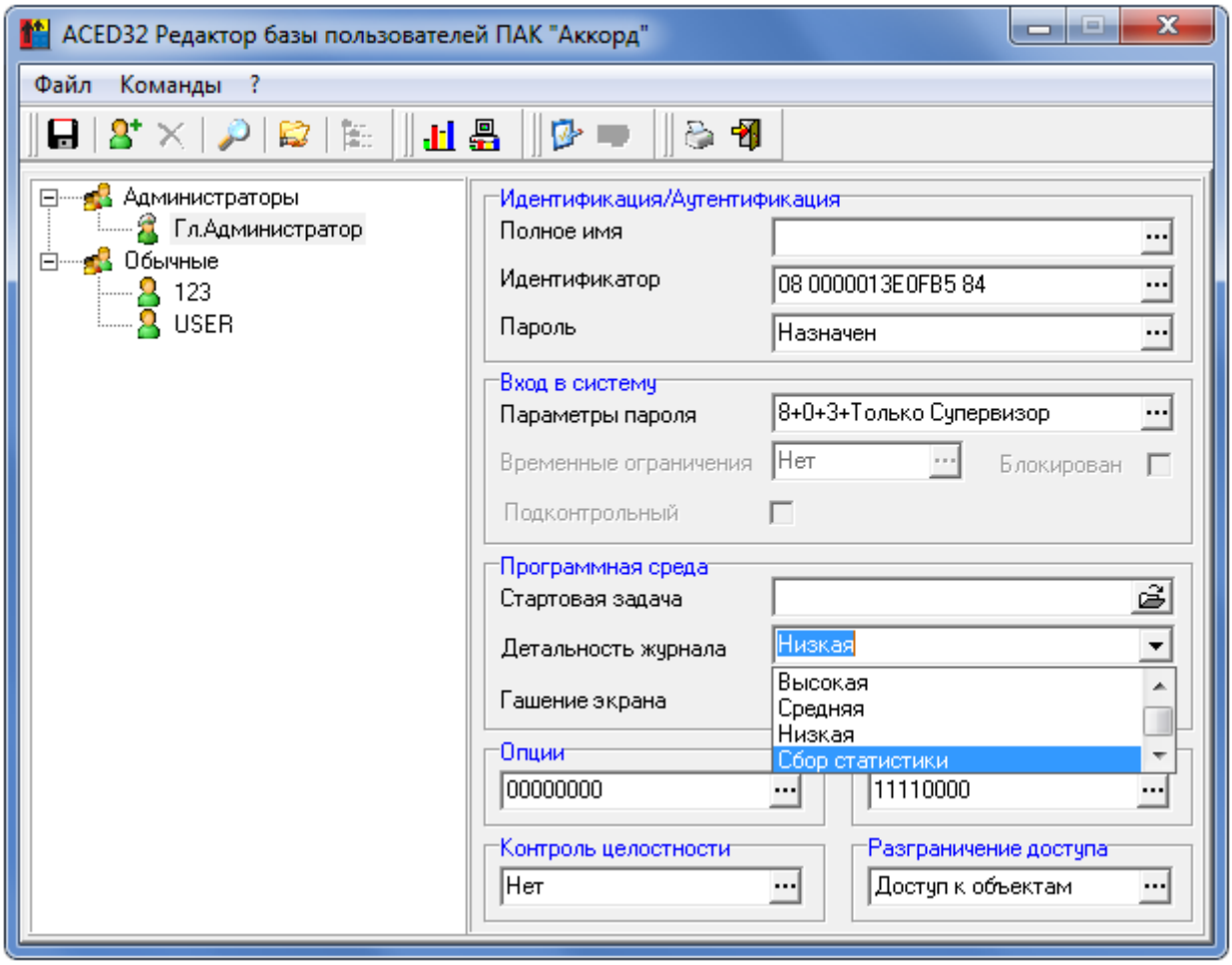

Рисунок 30 – Выбор детальности журнала

Детальность журнала:

- «Нет» - регистрация только входа/выхода из системы и событий НСД.
- «Низкая» - регистрация входа/выхода из системы, попыток несанкционированного доступа, запуска исполняемых модулей, событий СЗИ (рисунок 31).

37222406.26.20.40.140.091 97

ОК 1	26.05.2015	12:38:34:044	SYSTEM	ОК	СЗИ	0	Login
ОК 2	26.05.2015	12:38:34:497	SYSTEM	ОК	СЗИ	0	Комплекс СЗИ НСД «Аккорд-Win64», System: Windows 7 x64 [Build 7601 free, Service Pack 1], Acrun.sys: v5.0.8.40, SN=59046548
ОК 3	26.05.2015	12:38:34:559	SYSTEM	ОК	СЗИ	0	Settings: SM=No, DA=Yes, MA=Yes, CP=Yes, DNSD=No, WLN=Yes, FPP=No
ОК 4	26.05.2015	12:38:35:231	SYSTEM	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SMSS.EXE
ОК 5	26.05.2015	12:38:35:262	SMSS.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\AUTOCHK.EXE
ОК 6	26.05.2015	12:38:35:262	SMSS.EXE	ОК	СЗИ	0	Start disks checking
ОК 7	26.05.2015	12:38:35:278	AUTOCHK.EXE	ОК	СЗИ	0	Stop disks checking
ОК 8	26.05.2015	12:38:35:372	AUTOCHK.EXE	ОК	Exit	H=0	
ОК 9	26.05.2015	12:38:41:231	SMSS.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SMSS.EXE
ОК 10	26.05.2015	12:38:41:325	SMSS.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\CSRSS.EXE
ОК 11	26.05.2015	12:38:41:684	SMSS.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SMSS.EXE
ОК 12	26.05.2015	12:38:41:684	SMSS.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\CSRSS.EXE
ОК 13	26.05.2015	12:38:41:715	SMSS.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\WININIT.EXE
ОК 14	26.05.2015	12:38:41:715	SMSS.EXE	ОК	Exit	H=0	
ОК 15	26.05.2015	12:38:41:840	SMSS.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\WINLOGON.EXE
ОК 16	26.05.2015	12:38:41:840	SMSS.EXE	ОК	Exit	H=0	
ОК 17	26.05.2015	12:38:42:106	WININIT.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SERVICES.EXE
ОК 18	26.05.2015	12:38:42:215	WININIT.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\LSASS.EXE
ОК 19	26.05.2015	12:38:42:450	WININIT.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\LSM.EXE
ОК 20	26.05.2015	12:38:43:059	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 21	26.05.2015	12:38:43:169	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 22	26.05.2015	12:38:43:184	WINLOGON.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\LOGONUI.EXE
ОК 23	26.05.2015	12:38:43:200	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 24	26.05.2015	12:38:43:325	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 25	26.05.2015	12:38:43:340	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 26	26.05.2015	12:38:43:340	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 27	26.05.2015	12:38:44:012	SVCHOST.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\AUDIODG.EXE
ОК 28	26.05.2015	12:38:44:512	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\IGFXCUISERVICE.EXE
ОК 29	26.05.2015	12:38:45:294	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 30	26.05.2015	12:38:46:247	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SPOOLSV.EXE
ОК 31	26.05.2015	12:38:46:262	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 32	26.05.2015	12:38:46:278	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 33	26.05.2015	12:38:46:419	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\ACRUNNT.EXE
! 34	26.05.2015	12:38:46:981	LOGONUI.EXE	НСД	ChangeDir	H=0	C:\ACCORD.X64\
ОК 35	26.05.2015	12:38:46:997	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\SVCHOST.EXE
ОК 36	26.05.2015	12:38:47:544	SVCHOST.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\DLLHOST.EXE
ОК 37	26.05.2015	12:38:50:294	SVCHOST.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\WUDFHOST.EXE
ОК 38	26.05.2015	12:38:50:465	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\TASKHOST.EXE
ОК 39	26.05.2015	12:38:50:794	WINLOGON.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\USERINIT.EXE
ОК 40	26.05.2015	12:38:50:794	SERVICES.EXE	ОК	Exec	H=0	C:\WINDOWS\MICROSOFT.NET\FRAMEWORK64\V3.0\WPF\PRESENTATIONFONTCACHE.EXE
ОК 41	26.05.2015	12:38:50:809	SVCHOST.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\DWM.EXE
ОК 42	26.05.2015	12:38:51:137	USERINIT.EXE	ОК	Exec	H=0	C:\WINDOWS\EXPLORER.EXE
ОК 43	26.05.2015	12:38:53:137	EXPLORER.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\ACRUNNT.EXE
! 44	26.05.2015	12:38:53:762	EXPLORER.EXE	НСД	ChangeDir	H=0	K:\$RECYCLE.BIN\
! 45	26.05.2015	12:38:53:762	EXPLORER.EXE	НСД	OpenFile	Read	K:\$RECYCLE.BIN\S-1-5-21-805032283-4188568234-3326661453-1012\DESKTOP.INI
! 46	26.05.2015	12:38:53:825	EXPLORER.EXE	НСД	OpenFile	Read	K:\$RECYCLE.BIN\S-1-5-21-805032283-4188568234-3326661453-1012\DESKTOP.INI
! 47	26.05.2015	12:38:53:825	EXPLORER.EXE	НСД	ChangeDir	H=0	K:\$RECYCLE.BIN\S-1-5-21-805032283-4188568234-3326661453-1012\
ОК 48	26.05.2015	12:38:54:372	IGFXCUISERVICE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\CMD.EXE
ОК 49	26.05.2015	12:38:54:387	CSRSS.EXE	ОК	Exec	H=0	C:\WINDOWS\SYSTEM32\CONHOST.EXE

Рисунок 31 – Журнал событий с низкой детальностью

- «Средняя» - то же, что при низкой детальности, плюс операции доступа к файлам и каталогам (рисунок 32).

OK 1	26.05.2015	12:44:25:079	SYSTEM	OK	СЗИ	0	Login
OK 2	26.05.2015	12:44:25:532	SYSTEM	OK	СЗИ	0	Комплекс СЗИ НСД «Аккорд-Win64», System: Windows 7 x64 [Build 7601 free, Service Pack 1], Acrun.sys: v5.0.8.40, SN=59046548
OK 3	26.05.2015	12:44:25:595	SYSTEM	OK	СЗИ	0	Settings: SM=No, DA=Yes, MA=Yes, CP=Yes, DNSD=No, WLN=Yes, FPP=No
OK 4	26.05.2015	12:44:25:954	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 5	26.05.2015	12:44:25:954	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\
OK 6	26.05.2015	12:44:25:954	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 7	26.05.2015	12:44:26:251	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\
OK 8	26.05.2015	12:44:26:251	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\
OK 9	26.05.2015	12:44:26:314	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 10	26.05.2015	12:44:26:345	SYSTEM	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\SMSS.EXE
OK 11	26.05.2015	12:44:26:501	SMSS.EXE	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\
OK 12	26.05.2015	12:44:26:501	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 13	26.05.2015	12:44:26:517	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 14	26.05.2015	12:44:26:517	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 15	26.05.2015	12:44:26:532	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 16	26.05.2015	12:44:26:548	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 17	26.05.2015	12:44:26:548	SMSS.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\AUTOCHK.EXE
OK 18	26.05.2015	12:44:26:548	SMSS.EXE	OK	СЗИ	0	Start disks checking
OK 19	26.05.2015	12:44:26:610	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 20	26.05.2015	12:44:26:735	AUTOCHK.EXE	OK	СЗИ	0	Stop disks checking
OK 21	26.05.2015	12:44:26:814	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 22	26.05.2015	12:44:26:814	AUTOCHK.EXE	OK	Exit	H=0	
OK 23	26.05.2015	12:44:26:814	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 24	26.05.2015	12:44:26:876	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\CONFIG\
OK 25	26.05.2015	12:44:26:876	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\
OK 26	26.05.2015	12:44:26:876	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\CONFIG\
OK 27	26.05.2015	12:44:26:876	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\CONFIG\
OK 28	26.05.2015	12:44:26:876	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\CONFIG\
OK 29	26.05.2015	12:44:26:876	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\CONFIG\
OK 30	26.05.2015	12:44:26:876	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\CONFIG\
OK 31	26.05.2015	12:44:26:923	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
OK 32	26.05.2015	12:44:27:454	SYSTEM	OK	ChangeDir	H=0	D:\
OK 33	26.05.2015	12:44:27:454	SYSTEM	OK	ChangeDir	H=0	D:\
OK 34	26.05.2015	12:44:27:454	SYSTEM	OK	ChangeDir	H=0	D:\
OK 35	26.05.2015	12:44:27:454	SMSS.EXE	OK	ChangeDir	H=0	D:\BOOT\
OK 36	26.05.2015	12:44:27:454	SMSS.EXE	OK	ChangeDir	H=0	D:\BOOT\
OK 37	26.05.2015	12:44:27:470	SMSS.EXE	OK	CreateFile	H=0	C:\HIBERFIL.SYS
OK 38	26.05.2015	12:44:27:532	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\CONFIG\REGBACK\
OK 39	26.05.2015	12:44:27:579	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\LOGFILES\WMI\RTBACKUP\
OK 40	26.05.2015	12:44:27:579	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\LOGFILES\WMI\RTBACKUP\
OK 41	26.05.2015	12:44:27:579	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\LOGFILES\WMI\RTBACKUP\
OK 42	26.05.2015	12:44:27:579	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\LOGFILES\WMI\RTBACKUP\
OK 43	26.05.2015	12:44:27:610	SMSS.EXE	OK	ChangeDir	H=0	C:\
OK 44	26.05.2015	12:44:27:610	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\LOGFILES\WMI\
OK 45	26.05.2015	12:44:27:610	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\LOGFILES\WMI\
OK 46	26.05.2015	12:44:27:610	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\LOGFILES\WMI\
OK 47	26.05.2015	12:44:27:610	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\CONFIG\
OK 48	26.05.2015	12:44:27:610	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\LOGFILES\WMI\

Рисунок 32 - Журнал событий со средней детальностью

- «Высокая» - то же, что и при средней детальности, плюс все файловые операции, включая параметры команд (рисунок 33).

ОК 1	26.05.2015	12:48:48:398	SYSTEM	OK	СЗИ	0	Login
ОК 2	26.05.2015	12:48:48:804	SYSTEM	OK	СЗИ	0	Комплекс СЗИ НСД «Аккорд-Win64», System: Windows 7 x64 [Build 7601 free, Service Pack 1], Acrun.sys: v5.0.8.40, SN=59046548
ОК 3	26.05.2015	12:48:48:882	SYSTEM	OK	СЗИ	0	Settings: SM=No, DA=Yes, MA=Yes, CP=Yes, DNSD=No, WLN=Yes, FPP=No
ОК 4	26.05.2015	12:48:49:226	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 5	26.05.2015	12:48:49:226	SYSTEM	OK	OpenFile	ReadWrite	C:\WINDOWS\BOOTSTAT.DAT
ОК 6	26.05.2015	12:48:49:226	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\
ОК 7	26.05.2015	12:48:49:226	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 8	26.05.2015	12:48:49:492	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 9	26.05.2015	12:48:49:507	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\
ОК 10	26.05.2015	12:48:49:507	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\
ОК 11	26.05.2015	12:48:49:507	SYSTEM	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\SMSS.EXE
ОК 12	26.05.2015	12:48:49:507	SMSS.EXE	OK	OpenFile	ReadWrite	C:\WINDOWS\BOOTSTAT.DAT
ОК 13	26.05.2015	12:48:49:523	SMSS.EXE	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\
ОК 14	26.05.2015	12:48:49:538	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 15	26.05.2015	12:48:49:538	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 16	26.05.2015	12:48:49:538	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 17	26.05.2015	12:48:49:538	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 18	26.05.2015	12:48:49:538	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 19	26.05.2015	12:48:49:554	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 20	26.05.2015	12:48:49:570	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 21	26.05.2015	12:48:49:570	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 22	26.05.2015	12:48:49:585	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 23	26.05.2015	12:48:49:585	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 24	26.05.2015	12:48:49:585	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 25	26.05.2015	12:48:49:585	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 26	26.05.2015	12:48:49:601	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 27	26.05.2015	12:48:49:601	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 28	26.05.2015	12:48:49:601	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 29	26.05.2015	12:48:49:601	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 30	26.05.2015	12:48:49:601	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 31	26.05.2015	12:48:49:617	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 32	26.05.2015	12:48:49:617	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 33	26.05.2015	12:48:49:617	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 34	26.05.2015	12:48:49:617	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 35	26.05.2015	12:48:49:617	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 36	26.05.2015	12:48:49:632	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 37	26.05.2015	12:48:49:632	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 38	26.05.2015	12:48:49:648	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 39	26.05.2015	12:48:49:648	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 40	26.05.2015	12:48:49:663	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 41	26.05.2015	12:48:49:663	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 42	26.05.2015	12:48:49:663	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 43	26.05.2015	12:48:49:679	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 44	26.05.2015	12:48:49:788	SMSS.EXE	OK	Exec	H=0	C:\WINDOWS\SYSTEM32\AUTOCHK.EXE
ОК 45	26.05.2015	12:48:49:788	SMSS.EXE	OK	СЗИ	0	Start disks checking
ОК 46	26.05.2015	12:48:49:913	SYSTEM	OK	ChangeDir	H=0	C:\WINDOWS\SYSTEM32\DRIVERS\
ОК 47	26.05.2015	12:48:49:913	AUTOCHK.EXE	OK	СЗИ	0	Stop disks checking
ОК 48	26.05.2015	12:48:50:007	AUTOCHK.EXE	OK	Exit	H=0	
ОК 49	26.05.2015	12:48:50:007	SMSS.EXE	OK	OpenFile	ReadWrite	C:\WINDOWS\BOOTSTAT.DAT

Рисунок 33 - Журнал событий с высокой детальностью

• «Сбор статистики» - то же, что и при высокой детальности журнала, кроме того, для пользователя не действуют установленные правила разграничения доступа[2]. С таким режимом детальности, если пользователь запускает СВТ, то до появления окна приветствия ОС на экране появляется предупреждение «WARNING!!! SAFE MODE ACTIVE» (предупреждение появляется на несколько секунд, поэтому его можно легко пропустить). Если в разделе «Результаты И/А» (рисунок 2) не установлены первые пять флагов, то после входа в систему (после предъявления идентификатора) пользователю выдается сообщение. Продолжить работу он сможет только при нажатии кнопки <ОК>, однако кнопка становится доступной по истечении 20 секунд с момента появления сообщения[3]. Такое же сообщение (с таймаутом в 20 секунд) появляется, если завершить сессию пользователя и запустить сессию пользователя с установленным значением «Сбор статистики».

7.6. Установка режима блокировки экрана

Блокировка экрана используется для временного отключения экрана и доступа к клавиатуре и мыши по истечении установленного интервала

---

[2] «Сбор статистики» – параметр, похожий на «Мягкий режим», но только для конкретного пользователя

[3] Это сделано с целью напомнить о снятии режима детальности «Сбор статистики» для пользователя

«неактивности» пользователя либо при нажатии комбинации горячих клавиш «Гашение» (по умолчанию установлена комбинация <Ctrl+F12>). Вернуться в рабочий режим можно только при помощи данных для идентификации пользователя, с которыми был начат данный сеанс работы. Для редактирования параметров гашения экрана щелкните мышью на кнопке, расположенной справа в поле «Гашение экрана» (рисунок 2), или нажмите клавишу <Enter>. Выводится окно «Параметры Screen Saver» (рисунок 34).

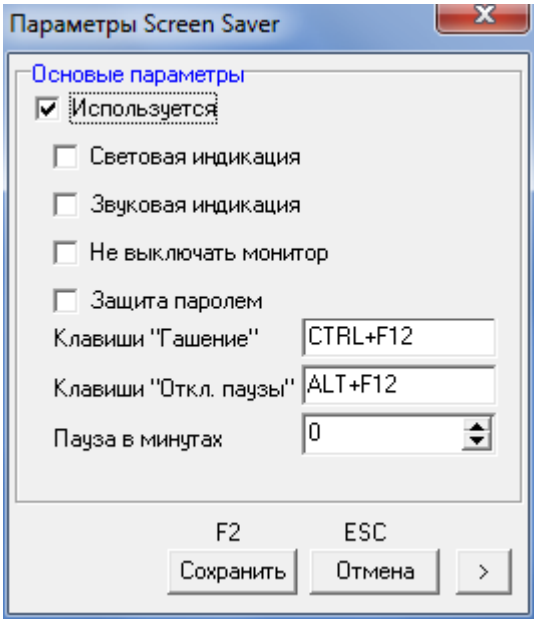

Рисунок 34 - Параметры гашения экрана

ВНИМАНИЕ! В терминальном режиме, чтобы включить режим блокировки экрана, необходимо использовать комбинацию клавиш <Win><L>. После включения хранителя экрана клавиатура и мышь блокируются, на экране появляется сообщение «Предъявите идентификатор».

С помощью мыши задайте необходимые параметры гашения. Если необходимо включить режим гашения экрана, установите параметр «Используется» (этот параметр имеет наиболее высокий приоритет). Затем, если необходимо, установите дополнительные параметры:

«Световая индикация» - мигание индикаторов <Num Lock>, <Caps Lock> и <Scroll Lock> во время работы экранной заставки[4];

«Звуковая индикация» - звуковые сигналы в режиме гашения;

«Не выключать монитор» - режим, при котором заставка экрана не включается. При этом если в поле «Пауза в минутах» установить значение «0», то блокировки мыши и клавиатуры не произойдет, если же в поле «Пауза в минутах» установить значение, отличное от нуля, то блокировка клавиатуры и мыши произойдет по истечении указанного времени. Такой режим может быть полезен на рабочих станциях, которые осуществляют мониторинг сети, почты и т.д.

[4] Данная опция может быть корректно использована только на PS/2-клавиатурах

Интервал времени, по истечении которого выполняется переход в режим гашения экрана, если клавиатура и мышь не используются, устанавливается в строке «Пауза в минутах» (по умолчанию – 5 минут).

Можно установить комбинацию клавиш принудительного включения Screen Saver – в поле «Клавиши «Гашение» (по умолчанию <Ctrl+F12>). Предусмотрена установка комбинации «Клавиши «Откл. паузы» (по умолчанию <Alt+F12>), при нажатии которой отключается режим срабатывания хранителя экрана по времени, и для включения используется только клавиатура или мышь. Для выхода с сохранением установленных параметров нажмите кнопку <Сохранить> или клавишу <F2>, выход без сохранения – <Отмена> или <Esc>.

Для установки другой комбинации клавиш «Гашение» или «Откл. паузы» необходимо перейти в поле «Гашение» или «Откл. паузы» соответственно и одновременно нажать клавиши Shift, Ctrl или Alt и одну из клавиш F1=F12.

Примечание: В режиме терминальной сессии при нажатии кнопки <Гашение экрана> появляется предупреждение о том, что в терминальной версии возможна только блокировка компьютера (рисунок 35):

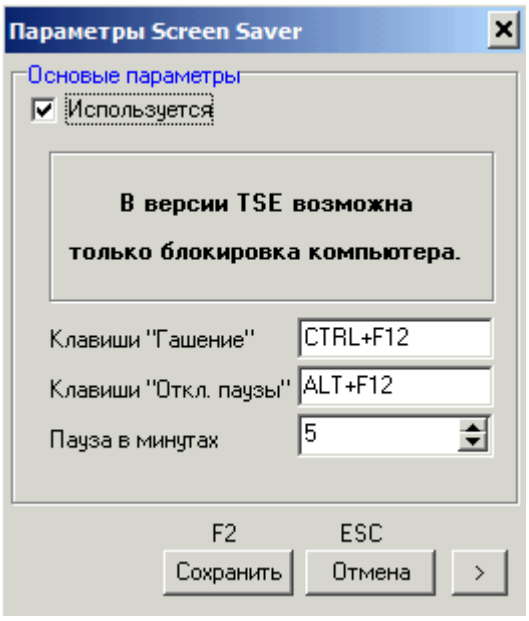

Рисунок 35 – Параметры гашения экрана в режиме терминальной сессии

В нижнем правом углу окна настроек Screen Saver находится кнопка со стрелкой. При нажатии на эту кнопку открывается поле дополнительных параметров блокировки (рисунок 36). Эти параметры определяют специальные режимы блокировки (выключение) при использовании идентификаторов, подключаемых к USB-портам компьютера. В стандартных режимах используется только в момент процедуры идентификации, но настройки дополнительных параметров позволяют задавать поведение компьютера при извлечении идентификатора из USB-порта.

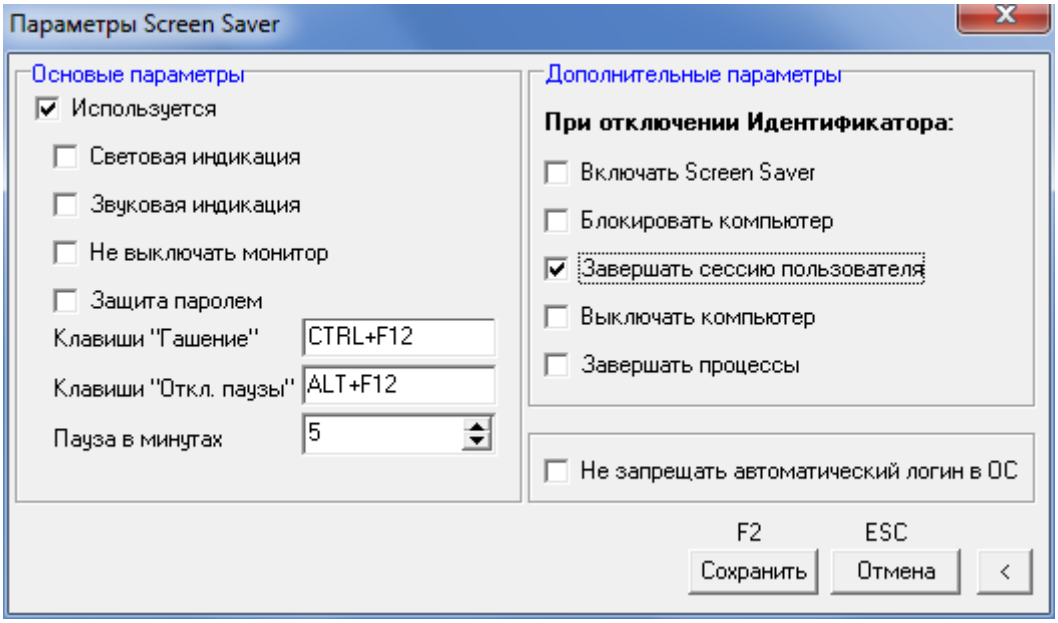

Рисунок 36 - Дополнительные параметры блокировки компьютера[5]

Примечание: В режиме терминальной сессии при нажатии кнопки со стрелкой в нижнем правом углу окна «Параметры Screen Saver» на экране появляется окно с предупреждением о том, что в терминальной версии возможна только блокировка компьютера (рисунок 37):

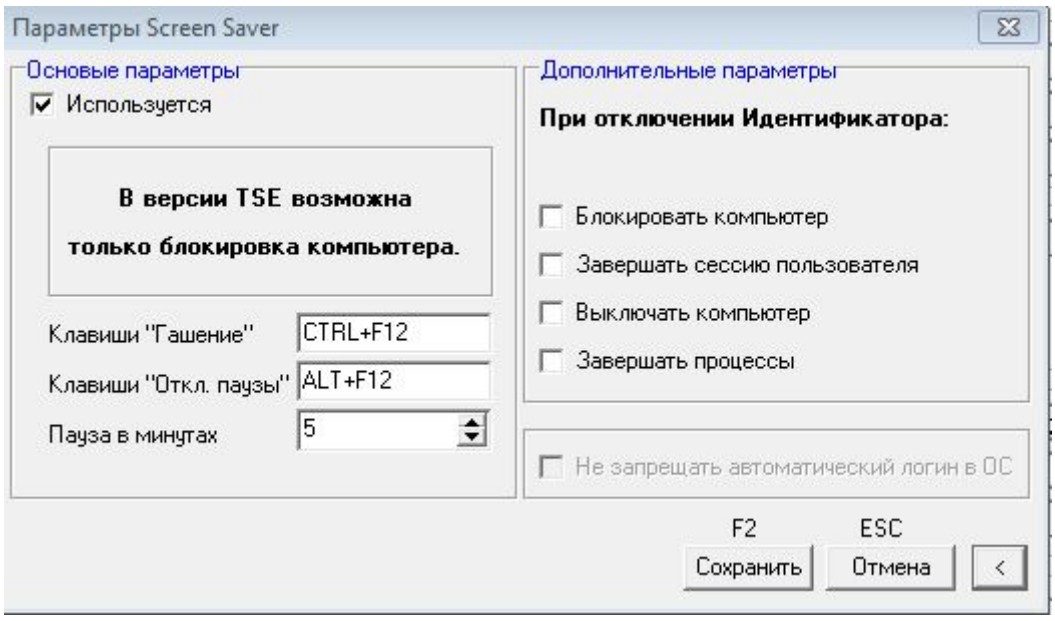

Рисунок 37 - Дополнительные параметры блокировки компьютера в режиме терминальной сессии

В окне, показанном на рисунке 37, можно выбрать дополнительные параметры блокировки. Настройка дополнительных параметров позволяет

[5)] В случае необходимости одновременного использования параметра Screen Saver «Блокировать компьютер» и флага «Автоматический логин» (см. документ «Руководство по установке» 37222406.26.20.40.140.091 98) рекомендуется установить флаг «Не запрещать автоматический логин в ОС» (см.рисунок 36)

задавать поведение компьютера при извлечении устройства ШИПКА из USB-порта в режиме терминальной сессии.

ВНИМАНИЕ! Дополнительные параметры «хранителя экрана» будут действовать только после выбора необходимых опций (рисунок 36). В терминальной сессии хранитель экрана не включается при нажатии клавиш <Ctrl><F12>, а если необходимо временно заблокировать доступ к компьютеру, то нужно использовать комбинацию клавиш <Win><L>.

В СВТ, оснащенном ОС Windows Server 2008/2012, в режиме терминальной сессии не запускается хранитель экрана (даже если на СВТ не установлен Аккорд). Поэтому в СВТ, оснащенном ОС Windows Server 2008/2012, в режиме терминальной сессии происходит блокировка сессии пользователя, если компьютерная мышь и клавиатура неактивны заданный промежуток времени.

Предусмотрены четыре основных варианта реакции на извлечение идентификатора: от включения экранной заставки до выключения компьютера. Для одного пользователя можно выбрать только один основной параметр. В комбинации с основным параметром можно использовать дополнительный «Завершать процессы». Список процессов, которые нужно завершить при извлечении идентификатора, прописывается в файле <UserName>.kit. Это обыкновенный текстовый файл в Windows-кодировке, каждая строка которого описывает процесс:

```
c:\windows\system32\Wordpad.exe
notepad.exe
c:\program files\far\far.exe
```

Можно прописывать как полный путь, так и просто имя.

Таблица 9 - Сообщения, выдаваемые программой при установке режима гашения экрана, и порядок действий по ним

Сообщение	Причина	Порядок действий
«Такая комбинация клавиш уже назначена»	Выбранная Вами комбинация клавиш уже назначена	Назначьте другую комбинацию клавиш

При снятом флаге «Автоматический логин в ОС» для выхода из режима блокировки экрана (при условии, что такой режим используется) необходимо предъявить идентификатор пользователя, который включил компьютер. Кроме того, если компьютер блокирован нажатием клавиш C-A-D «блокировать», то для выхода из режима блокировки потребуется предъявить идентификатор (если для этого пользователя используется хранитель экрана), затем ввести пароль пользователя, включающего компьютер.

7.7. Установка временных ограничений для сеанса работы пользователя

В списке пользователей с помощью мыши или клавиатуры выделите пользователя или группу пользователей.

В поле «Временные ограничения» окна «Параметры пользователя» (рисунок 2) отображается информация о наличии временных ограничений у активного (выделенного) пользователя. Возможны следующие режимы ограничений:

T - ограничение по времени;

D - ограничение по датам (при установке в программе настройки комплекса «Аккорд» (AcSetup.exe) флага «Проверка времени действия учетной записи пользователя»);

L – ограничение, если период времени с даты последнего входа больше, чем заданный период неактивности (период задается в опциях программы настройки комплекса «Аккорд»).

Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «Временные ограничения», или клавишу <Enter>. Появляется окно «Временные ограничения для (*указывается имя_пользователя)*» (рисунок 38).

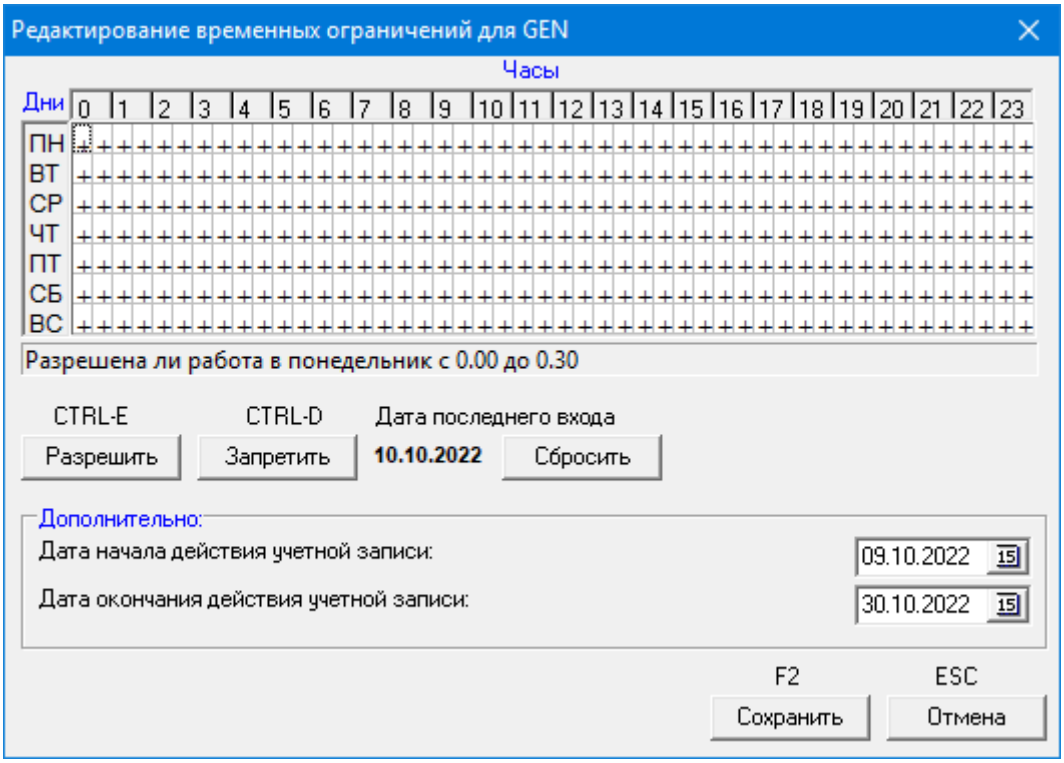

Рисунок 38 - Окно редактирования временных ограничений

В этом окне отображена таблица со строками, соответствующими дням недели, и столбцами, соответствующими временным промежуткам (часам).

Ячейки таблицы заполнены знаками «+» и «-»:

«+» - работа возможна.

«-» - работа невозможна.

При помощи мыши, удерживая левую кнопку, можно выделить область редактирования. Для того чтобы разрешить пользователю работу в выделенной области, необходимо нажать кнопку <Разрешить> (<Ctrl+E>). Для запрета работы в выделенной области необходимо нажать кнопку <Запретить> (<Ctrl+D>). Двойное нажатие мыши (<Пробел>) на ячейку меняет ее значение

на противоположное. Перемещение по таблице возможно как при помощи мыши, так и при помощи клавиатуры.

В окне редактирования также отображается дата последнего входа пользователя, которую можно обнулить с помощью кнопки <Сбросить>. Если период времени, прошедший с этой даты, больше, чем заданный период неактивности, дата будет красного цвета, а в главном окне программы в строке «Временные ограничения» будет отображаться режим L.

В поле «Дополнительно» (появляется в режиме D) можно настроить следующие параметры:

«Дата начала действия учетной записи» – определяет дату, с наступлением которой работа для пользователя разрешается на текущем компьютере;

«Дата окончания действия учетной записи» – определяет дату, с наступлением которой работа для пользователя запрещается на текущем компьютере.

Для выхода из режима редактирования с сохранением нажмите кнопку <Сохранить> или клавишу <F2>, без сохранения – <Отмена> или <Esc>.

7.8. Блокировка пользователя

В главном окне программы (рисунок 2) правее поля «Временные ограничения» находится флаг «Блокирован». При установке этого флага все параметры пользователя сохраняются в базе данных, но вход в систему и работа данного пользователя будут запрещены. Данный флаг можно использовать для временной блокировки пользователя. После того как администратор снимет блокировку, работа пользователя восстановится со всеми установленными настройками. Для этого необходимо просто перезагрузить компьютер.

7.9. Установка стартовой задачи пользователя

В главном окне программы (рисунок 2) нажмите левой кнопкой мыши на раскрывающийся список в строке «Стартовая задача», и на экран выведется окно выбора исполняемого файла (задачи). Выбранная задача запускается для данного пользователя после старта операционной системы в качестве программной оболочки (shell) вместо explorer.exe. При этом пользователь может работать только в загруженной программной среде (рабочий стол Windows, кнопка <Пуск> и панель задач на экран не выводятся). В случае, когда пользователю в рамках его функциональных обязанностей необходимо запускать на выполнение несколько различных задач, то в качестве задачи для запуска можно указать программу AcTskMng.EXE, входящую в состав СПО «Аккорд» (рисунок 39).

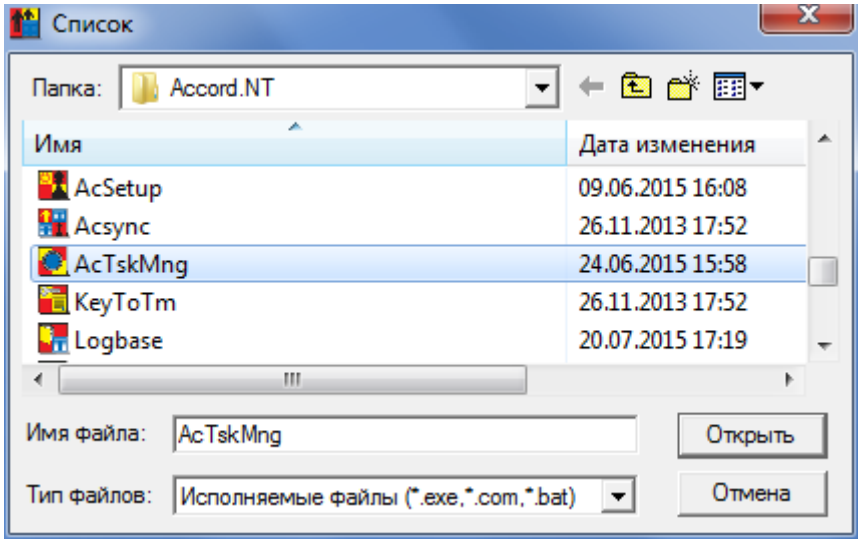

Рисунок 39 - Выбор стартовой задачи – менеджера приложений СПО «Аккорд»

Для успешной работы этой программы необходимо создать текстовый файл – список задач, разрешенных для запуска данному пользователю. Имя этого файла должно совпадать с именем пользователя, расширение файла должно быть .ACT.

ВНИМАНИЕ! При назначении для пользователя в ACED32.EXE в качестве задачи запуск программы AcTskMng.EXE можно использовать следующие варианты имен файлов типа .ACT:

1)совпадающий с именем пользователя;

2)совпадающий с именем группы;

3)Default.ACT.

Приоритет применения: применяется .ACT-файл пользователя, в случае его отсутствия используется .ACT-файл группы. В случае отсутствия обоих вышеуказанных типов файлов используется файл Default.ACT.

Простой список задач в файле .ACT должен выглядеть следующим образом:

```
[Task1]
DisplayName=Администрирование САБС
ImagePath=P:\bin\adm_sec.exe
WaitEndTask=Yes
[Task2]
DisplayName=Настройки САБС
ImagePath=P:\bin\sabs_set.exe
WaitEndTask=Yes
[Task3]
DisplayName=Модификации САБС
ImagePath=P:\bin\sabs_mod.exe
WaitEndTask=Yes
[Task4]
```

```
DisplayName=Пусковое решение САБС
ImagePath=P:\bin\sabs_pusk.exe
WaitEndTask=Yes
[Task5]
DisplayName=FAR
ImagePath=C:\Program Files (x86)\FAR3\far.exe
WaitEndTask=Yes
```

DisplayName — определяет название приложения, отображаемое в окне Менеджера задач.

ImagePath — указывает путь к исполняемому файлу приложения.

WaitEndTask — определяет последовательность выполнения задач, включенных в список. Значение ключа «Yes» означает, что запуск следующей задачи из списка будет возможен только после завершения уже запущенного приложения. Значение ключа «No» разрешает одновременный запуск нескольких приложений. Если для определенного приложения этот параметр не задан в act-файле, то на него будет распространятся значение соответствующего параметра из файла Actskmng.ini.

В вышеприведенном примере простого файла .ACT при старте монитора разграничения доступа запустится оболочка AcTskMng со списком программ, доступных для выполнения данным пользователем (рисунок 40). До выбора конкретной задачи кнопка <Запуск> в окне Менеджера задач остается неактивной.

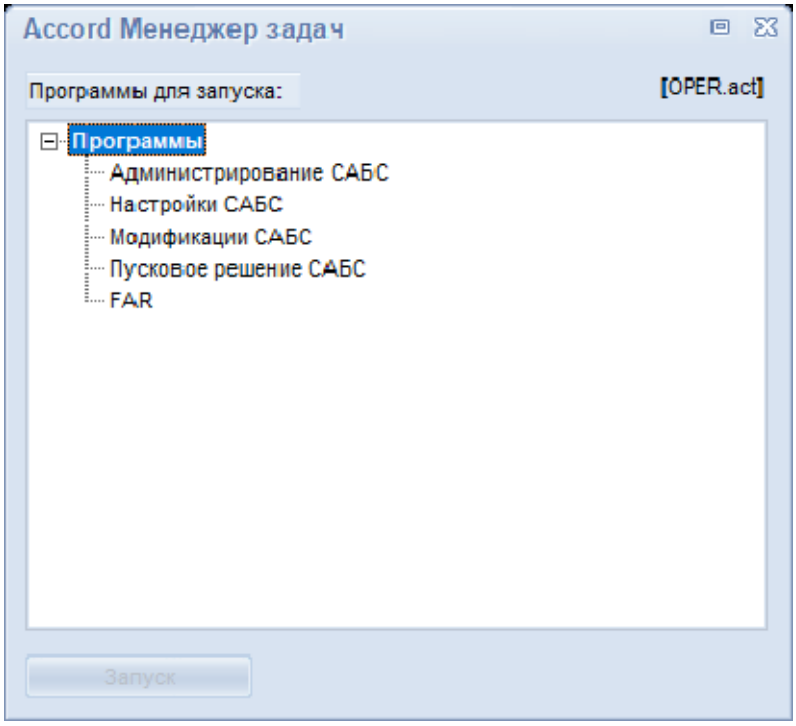

Рисунок 40 - Окно Менеджера задач при запуске файла без групп задач

Задачи пользователя можно объединять в группы по функциональному признаку. Если в файле используются русские наименования группы или задачи, то они должны вводиться в windows-кодировке.

Файл .ACT с группами задач должен выглядеть следующим образом:

```
[Group1]
GroupName=Работа с САБС
Expand=Yes
[Task1.1]
DisplayName=Администрирование САБС
ImagePath=P:\bin\adm_sec.exe
WaitEndTask=Yes
[Task1.2]
DisplayName=Настройки САБС
ImagePath=P:\bin\sabs_set.exe
WaitEndTask=Yes
[Task1.3]
DisplayName=Модификации САБС
ImagePath=P:\bin\sabs_mod.exe
WaitEndTask=Yes
[Task1.4]
DisplayName=Пусковое решение САБС
ImagePath=P:\bin\sabs_pusk.exe
WaitEndTask=Yes
[Group2]
GroupName=File managers
Expand=Yes
[Task2.1]
DisplayName=FAR
ImagePath=C:\Program Files (x86)\FAR3\far.exe
WaitEndTask=Yes
```

Expand - параметр группы, определяющий режим отображения содержимого группы в Менеджере задач. Значение «Yes» означает, что содержимое группы будет показано. Параметр обладает большим приоритетом, чем подобный параметр в файле запуска Actskmng.ini.

В данном примере окно Менеджера задач будет выглядеть, как показано на рисунке 41.

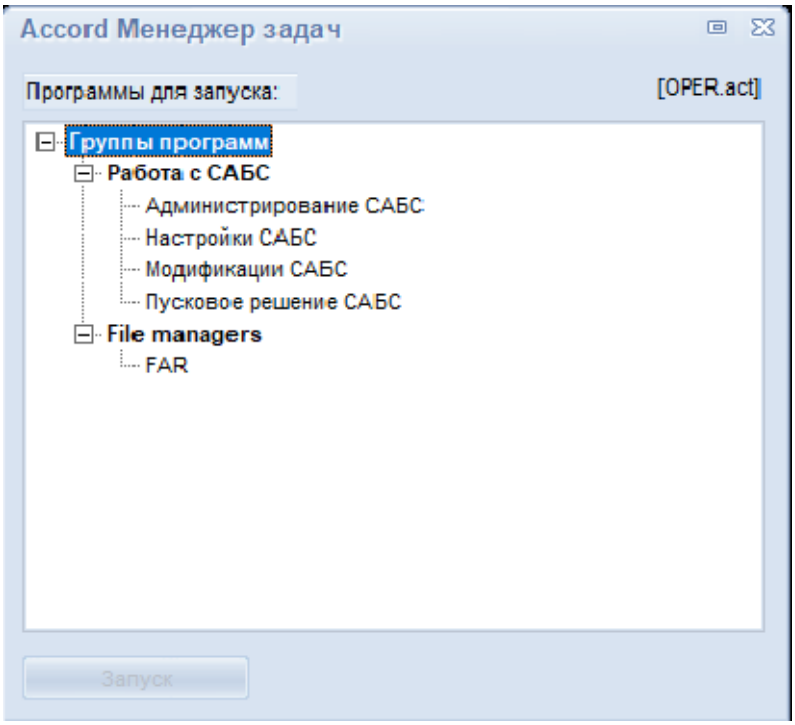

Рисунок 41 - Окно Менеджера задач при запуске файла с группами задач

И еще один пример файла .ACT, задачи в котором распределены не только по группам, но и по подгруппам:

```
[Group1]
GroupName=File managers
Expand=Yes
[Task1.1]
DisplayName=Notepad1
ImagePath=C:\windows\system32\notepad.exe
WaitEndTask=Yes
[Group1.1]
GroupName=File managers1
Expand=Yes
[Task1.1.1]
DisplayName=FAR Manager1
ImagePath=C:\PROGRA~1\Far.x64\Far.exe
[Task1.2]
DisplayName=Notepad1
ImagePath=C:\windows\system32\notepad.exe
WaitEndTask=Yes
[Task1.1.2]
DisplayName=Volcov Commander1
ImagePath=c:\vc\vc.com
[Task1.4]
```

```
DisplayName=Notepad4
ImagePath=C:\windows\system32\notepad.exe
WaitEndTask=Yes
[Task1.3]
DisplayName=Notepad3
ImagePath=C:\windows\system32\notepad.exe
WaitEndTask=Yes
[Group1.2]
GroupName=File managers2
Expand=Yes
[Task1.2.1]
DisplayName=FAR Manager2
ImagePath=C:\PROGRA~1\Far.x64\Far.exe
[Task1.2.2]
DisplayName=Volcov Commander2
ImagePath=c:\vc\vc.com
[Group2]
GroupName=Язык и региональные стандарты
Expand=Yes
[Task2.1]
DisplayName=Язык
ImagePath=rundll32.exe
Parameters=shell32.dll,Control_RunDLL intl.cpl
WorkDir=c:\windows\system32\
WaitEndTask=Yes
[Task2.2]
DisplayName=Язык Link
ImagePath=c:\link.lnk
WorkDir=c:\
WaitEndTask=No
```

WorkDir – параметр предоставляет возможность задать рабочий каталог для программы, если он отличается от месторасположения исполняемого файла.

Parameters — позволяет при необходимости задать дополнительные параметры запуска исполняемого файла.

Окно Менеджера задач в случае запуска этого файла примет вид, показанный на рисунке 42.

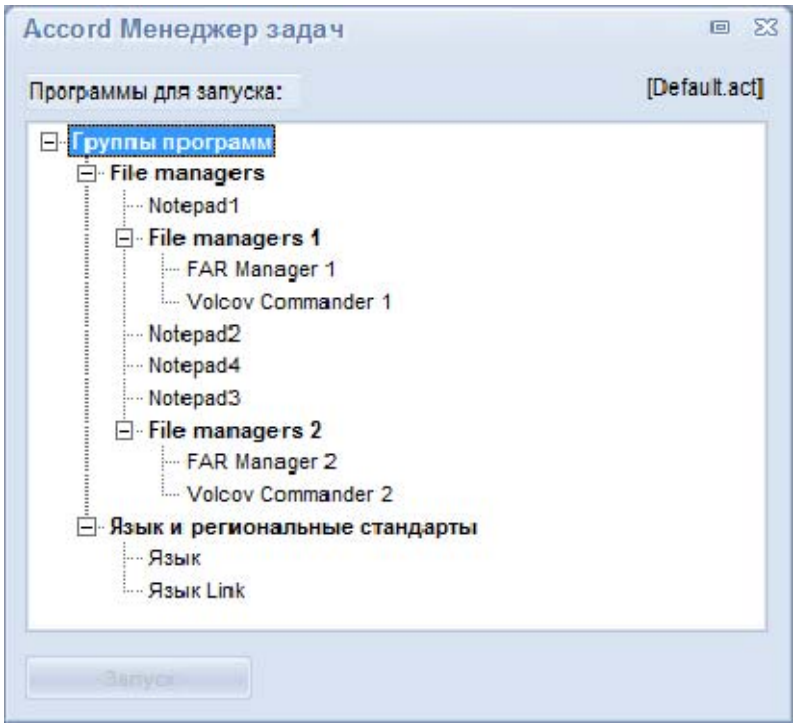

Рисунок 42 - Окно Менеджера задач при запуске файла с группами и подгруппами

Секция [RUN_BEFORE] определяет группу задач, которые запускаются перед загрузкой оболочки AcTskMng и остаются резидентными в памяти:

```
[RUN_BEFORE]
GroupName=Предварительный запуск
[RunTask1]
DisplayName=FAR manager
ImagePath=c:\progra~1\Far\Far.exe
[RunTask2]
DisplayName=Notepad
ImagePath=c:\windows\system32\notepad.exe
```

При нажатии кнопки <Пуск> появляется меню (рисунок 43).

ВНИМАНИЕ! Для корректного отображения символов кириллицы в трее оболочки AcTskMng необходимо выполнить (однократный) вход пользователя в ОС после активации ПАК «Аккорд».

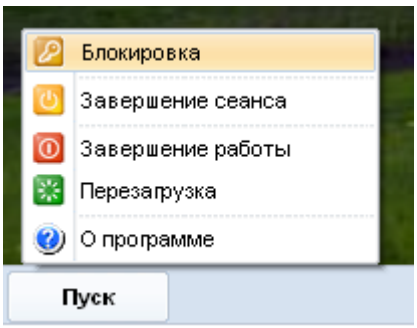

Рисунок 43 – Меню менеджера задач СПО «Аккорд»

В меню пользователю доступны кнопки завершения работы, перезагрузки и завершения сеанса, информация о программе, а также кнопка включения блокировки экрана (Screen Saver). Если пользователь не входит в группу администраторов, то для него также блокируется возможность запуска диспетчера задач Windows (по комбинации клавиш Ctrl-Alt-Del).

При выборе пункта меню «О программе» (рисунок 43) на экране появляется информация о программе, а также информация о сессии пользователя (версия драйвера разграничении доступа, дата и время начала сессии пользователя, имя пользователя, дата и время завершения сессии пользователя[6]).

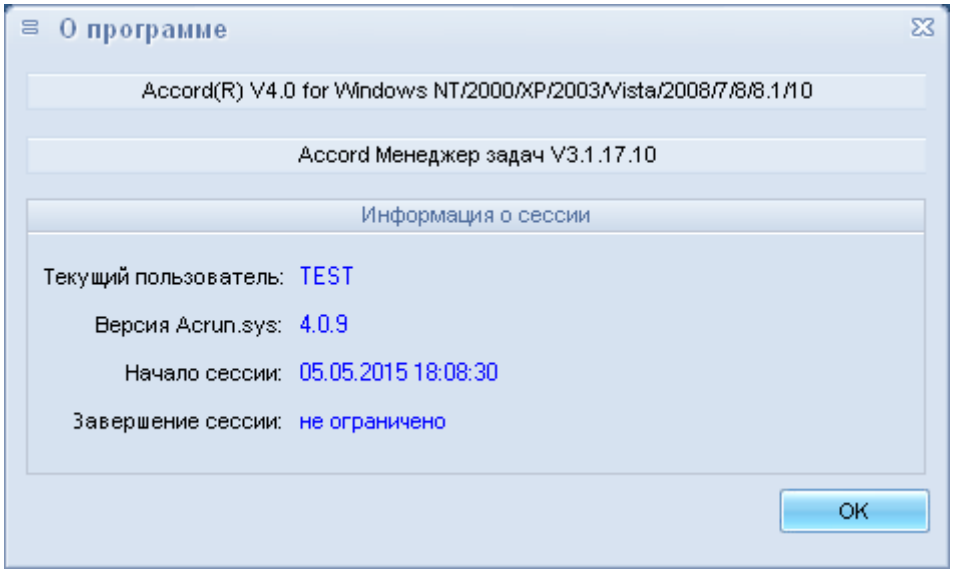

Рисунок 44 – Информация о программе

В качестве исполняемых задач можно задавать файлы типа .lnk. Кроме этого, можно управлять режимом запуска программы AcTskMng.exe. В папке Accord.NT (Accord.x64 – для 64-битных ОС) находится файл Actskmng.ini с набором ключей.

Ключ ProceedRegistryKeyRun=Yes разрешает загрузку резидентных программ, запускаемых при старте ОС, прописанных в ключе HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run (значки этих программ располагаются на панели задач Windows в правом углу). Программы, прописанные в ключе системного реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, автоматически запускаются для всех пользователей СВТ.

По умолчанию этот ключ установлен в значение Yes, т.е. запуск таких программ разрешен. Если администратор желает запретить запуск всех приложений кроме AcTskMng.exe, то значение ключа нужно установить в No.

---

[6] Время завершения сессии пользователя отображается в том случае, если для пользователя установлены временные ограничения для сеанса работы

ВНИМАНИЕ! Если при установке стартовой задачи в опциях пользователя (см. п.6.12) был выбран пункт «проверять доступ к реестру», то в список правил разграничения доступа данного пользователя нужно добавить объект \HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft \ Windows NT\ CurrentVersion\ Winlogon\ Shell и разрешить к нему полный доступ.

Ключ ProceedRegistryKeyRunCU=Yes разрешает загрузку резидентных программ, запускаемых при старте ОС, прописанных в ключе HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run. Программы, прописанные в ключе системного реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, автоматически запускаются только для текущего пользователя СВТ.

Ключ CorrectLanguageLayout=Yes запрещает запуск процесса CTFMON.EXE.

Ключ CorrectLanguageLayoutTS=Yes запрещает запуск процесса CTFMON.EXE в режиме терминальной сессии.

Ключ WaitEndTask=Yes определяет последовательность выполнения задач, включенных в список. Значение ключа «Yes» означает, что запуск следующей задачи из списка будет возможен только после завершения уже запущенного приложения. Значение ключа «No» разрешает запуск одновременно нескольких приложений. Переключаться между запущенными приложениями можно стандартной комбинацией клавиш <Alt-Tab>.

Ключ SortTask=0 определяет расположение задач в иерархическом списке после подразделов группы (рисунок 45). Такое же расположение устанавливается и при отсутствии ключа SortTask.

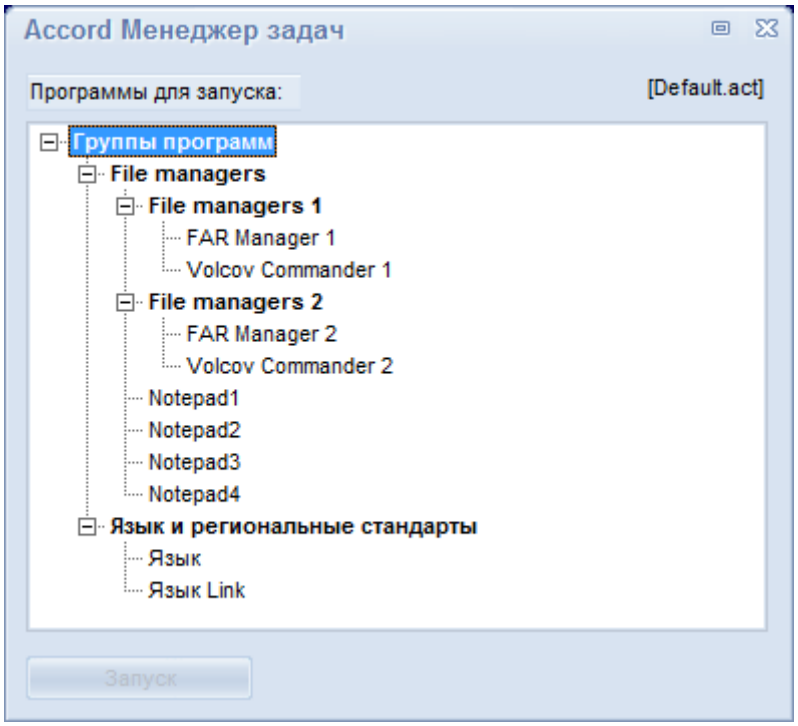

Рисунок 45 – Расположение задач в Менеджере задач при SortTask=0

Ключ SortTask=1 определяет расположение задач в иерархическом списке перед подразделами группы (рисунок 46).

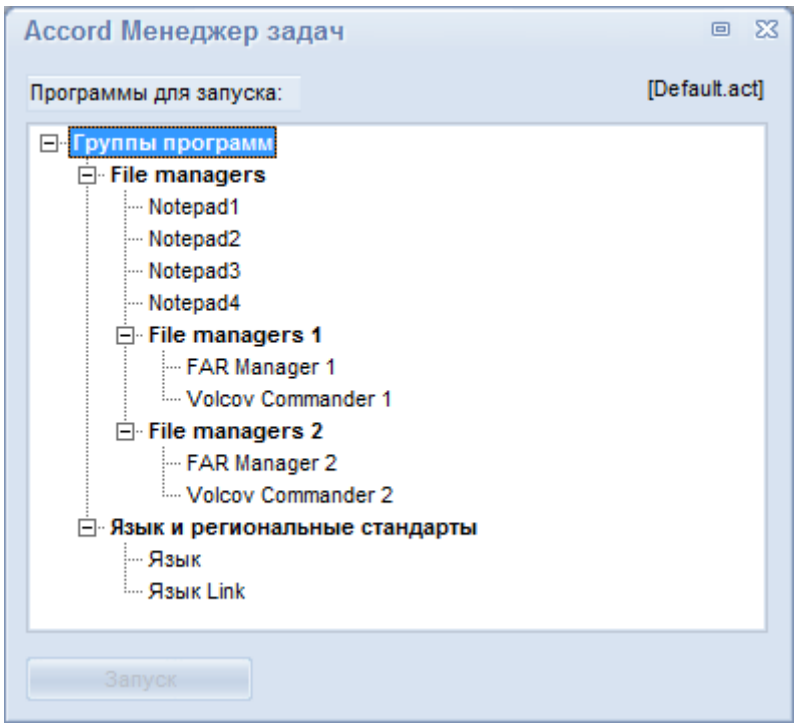

Рисунок 46 - Расположение задач в Менеджере задач при SortTask=1

Ключ SortTask=2 определяет расположение задач в Менеджере задач без сортировки, подобно их описанию в файле .ACT (рисунок 40).

Ключ Expand=Yes при старте приложения AcTskMng разворачивает весь иерархический список задач.

Ключ ShowTrayIcons=Yes позволяет выводить на панель задач в правом нижнем углу окна AcTskMng.exe иконки из системного трея (панели задач Windows).

Ключ FontSize определяет размер шрифта в окне программ. Значение можно установить от 8 до 20.

Примечания:

1)для корректной работы раскладки клавиатуры рекомендуется установить следующие значения параметров: ProceedRegistryKeyRunCU=No, CorrectLanguageLayout=Yes (в режиме терминальной сессии: ProceedRegistryKeyRunCU=No, CorrectLanguageLayoutTS=Yes);

2)для корректного отображения иконок в системном трее рекомендуется установить следующие значения параметров: ProceedRegistryKeyRun=Yes, ProceedRegistryKeyRunCU=No, ShowTrayIcons= Yes.

Если AcTskMng.exe запускается в терминальной сессии пользователя, то кнопки <Завершение работы> и <Перезагрузка> будут заблокированы.

ВНИМАНИЕ! Создание списка выполняемых задач в AcTskMng еще не означает реализацию изолированной программной среды, т.к. запущенное приложение может иметь в своем составе средства запуска других программ. Создание изолированной программной среды на основе «белого» списка исполняемых модулей в СПО «Аккорд» можно реализовать с помощью мандатного и/или дискреционного механизма доступа с контролем процессов и динамического контроля целостности файлов из этого списка (см. 7.12.3), как используя, так и не используя утилиту Actskmng.exe.

7.10. Контроль целостности файлов

СПО «Аккорд-Win64 K» позволяет контролировать целостность файлов по индивидуальному списку, созданному администратором для каждого пользователя (или группы). Предусмотрены два режима контроля: ***«статический»*** - это контроль целостности любых файлов, расположенных на жестком диске, в момент начала сеанса пользователя;

«динамический» - это контроль исполняемых модулей перед их загрузкой в оперативную память СВТ.

7.10.1. «Статический» контроль целостности файлов

Для создания списка контролируемых файлов нажмите кнопку, расположенную справа в поле «Контроль целостности», в главном окне (рисунок 2). На экран выводится окно «Контроль целостности объектов для *(указывается имя_пользователя)*», показанное на рисунке 47.

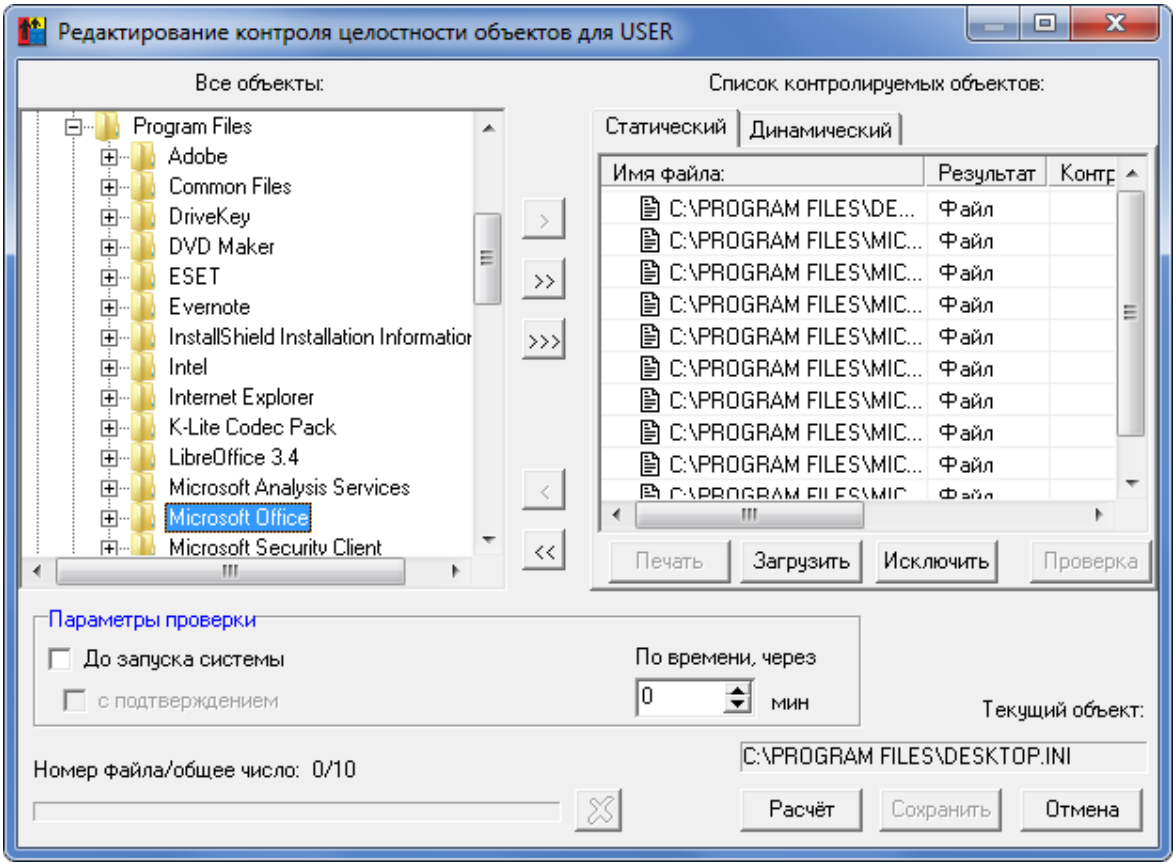

Рисунок 47 - Окно контроля целостности объектов

На первом этапе необходимо сформировать список файлов. Возможен выбор отдельного файла или всех файлов из выбранного каталога. В левой половине окна «Все объекты» выберите нужный файл с помощью мыши (левая кнопка). Выбранный файл переместится в правую часть окна в «Список контролируемых объектов» при двойном щелчке мыши или при нажатии на кнопку «>».

Для перемещения всех файлов каталога в «Список контролируемых объектов» в разделе «Все объекты» выберите нужный каталог с помощью мыши (левая кнопка). При нажатии на кнопку «>>» выводится окно (рисунок 48), предлагающее ввести необходимый фильтр. Стрелка в правой части строки позволяет задавать маску по расширению файлов (*.* означает выбор всех файлов). При нажатии кнопки «ОК» или клавиши <Enter> все файлы выбранного каталога, удовлетворяющие заданному фильтру, переместятся в «Список контролируемых объектов». Клавиша <Esc> отменяет добавление фильтра.

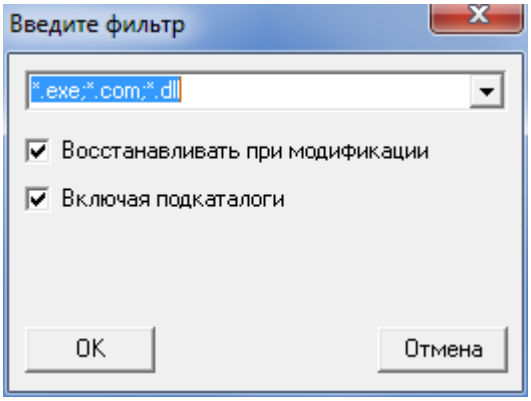

Рисунок 48 - Задание фильтра для выбора контролируемых файлов

Флаг «Включая подкаталоги» распространяет действие фильтра на все уровни вложенности подкаталогов в выбранном каталоге.

Флаг «Восстанавливать при модификации» включает дополнительную функцию создания копии контролируемого файла. При обнаружении изменений в контролируемых файлах выполняется восстановление исходного состояния файла из резервной копии.

Еще один специфический объект контроля – это контейнер. Для формирования контейнера нужно выделить объект (в качестве объекта может выступать корневой каталог логического раздела жесткого диска или отдельный каталог) и нажать на кнопку «>>>». После этого выводится окно выбора параметров контейнера контролируемых объектов (рисунок 49).

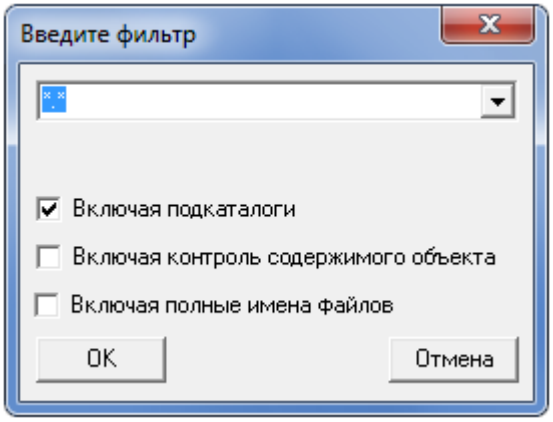

Рисунок 49 - Задание фильтра для контейнера объектов

Флаг «Включая подкаталоги» действует следующим образом. Контрольная сумма содержимого самих файлов не вычисляется. В списке контролируемых объектов сохраняется одна запись с результирующей контрольной суммой. Такая процедура контроля может успешно использоваться, если установлен режим автоматического обновления компонентов ПО из доверенного источника, а состав(список) файлов не меняется.

Флаг «Включая контроль содержимого объекта» добавляет следующий уровень контроля, т.е. рассчитывается контрольная сумма содержимого каталога и содержимого файлов (одна на весь контейнер).

Флаг «Включая полные имена файлов» автоматически включает флаг «Включая контроль содержимого объекта». В контейнере хранится полный список файлов с контрольной суммой для каждого объекта. Нарушение целостности выявится при изменении состава контролируемых объектов, т.е. при удалении существующих или добавлении новых файлов или папок, а также при изменении КС самих объектов.

Пользоваться возможностями контроля целостности контейнера объектов следует по принципу «разумной достаточности». Можно, например, установить полный контроль на папку Windows, но следует понимать, что время расчета хэш-функции нескольких тысяч файлов будет значительным, да к тому же пользователь не сможет нормально работать на таком «защищенном» компьютере. Операционная система при работе создает некоторое количество временных файлов, и при каждом новом сеансе будет выявлено нарушение целостности.

В то же время контроль контейнера объектов может быть эффективным, когда нужно отследить целостность и неизменность набора данных, необходимых для выполнения технологического процесса обработки информации. Процедура контроля будет выявлять не только изменение контрольных сумм отдельных файлов, но также изменение состава ПО, т.е. появление новых файлов, которые изначально в состав пакета не входили.

Очистить «Список контролируемых объектов» можно, нажав на кнопку «<<». Удалить файл из «Списка контролируемых объектов» можно посредством нажатия кнопки «<» после его выделения в списке или двойным щелчком мыши на выделенном файле.

На втором этапе осуществляется установка режимов контроля целостности.

Выбор режимов осуществляется установкой флагов в нижней панели окна. Возможны следующие варианты:

- *«До запуска системы»* - контроль целостности до запуска операционной системы.
- *«С подтверждением»* - запрос подтверждения контроля целостности до запуска ОС (пользователь может отказаться от выполнения процедуры контроля).
- *«При выходе из системы»* - обновление КС после завершения сеанса работы пользователя (при выходе из системы).
- *«С подтверждением»* - запрос подтверждения обновления КС после завершения сеанса работы.
- «По времени, через» - контроль целостности в рамках сеанса пользователя по истечении заданного интервала времени. Если установлено значение 0, то процедура контроля целостности по времени не выполняется. Если установлено отличное от нуля значение интервала времени, то процедура контроля целостности осуществляется по его истечении.

ВАЖНО! При установке файлов на статический контроль целостности необходимо убедиться в наличии установленного флага «Перезагрузка при ошибках» в программе «Настройки комплекса «Аккорд» (подробнее см. «Руководство по установке»). В противном случае при возникновении ошибок контроля целостности драйвер разграничения доступа AcRun.sys не будет запущен!

На третьем этапе производится расчет КС выбранных файлов при нажатии кнопки <Расчет>. В процессе расчета запрашивается идентификатор данного пользователя. В алгоритме расчета используется ключ пользователя, записанный в идентификатор при регистрации пользователя. Тем самым исключается возможность подделки результирующей КС при несанкционированном изменении файлов. При попытке рассчитать контрольную сумму без установки режимов выводится сообщение об ошибке (рисунок 50).

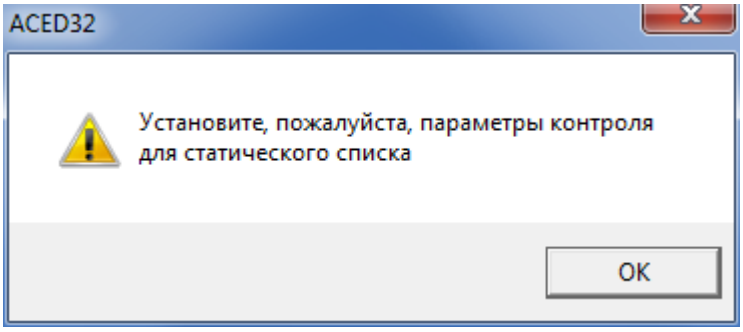

Рисунок 50 - Предупреждение о необходимости установки режимов контроля

Выход из процедуры контроля с сохранением результатов расчета - нажатие кнопки <Сохранить> или клавиши <F2>, без сохранения – кнопки <Отмена> или клавиши <Esc>.

7.10.2. «Динамический» контроль целостности файлов

Эта операция выполняется при **каждом** запуске процесса (исполняемого модуля). Для создания списка контролируемых процессов нажмите кнопку, расположенную справа в поле «Контроль целостности», в главном окне (рисунок 2). На экран выводится окно «Контроль целостности файлов для (указывается имя_пользователя)».

Щелкните мышью на закладке «Динамический» - откроется список файлов для динамического контроля, показанный на рисунке 51.

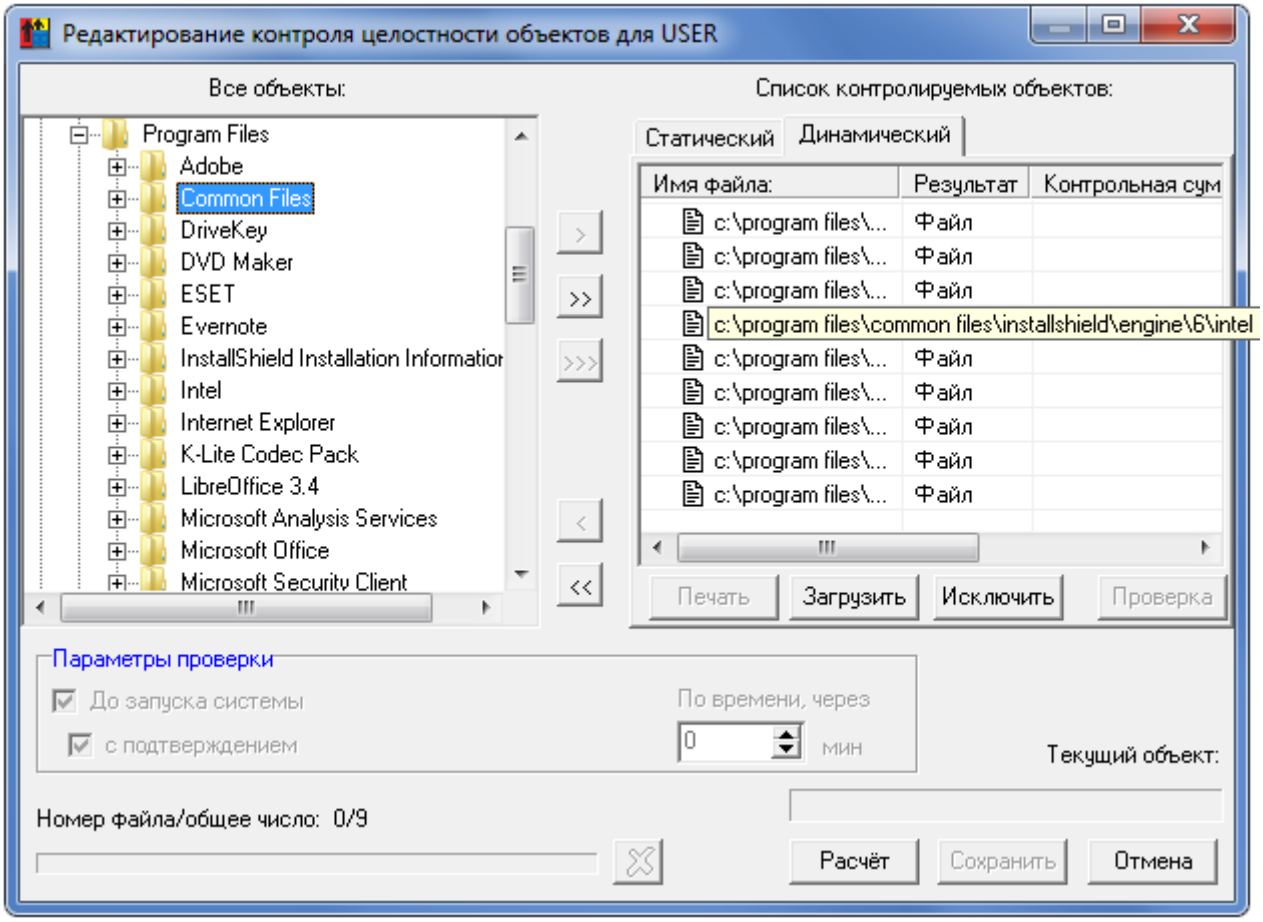

Рисунок 51 - Список файлов для динамического контроля

С этим списком можно работать так же, как и со «статическим», но не требуется задания параметров проверки.

Список контролируемых объектов можно задавать как для отдельного пользователя, так и для группы. В этом случае контроль будет выполняться для любого пользователя из группы.

Как для статического, так и для динамического режима контроля возможна загрузка списка контролируемых файлов из специального файла. Файл можно создать на основе анализа журналов событий с помощью

программы AcProc.EXE (см. документ «Подсистема регистрации программы работы с журналами регистрации» 37222406.26.20.40.140.091 99). Список файлов для контроля имеет расширение HSH. Для выполнения этой операции щелкните мышкой по кнопке <Загрузить> - откроется окно выбора файла (рисунок 52).

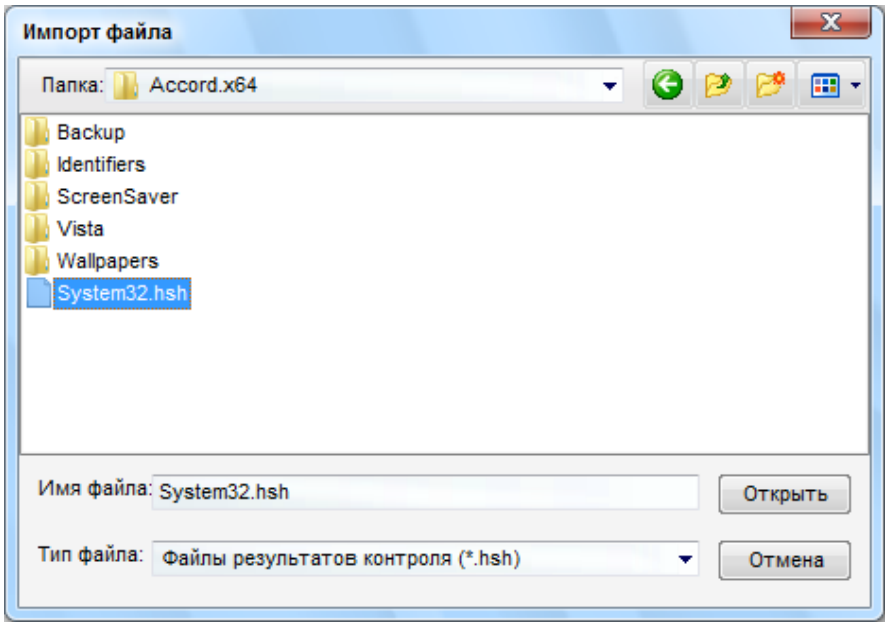

Рисунок 52 - Выбор файла со списком контролируемых объектов

Отметьте необходимый файл и нажмите кнопку <Открыть>. Файлы будут добавлены в соответствующий список контроля (рисунок 53).

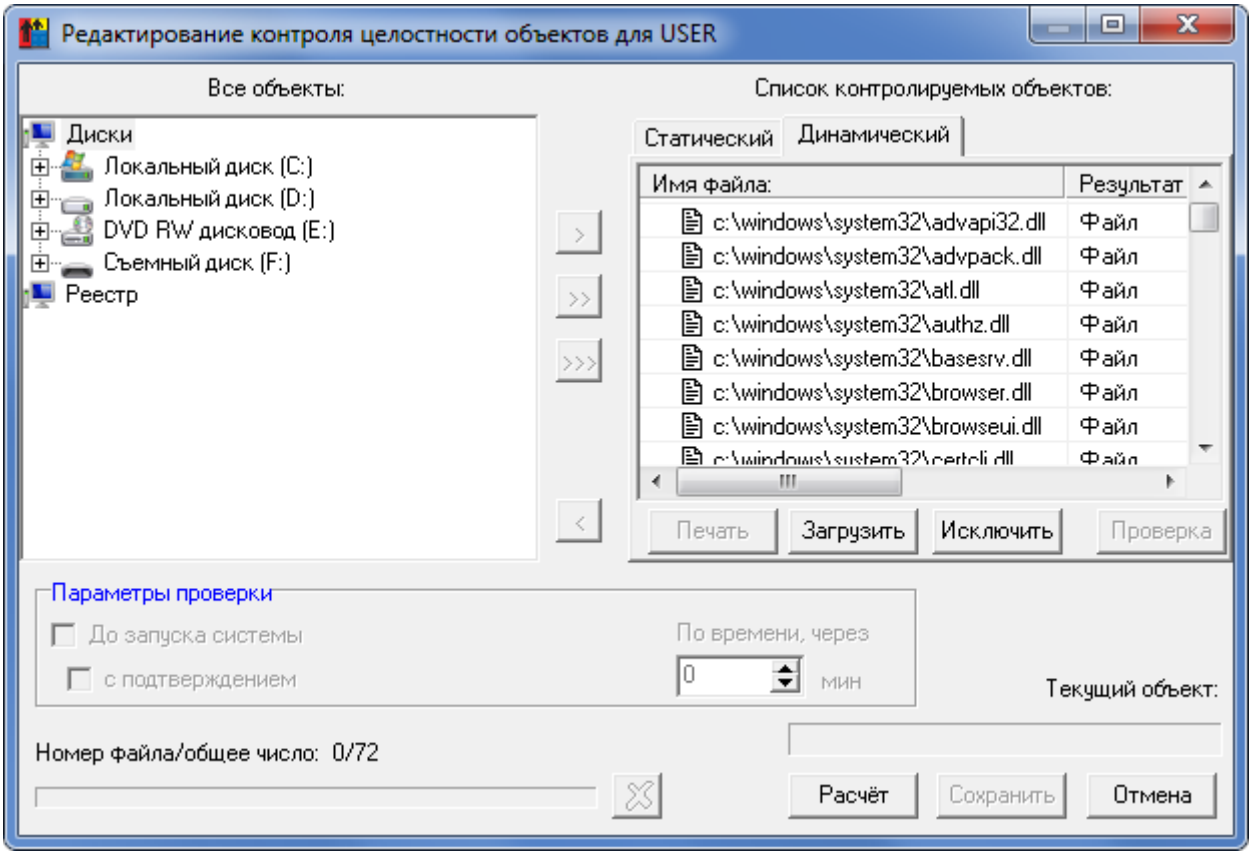

Рисунок 53 - Загрузка файлов в список контроля

После этого необходимо выполнить расчет контрольных сумм файлов. После выполнения расчета список файлов с контрольными суммами можно сохранить (становится доступной кнопка <Печать>, и файл можно распечатать на принтере или записать на диск в виде файла с расширением .HSH). Этот файл можно использовать на других защищаемых СВТ с идентичным составом прикладного ПО, чтобы не вводить каждый раз список вручную. Не забудьте только выполнить пересчет контрольных сумм для конкретного пользователя или группы.

ВНИМАНИЕ! Файл с СКЦ можно редактировать вручную. Формат содержимого файла с СКЦ (*.hsh) имеет следующий вид:

#W:WinSxS\x86_microsoft.vc80.atl_1fc8b3b9a1e18e3b_8.0.50727.762_none_11ecb0ab9b2caf3c\ATL80.dll

Для наиболее часто используемых каталогов введены следующие обозначения:

#W: - Windows

#S: - Windows\System32

#D: - Windows\System32\Drivers

#P: - Program Files

#A: - Accord.NT/Accord.X64

При установке на контроль целостности системного реестра файл .hsh будет иметь следующий вид:

[] #A:ACED32.exe

[] C:\!BK\666.XPS

[] C:\!BK\ACSETUP_ERROR.PNG

[] HKLM\SOFTWARE\ACRONIS\MMS\CONFIGURATION\ALERTS:>CURRENTCONFIGURATION

Если список контролируемых объектов не пуст, то становится доступной кнопка <Исключить>. Эта команда позволяет исключить из списка контролируемых объектов набор файлов, предварительно сохраненный в файле .HSH. Такая функция может быть полезной в случае, когда изменился состав контролируемого ПО в сторону уменьшения числа файлов на жестком диске, и нужно эти изменения выполнить на нескольких компьютерах. Порядок действий может быть таков:

- на одном компьютере сохраняем резервную копию списка файлов;
- очищаем список;
- включаем в список только те файлы, которые предполагается исключить из процедуры контроля, и сохраняем этот список в отдельном файле;
- восстанавливаем полный список с резервной копии и выполняем команду <Исключить>, используя второй сохраненный файл в качестве шаблона;
- скопировав на носитель файл №2, используем его для исключения файлов из списка контроля на других компьютерах.

7.11.Установка правил разграничения доступа (ПРД) к объектам доступа

СПО «Аккорд» поддерживает два типа управления правилами разграничения доступа:

- дискреционный механизм ПРД;
- мандатный механизм ПРД.

Система атрибутов доступа и особенности ее реализации описаны в «Руководстве администратора» (37222406.26.20.40.140.091 90). Можно

использовать отдельно каждый механизм управления. Возможен вариант использования комбинированной политики безопасности с применением обоих механизмов задания ПРД.

Выбор механизма управления ПРД осуществляется:

- установкой соответствующих флагов («Дискреционный», «Мандатный», «Контроль процессов») в программе настройки комплекса «Аккорд» – ACSETUP.EXE (рисунок 54), подробнее о работе с данной программой см. документ «Руководство по установке»;
- установкой в файле accord.ini соответствующих значений (Yes или No) для параметров Discrete Access, Mandatory Access, CheckProcess (см. Приложение 2 настоящего Руководства).

Установка доступа к объектам и процессам с использованием дискреционного и/или мандатного механизмов разграничения доступа осуществляется в программе ACED32.EXE.

7.11.1. Установка доступа к объектам с использованием дискреционного метода ПРД

7.11.1.1. Общие сведения

Для включения дискреционного механизма задания и контроля ПРД необходимо в программе настройки комплекса «Аккорд» (ACSETUP.EXE) установить флаг «Дискреционный» (рисунок 54).

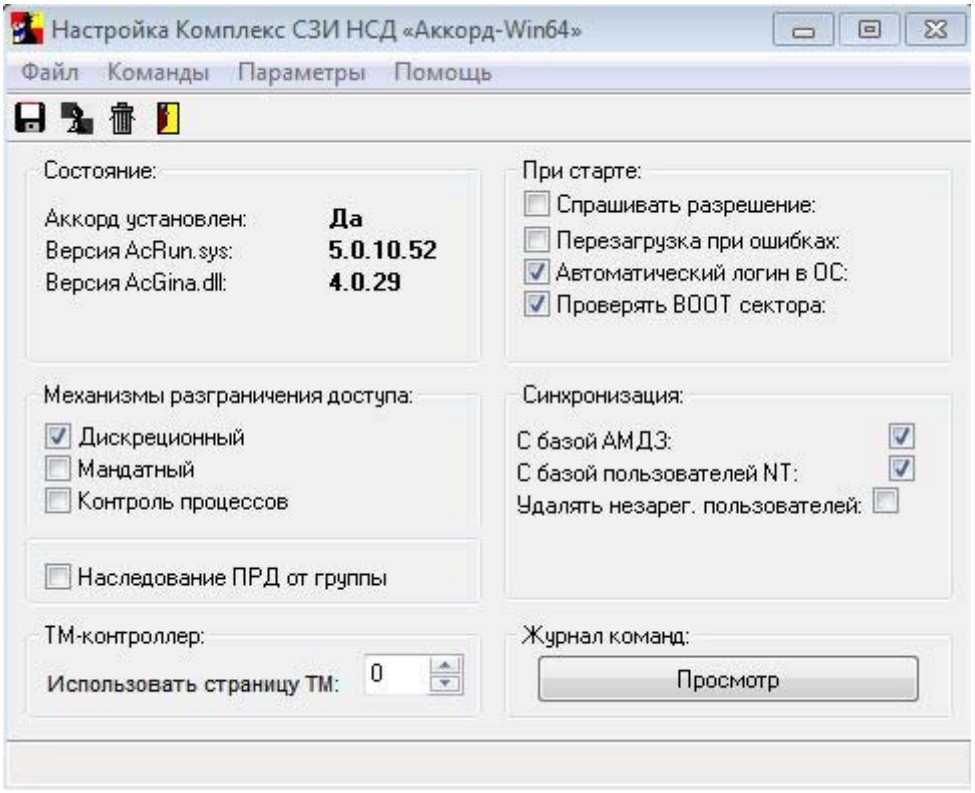

Рисунок 54 - – Главное окно утилиты «Настройка комплекса Аккорд»

Для редактирования правил разграничения доступа в главном окне программы ACED32.EXE (рисунок 2) нажмите мышкой правую кнопку в строке «Разграничение доступа», и на экран выведется окно с правами доступа пользователя к ресурсам СВТ, показанное на рисунке 55. По умолчанию выведен перечень всех доступных корневых каталогов (для сетевых корневых каталогов указано полное сетевое имя), ключей реестра (строки, начинающиеся с «\HKEY_»), сетевых и локальных принтеров. В этом окне нет деления на диски, каталоги, файлы и т.д., а ведется один общий список объектов. Для того чтобы запретить доступ к логическому диску, достаточно исключить корневой каталог этого диска из списка объектов.

Для того чтобы сделать какой-либо файл «скрытым», т.е. полностью запретить к нему доступ, нужно включить его в список объектов, но не назначать ни одного атрибута доступа.

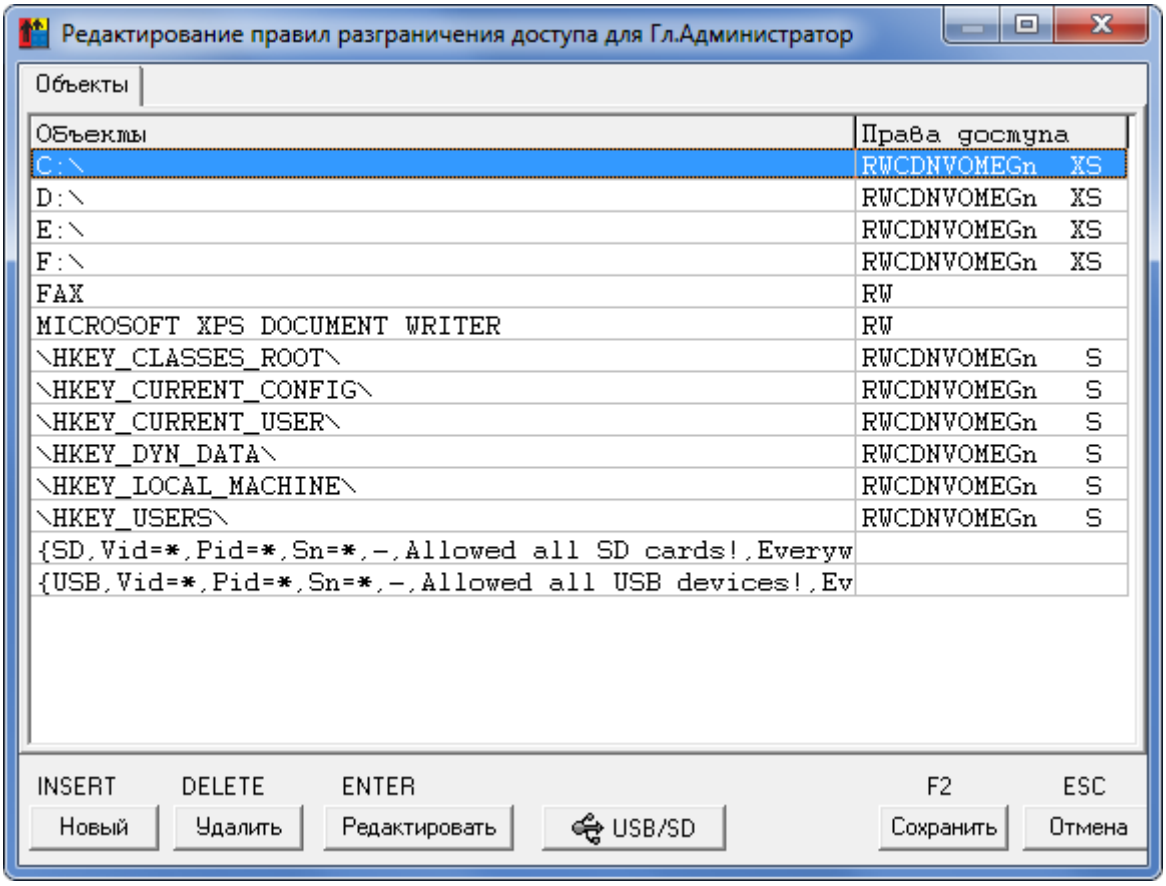

Рисунок 55 - Окно установки дискреционных ПРД к объектам

Более подробно действие атрибутов доступа описано в «Руководстве администратора» (37222406.26.20.40.140.091 90).

В список объектов для обычных пользователей уже включены ограничения, которые защищают от модификации программные компоненты СПО «Аккорд». В разделе «Объекты» (рисунок 55) выберите строку с нужным именем объекта и нажмите кнопку <Редактировать> или клавишу <Enter> - выводится окно для определения правил доступа к объекту, показанное на рисунке 56.

Если Вы хотите удалить какой-либо объект и установленные для него ПРД, выберите строку с названием объекта, нажмите кнопку <Удалить> или клавишу <Delete>. Подтвердите или отмените удаление.

Для выхода из режима редактирования с сохранением нажмите кнопку <Сохранить> или клавишу <F2>, без сохранения – <Закрыть> или <Esc>.

Примечание: при вводе имени файла можно пользоваться простым групповым обозначением имени файла, используя шаблон *.расширение. Например, можно *.bak, *.exe и т.п., нельзя *a.exe, a*.bat, &a.dat, ?a.dat, a.* и т.п.

ВНИМАНИЕ! При обновлении СПО «Аккорд» следует учитывать, что ПРД для новых объектов, сформированных производителем СПО «Аккорд», автоматически могут быть добавлены в базу Accord.amz только посредством выполнения процедуры импорта из файла AccordUpdate.prd (подробнее о процедуре импорта ПРД см. 7.15.2), входящего в комплект обновлений для СПО «Аккорд».

В новых версиях СПО «Аккорд», устанавливаемых впервые, новые ПРД для объектов уже добавлены по умолчанию в базу Accord.amz.

Права доступа по умолчанию могут отличаться в зависимости от типа операционной системы и установленных антивирусов.

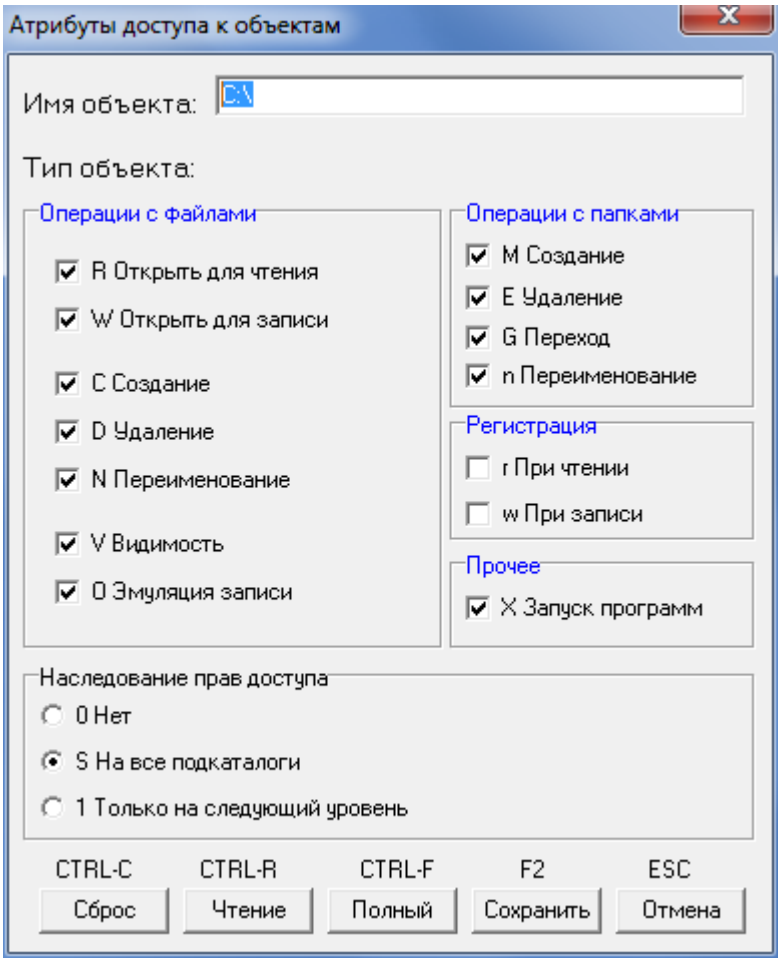

Рисунок 56 - Атрибуты доступа к объекту

ВНИМАНИЕ! Если программа ACED32 в окне «Атрибуты доступа к объектам» не выводит в дереве объектов необходимые ключи реестра, то эти ключи можно прописать вручную в поле «Имя объекта».

При установке дискреционных ПРД могут использоваться следующие атрибуты доступа:

1) Операции с файлами:

- R - разрешение на открытие файлов только для чтения.
- W - разрешение на открытие файлов для записи.
- C - разрешение на создание файлов на диске.
- D - разрешение на удаление файлов.
- N - разрешение на переименование файлов.
- V - видимость файлов. Позволяет делать существующие файлы невидимыми для пользовательских программ. Доступ возможен только по полному пути в формате Windows NT. Этот параметр имеет более высокий приоритет, чем R,W,D,N,O.
- O - эмуляция разрешения на запись информации при открытии файла. Этот параметр имеет более низкий приоритет, чем W (открыть для записи). Параметр может пригодиться в том случае, если программа по умолчанию открывает файл для чтения/записи, а мы хотим разрешить пользователю только просмотр файла.

2) Операции с каталогом:

- M - создание каталогов на диске (или подкаталогов в каталоге, для которого устанавливается атрибут).
- E - удаление каталогов на диске (или подкаталогов в каталоге, для которого устанавливается атрибут).
- G - разрешение перехода в этот каталог.
- n – переименование каталога. В ОС Windows, например, удаление папки в «корзину» – это, на самом деле, переименование каталога.

3) Прочее:

- X - разрешение на запуск программ.

4) Регистрация:

- r - регистрируются все операции чтения файлов диска (папки) в журнале.
- w - регистрируются все операции записи файлов диска (папки) в журнале.

Примечание: для группового манипулирования параметрами доступа пользуйтесь кнопками <Сброс> (сбрасывает все параметры), <Чтение> (устанавливает параметры R, V, G, X, S), <Полный> (устанавливает все параметры кроме параметров группы «Регистрация») или соответствующими им горячими клавишами - <Ctrl+C>, <Ctrl+R>, <Ctrl+F> (рисунок 39).

Для каталогов, в том числе и корневого каталога диска, устанавливается отдельный параметр, который очень важен для реализации ПРД – это параметр наследования прав доступа.

Параметр наследования прав доступа может принимать три значения:

- S - параметры доступа наследуются существующими и созданными в дальнейшем подкаталогами **всех** уровней текущего каталога, т.е. для них устанавливаются те же параметры доступа, что и у «родительского» каталога, при этом для отдельных подкаталогов можно явно определять атрибуты доступа;
- 1 - параметры доступа текущего каталога наследуются **только** подкаталогами следующего уровня;
- 0 - параметры доступа текущего каталога не наследуются подкаталогами.

Например, если для корня дерева каталогов диска C:\ установить атрибут 0, доступными будут только файлы в корневом каталоге, а остальные каталоги для данного пользователя как бы не существуют. Каталог на диске C:\ будет доступен пользователю (с любой непротиворечивой комбинацией атрибутов) только при явном его описании в списке прав доступа. Если для корневого каталога C:\ установить атрибут S, то все его файлы, каталоги и подкаталоги доступны пользователю, и правила доступа к ним определяется атрибутами, установленными для C:\. В этом случае отдельный каталог можно включить в список ПРД и установить для него персональные атрибуты, отличные от «родительских». Если какой-либо объект (каталог, файл, раздел реестра, сетевой ресурс, съемный диск или очередь печати) явно прописан в списке доступа, то для него действуют установленные ПРД, независимо от атрибутов наследования объектов вышестоящего уровня.

Если необходимый Вам объект отсутствует в списке (рисунок 55), нажмите кнопку <Новый> или клавишу <Insert> - на экран выводится расширенное окно «Атрибуты доступа к объектам» (рисунок 57). Справа в этом окне отображен список всех объектов. Каждый объект выделен цветом, соответствующим наследованию прав доступа и наличию объекта в списке разграничения прав доступа (таблица 10).

Таблица 10 – Список объектов в расширенном окне «Атрибуты доступа к объектам»

Наличие объекта в списке	Атрибут наследования прав доступа	Цвет
Есть	Полное наследование	Зеленый
Есть	Наследование на один уровень	Синий
Есть	Нет наследования	Красный
Нет	Атрибуты доступа наследуются	Коричневый
Нет	Нет доступа	Черный

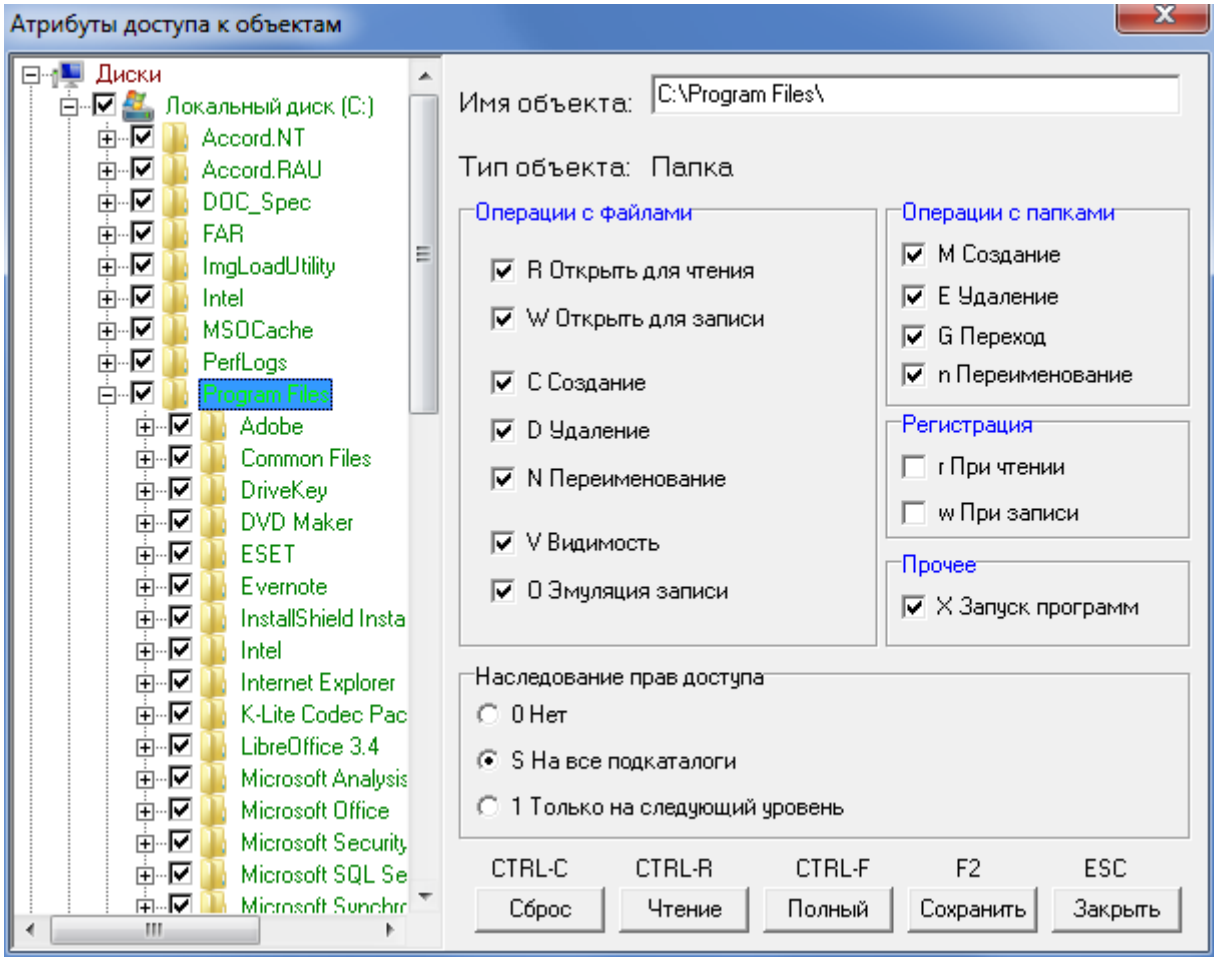

Рисунок 57 - Выбор нового объекта и установка ПРД

Введите в поле «Имя объекта» имя объекта и установите для него необходимые атрибуты. С помощью мыши также можно выбрать имя объекта, щелкнув левой кнопкой мыши на имени объекта в дереве объектов, тогда в поле «Имя объекта» отобразится имя выделенного объекта, а не теневое. Если у выделенного объекта уже установлены ПРД, то будут отмечены соответствующие флаги, если нет, то все флаги будут сброшены. При установке ПРД можно воспользоваться клавишами <Сброс>, <Чтение>, <Полный> в нижней части панели. Клавиша <Сброс> снимает все флаги атрибутов доступа. Объект с такими атрибутами становится запрещенным, т.е. недоступным для ВСЕХ программ и процессов, включая и системные. Клавиша <Чтение> устанавливает для выбранного объекта «файл» атрибуты R – открыть для чтения, V – видимость, и X – запуск программ. Для объекта «папка» добавляется атрибут G – переход в данную папку, и S – наследование. Клавиша <Полный> включает все атрибуты для полного доступа. При работе в ОС Windows может случиться такая ситуация, что объект с набором атрибутов «Чтение» не будет открываться некоторыми программами. Это происходит потому, что многие программы (например, большинство приложений Microsoft Office) по умолчанию открывают файл на чтение/запись. В этом случае придется добавить атрибут O – запись, который имитирует разрешение на запись при открытии файла, но не позволяет модифицировать файл. Для сохранения изменений ПРД выделенного объекта нажмите кнопку <Сохранить>

или клавишу <F2>. Более подробно действие атрибутов доступа и их комбинаций описано в документе «Руководство администратора».

Примечание: Особенности работы некоторых прикладных приложений на СВТ с установленными правилами разграничения доступа СПО «Аккорд» приводят к возникновению непрогнозируемых последствий, однако нарушения логики работы СПО «Аккорд» при этом отсутствуют. Например, если установить запрет на удаление файлов для каталога «CatalogName», то при попытке сохранения файла «Name.txt» в каталог «CatalogName» на экране появляется сообщение «У вас отсутствуют права на изменение файлов на этом сетевом диске. Обратитесь к администратору, чтобы получить права для внесения изменений». При этом в самом каталоге «CatalogName» файл «Name.txt» сохраняется пустым. Описанная ситуация связана с особенностями работы программы NotePad.exe.

7.11.1.2. Установка ПРД к сетевым ресурсам

По умолчанию все сетевые ресурсы обычному пользователю запрещены. Для разрешения доступа нужно явно указать полное сетевое имя ресурса. Это относится и к сетевым принтерам, и к очередям печати. Если правила доступа к сетевым ресурсам определяются администратором домена (сервера), то можно задать универсальный сетевой ресурс. Для этого в список нужно включить объект \\ (ввести с клавиатуры), установить ему полный доступ и наследование на все подкаталоги.

ВНИМАНИЕ! При задании параметров доступа к сетевым ресурсам необходимо указывать полное сетевое имя ресурса, например: \\SERVER1\VOL2\DOC1\.

7.11.1.3. Установка ПРД к съемным устройствам

При описании правил доступа **к съемному устройству** (USB флэш-диску, USB Zip-диску) необходимо, чтобы это устройство было подключено к компьютеру. Нажмите кнопку <Новые>, выберите «Съемный диск» в списке, установите ему ПРД и сохраните изменения кнопкой <Сохранить> или клавишей <F2>. В дальнейшем при работе пользователя после подключения соответствующего устройства для него будут действовать установленные ПРД.

Установка ПРД возможна как непосредственно к самому устройству целиком, так и к отдельным каталогам и файлам, содержащимся на нем.

ВНИМАНИЕ! Процедура описания правил доступа к съемным дискам (USB флэш, Zip, floppy, съемные HDD) выполняется корректно только в том случае, когда съемное устройство подключено к компьютеру ДО запуска программы ACED32.EXE и остается подключенным до завершения процедуры сохранения базы данных пользователей.

При этом **необходимо, чтобы USB-устройство предварительно было включено в список устройств, разрешенных к использованию на данном компьютере.** Выполнение данной процедуры описано в п. 7.16 настоящего Руководства.

По умолчанию разрешено использование всех USB-устройств, т.е. в список объектов (рисунок 59) включена запись:

```
{USB, Vid=*, Pid=*, Sn=*, -, Allowed all USB devices!}
```

Разрешение на доступ для USB-устройства задается через vid/pid и серийный номер данного устройства сразу при добавлении разрешения на букву диска. Данное устройство отображается в окне задания атрибутов доступа к объектам (рисунок 58) следующим образом:

`#USB\VID=%номер vid%\PID=%номер pid%\SN=%серийный номер%`

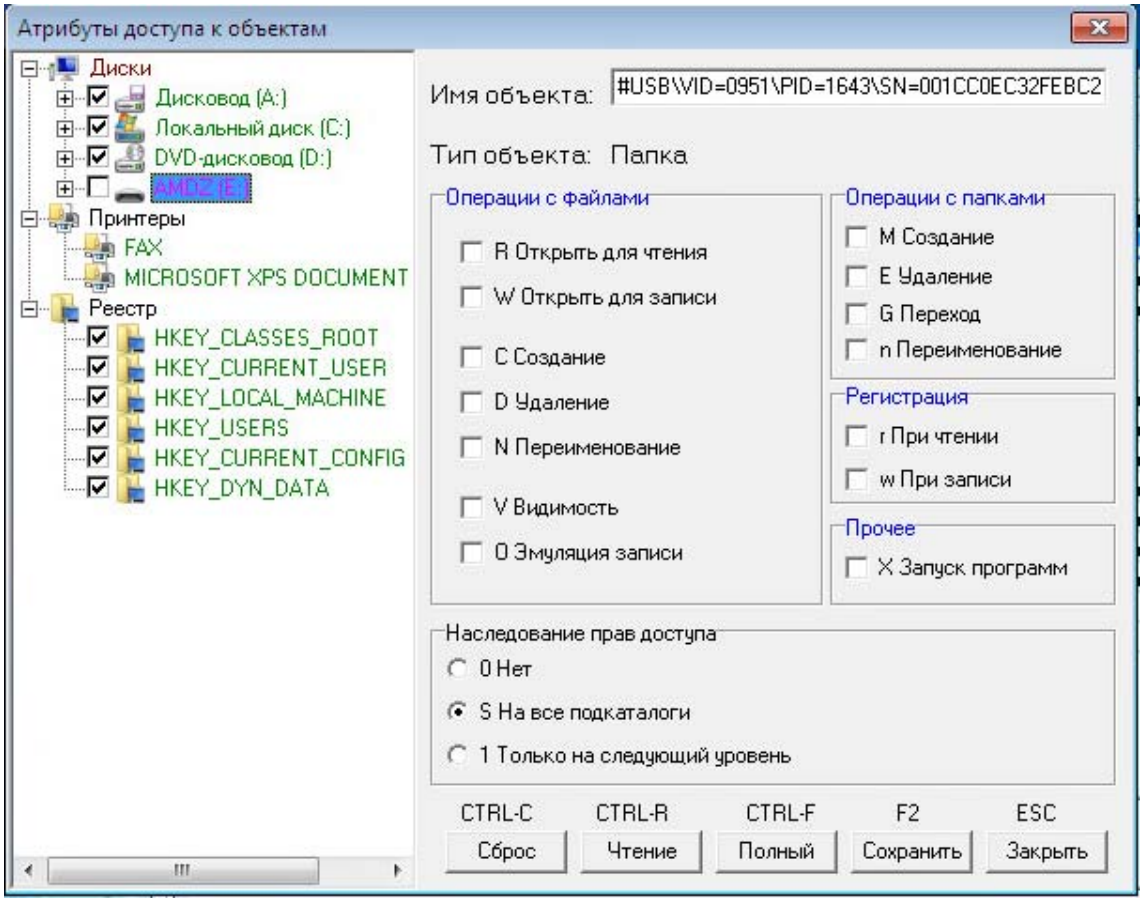

Рисунок 58 - Выбор USB-устройства и установка ПРД

После описания правил доступа для данного устройства в окне редактирования правил разграничения доступа (рисунок 59) будет добавлена запись вида

`#USB\VID=%номер vid%\PID=%номер pid%\SN=%серийный номер%`

с описанными для данного устройства ПРД.

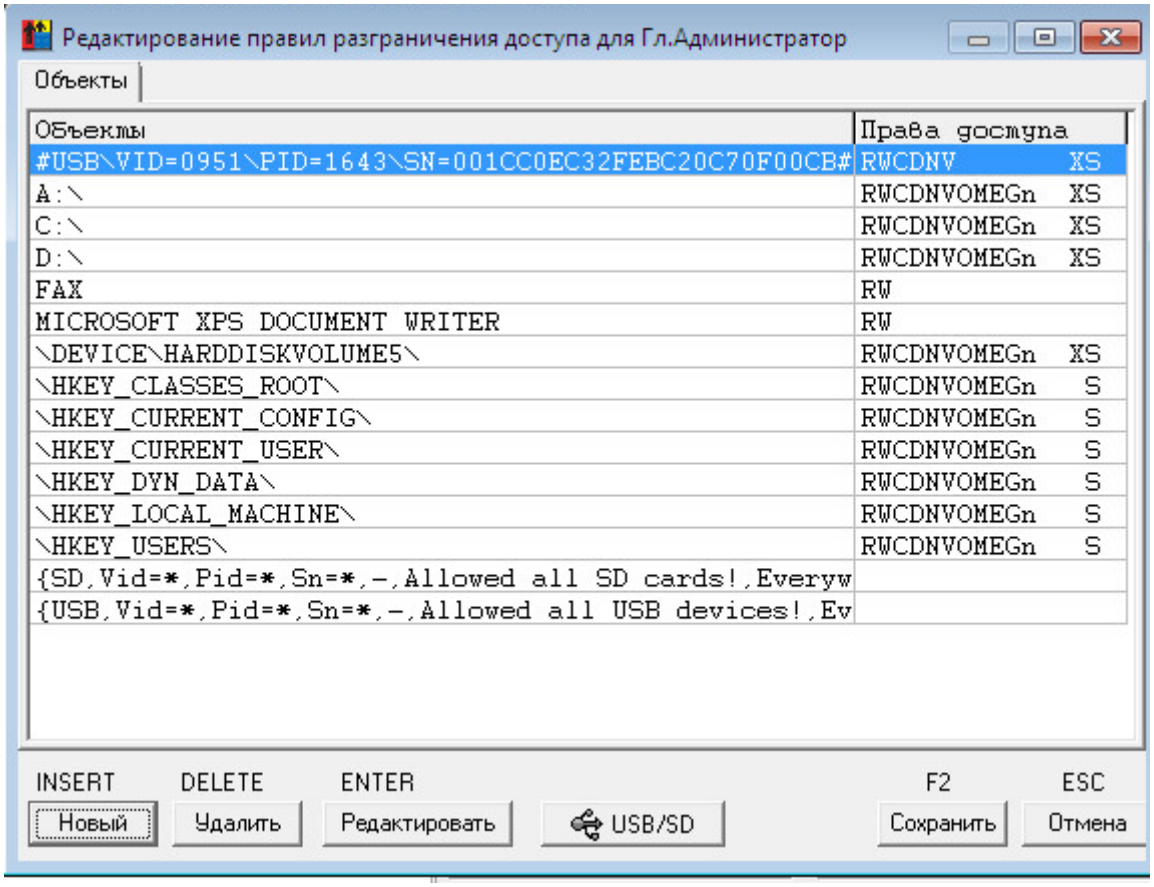

Рисунок 59 - Окно установки дискреционных ПРД к объектам

Для разрешения **доступа ко всем USB-накопителям** в окне задания атрибутов доступа к объектам (рисунок 58) следует добавить запись:

```
#USB\
```

Для разрешения **доступа к заданным USB-накопителям определенного производителя** в окне задания атрибутов доступа к объектам (рисунок 58) следует добавить запись:

```
#USB\VID=XXXX\PID=YYYY\
```

где XXXX, YYYY – соответствующие значения vid и pid.

Имеется также дополнительная возможность **задания простых имен устройствам, для которых уже заданы правила доступа**. Для этого необходимо в окне редактирования ПРД выбрать их нажатием правой кнопкой мышки и в выпадающем списке выбрать пункт «Установить имя USB-диска» (рисунок 60).

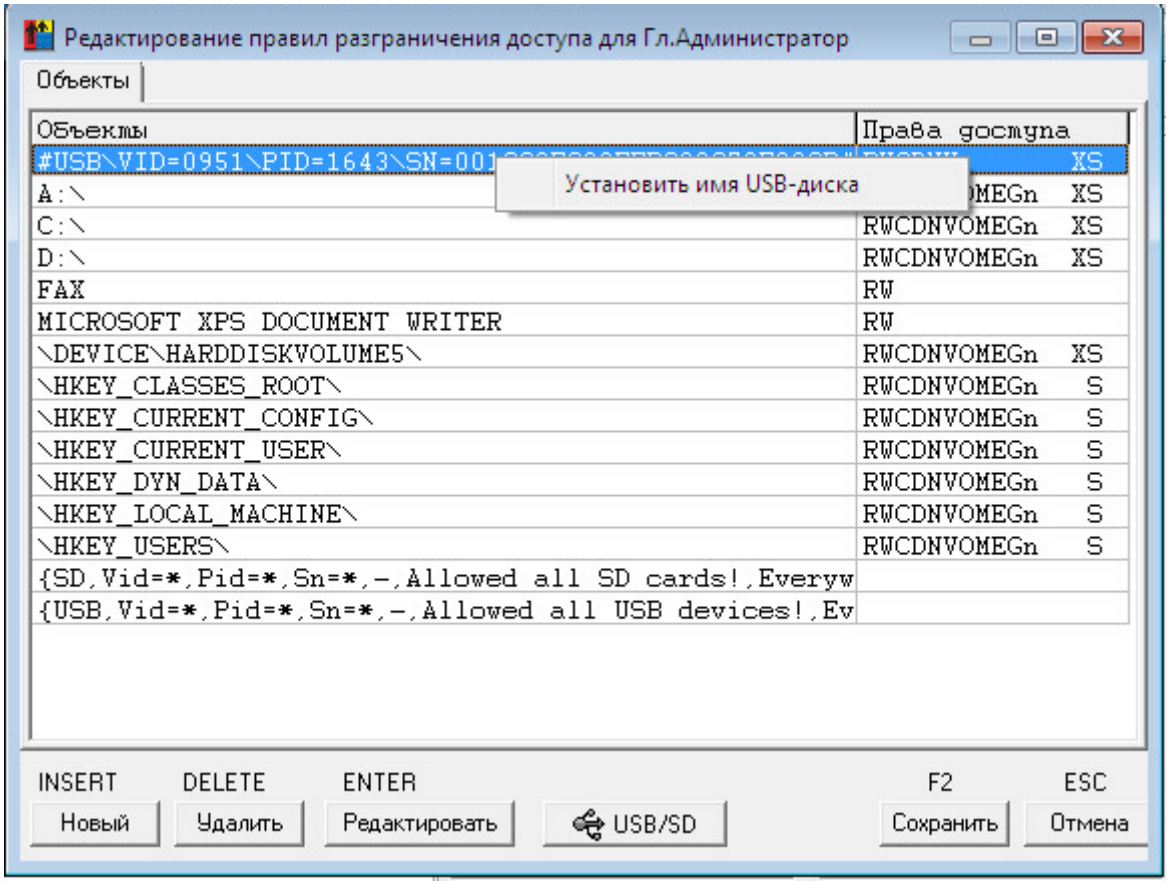

Рисунок 60 - Окно редактирования ПРД

В появившемся далее окне необходимо задать имя для диска (поле «Установить имя USB-диска»), которое в дальнейшем будет отображаться в списке правил разграничения доступа, и нажать на кнопку <OK> (рисунок 61).

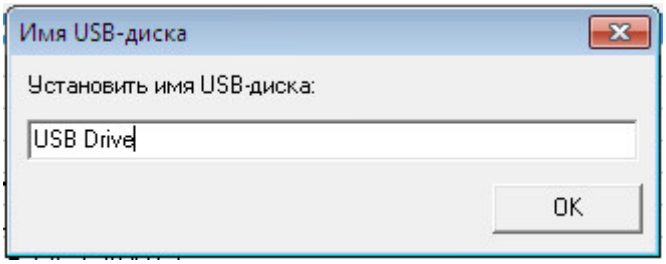

Рисунок 61 - Задание имени USB-диска

После этого заданное имя отобразится в списке объектов (рисунок 62) в следующем виде

`#USB\%название%#0\`

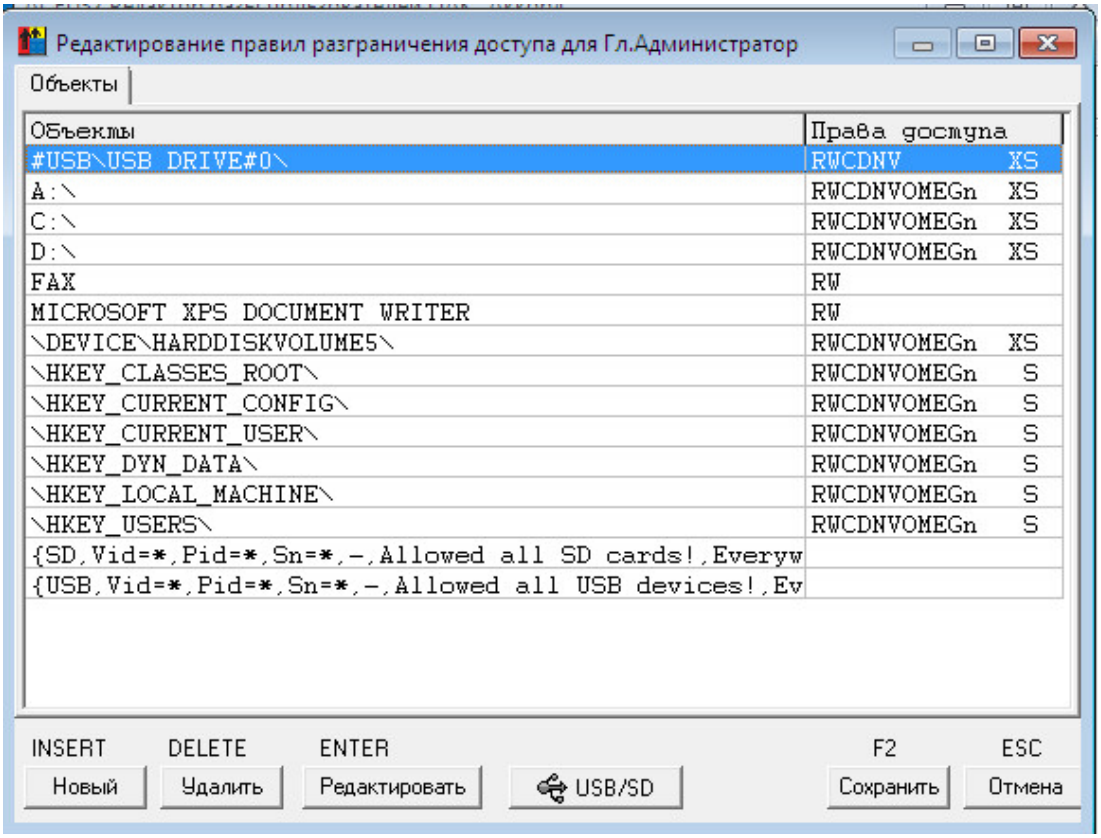

Рисунок 62 - Окно редактирования ПРД

Информация обо всех устройствах, для которых было изменено имя, заносится в файл AcUsbNames, находящийся в каталоге с установленным СПО «Аккорд». Пример содержимого данного файла показан на рисунке 63.

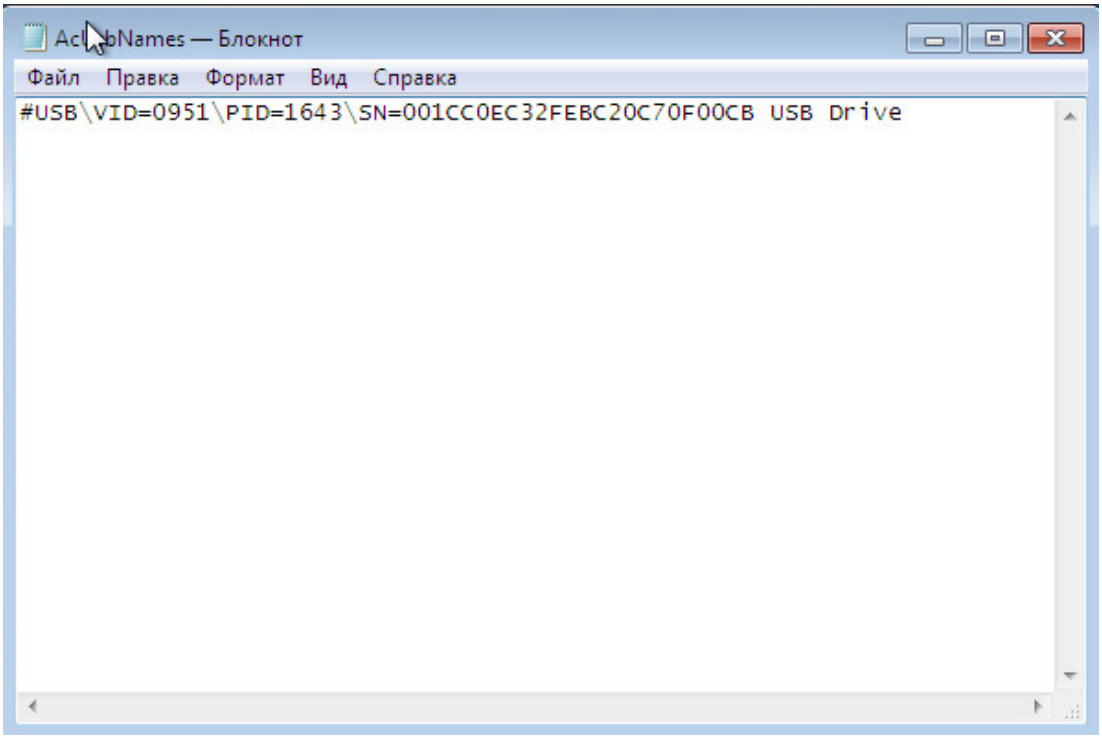

Рисунок 63 - Содержимое файла AcUsbNames

7.11.1.4. Установка ПРД к стационарным устройствам

Еще один важный момент – регулирование доступа **к стационарным устройствам**, которые входят в состав компьютера. В список объектов можно включить такие устройства, как Com1, Com2, LPT1.

По умолчанию доступ к этим устройствам разрешен, но если устройство отметить в списке ПРД, то доступ к нему будет ЗАПРЕЩЕН.

Для того чтобы список стационарных устройств отображался в редакторе ПРД, нужно в меню программы «Настройка комплекса «Аккорд» <Параметры> - <Дополнительные опции> на закладке «Контроль» в поле «Дополнительные подсистемы» отметить флаг «Включить контроль доступа к устройствам» и нажать кнопку «Принять». Выйти из программы с сохранением.

Далее зайти в программу «Редактор прав доступа», в правом нижнем углу нажать кнопку рядом с полем «Разграничение доступа». В окне «Редактирование правил разграничения доступа» нажать кнопку «Новый». В появившемся окне «Атрибуты доступа к объектам» появляется новый класс объектов – «Устройства» (рисунок 64).

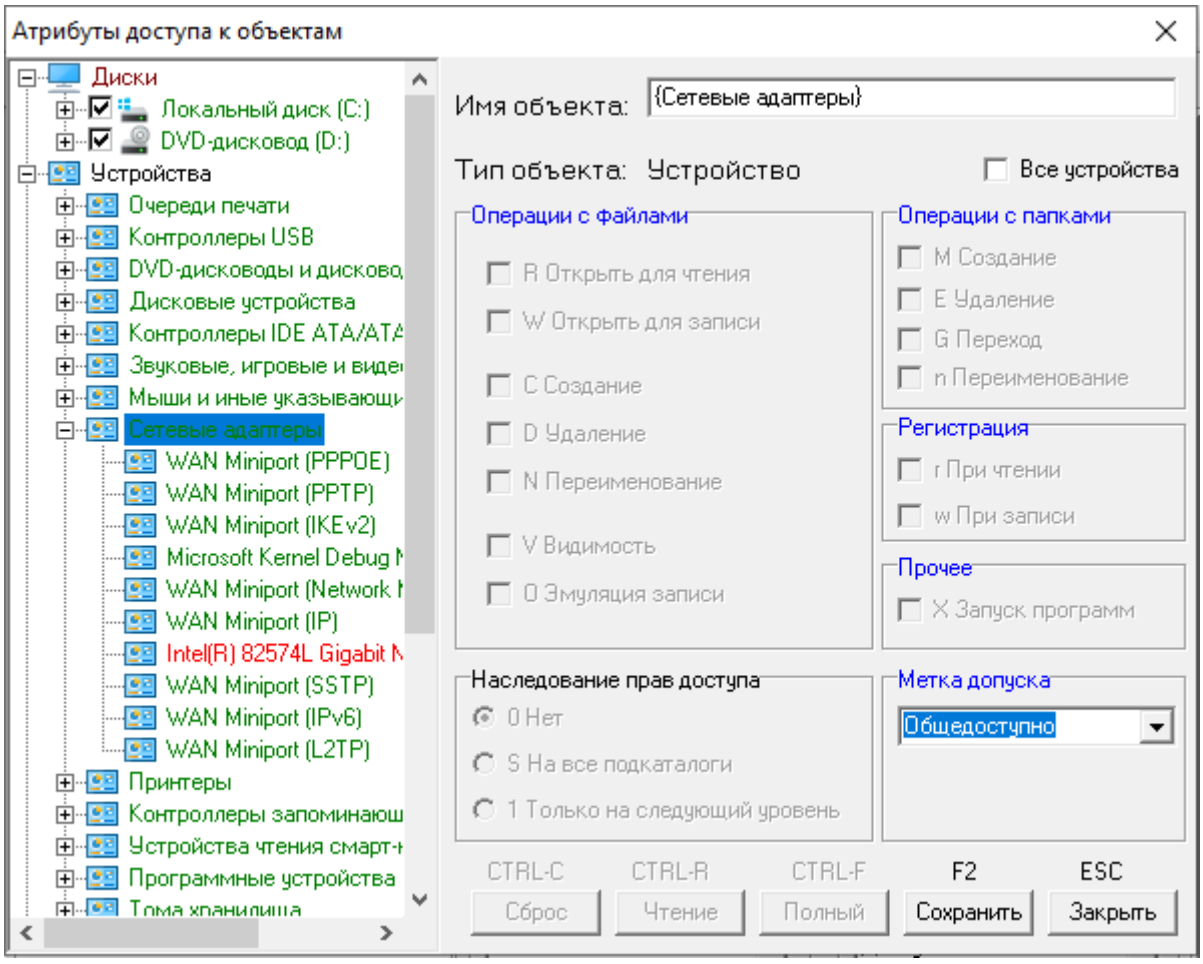

Рисунок 64 – Установка ПРД к стационарным устройствам

Можно выбрать конкретное устройство и нажать «Сохранить», при этом объект будет выделен красным цветом, что означает, что доступ к устройству

невозможен. Если выбрать класс устройств, то подобным образом можно заблокировать все устройства этого класса. При этом любое устройство, принадлежащее к данному классу, можно разблокировать. Для этого нужно выбрать устройство и снова нажать кнопку «Сохранить».

ВАЖНО! В журнале событий устройства могут отображаться с полными системными именами, например, LPT1 – это \DEVICE\PARALLEL0, а Com1 – это \DEVICE\SERIAL0.

Таблица 11 - Сообщения, выдаваемые программой при установке дискреционных ПРД, и порядок действий по ним

Сообщение	Причина	Порядок действий
«Сохранить изменения для объекта *(указывается имя_объекта)* доступа?»	После изменения ПРД объекта не сохранены изменения	«Да» - сохранить изменения «Нет» - не сохранять изменения.

7.11.2. Установка доступа к объектам с использованием мандатного метода контроля ПРД

7.11.2.1. Настройка уровня доступа пользователя

После включения в программе ACSETUP.EXE мандатного механизма задания и контроля ПРД (рисунок 54, флаг «Мандатный», подробнее о работе с данной программой см. документ «Руководство по установке») в главном окне программы ACED32.EXE (рисунок 2) появляется кнопка <Уровень доступа> на панели инструментов и пункт «Уровень доступа» в меню «Команды». Доступна также строка «Уровень доступа» в поле «Уровень доступа пользователя». С помощью этой команды можно установить или изменить уровень доступа пользователя[7] (рисунок 65).

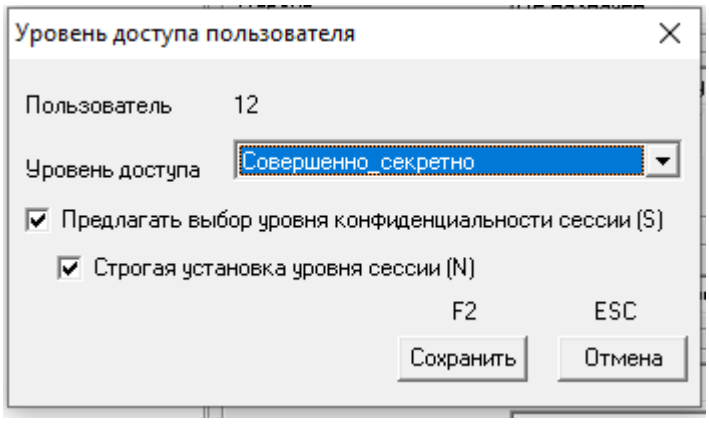

Рисунок 65 - Установка уровня доступа пользователя

[7] Флаги «Предлагать выбор уровня конфиденциальности сессии» и «Строгая установка уровня сессии» доступны в окне выбора уровня доступа пользователя только при включенном механизме контроля процессов

Мандатный механизм доступа реализуется по следующему правилу: если уровень доступа субъекта (пользователя) выше или равен метке допуска объекта (объектами для мандатного механизма могут выступать локальные каталоги и файлы, сетевые ресурсы, каталоги и файлы на съемных устройствах), то доступ к объекту предоставляется данному субъекту.

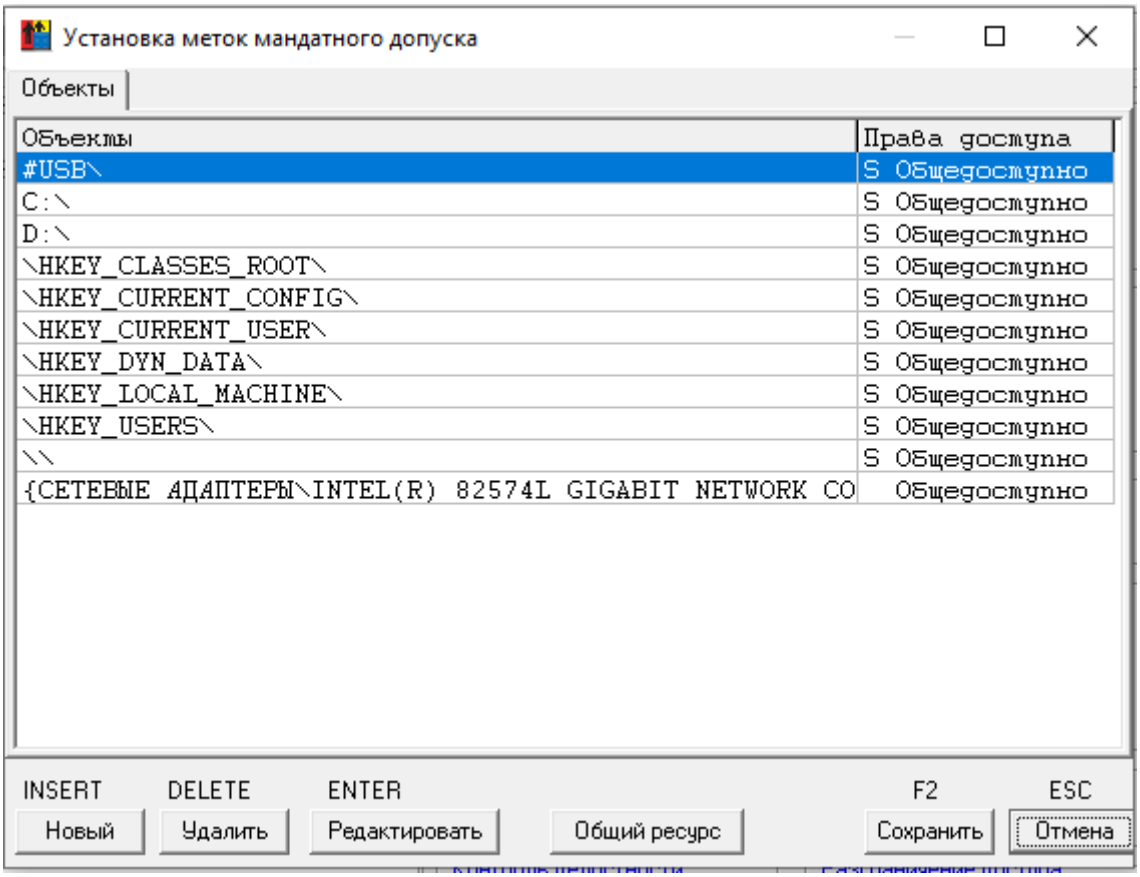

Рисунок 66 - Установка меток допуска объектов при использовании мандатных ПРД

7.11.2.2. Присвоение объектам меток допуска

Для присвоения объектам меток допуска нажмите кнопку на панели инструментов с изображением дерева каталогов или выберите пункт «Мандатный доступ» в меню «Команды». Выводится окно со списком объектов (рисунок 66).

По умолчанию всем объектам присваивается самый низкий уровень – общедоступно. Для изменения метки допуска установите курсор на нужную строку и нажмите Enter или мышью кнопку <Редактировать>. Откроется окно, в котором для объекта можно изменить только два параметра – метку допуска и наследование прав доступа. Метка допуска меняется нажатием мышью на кнопку в строке «Метка допуска» и выбором значения из списка.

Если необходимый Вам объект отсутствует в списке (рисунок 66), нажмите кнопку <Новый> или клавишу <Insert>. На экран выводится расширенное окно «Атрибуты доступа к объектам» (рисунок 67).

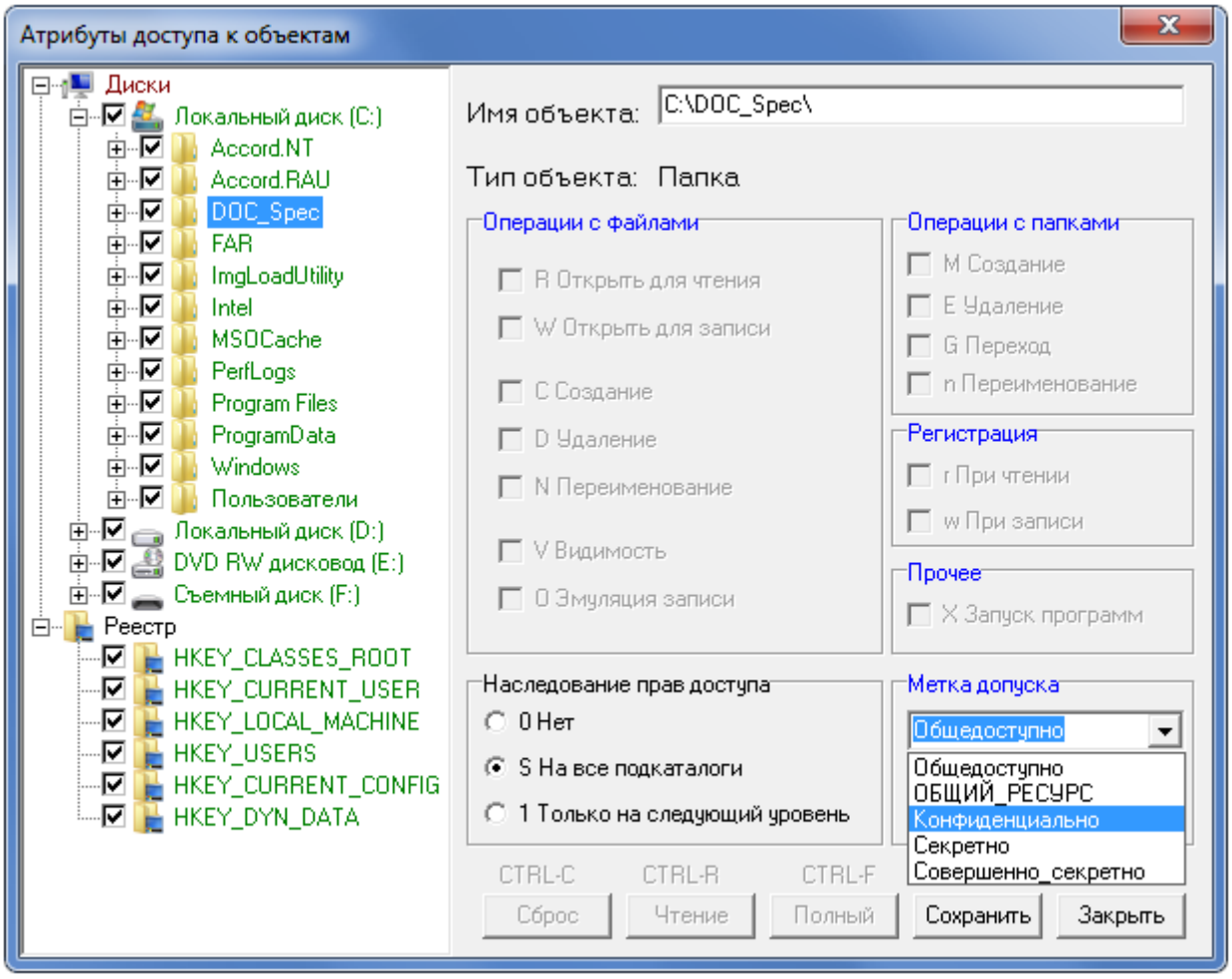

Рисунок 67 - Определение нового объекта и выбор его метки допуска

ВНИМАНИЕ! Если программа ACED32 в окне «Атрибуты доступа к объектам» не выводит в дереве объектов необходимые ключи реестра, то эти ключи можно прописать вручную в поле «Имя объекта».

Слева в этом окне отображен список всех объектов. Введите в поле «Имя объекта» имя объекта и установите для него необходимые атрибуты.

С помощью мыши также можно выбрать объект, щелкнув левой кнопкой мыши на имени объекта, тогда в поле «Имя объекта» отобразится имя выделенного объекта, а в поле «Тип объекта» - его тип (каталог, файл, реестр).

В правом нижнем секторе окна доступна функция установки меток допуска объекта. Установите указатель мыши на стрелку в правой части строки «Метка допуска» и нажмите левую кнопку мыши. Появится список, из которого можно выбрать значение метки допуска выбранного объекта.

Для сохранения изменений ПРД выделенного объекта нажмите кнопку <Сохранить> или клавишу <F2>.

Объект, которому не присвоена метка допуска, считается общедоступным для всех пользователей.

7.12. Контроль процессов с использованием мандатного и/или дискреционного механизмов разграничения доступа

7.12.1. Общие сведения

В СПО «Аккорд» реализована весьма важная с точки зрения безопасности и создания ИПС (изолированной программной среды) функция – это дискреционный и/или мандатный доступ к объектам со стороны такого субъекта, как процесс (задача), который загружен в оперативную память СВТ.

На первом этапе настройки необходимо установить тип механизма разграничения доступа, который планируется использовать для контроля процессов. Для этого следует:

1) запустить программу «Настройка комплекса «Аккорд» (посредством запуска исполняемого файла ACSETUP.EXE или с помощью меню Пуск–> Программы–> Аккорд–> Настройка комплекса Аккорд);

2) в главном окне программы установить необходимые флаги: «Контроль процессов», «Дискреционный» и/или «Мандатный» (рисунок 68);

ВНИМАНИЕ! Контроль процессов может осуществляться только совместно с одним или несколькими механизмами разграничения доступа (дискреционным и/или мандатным).

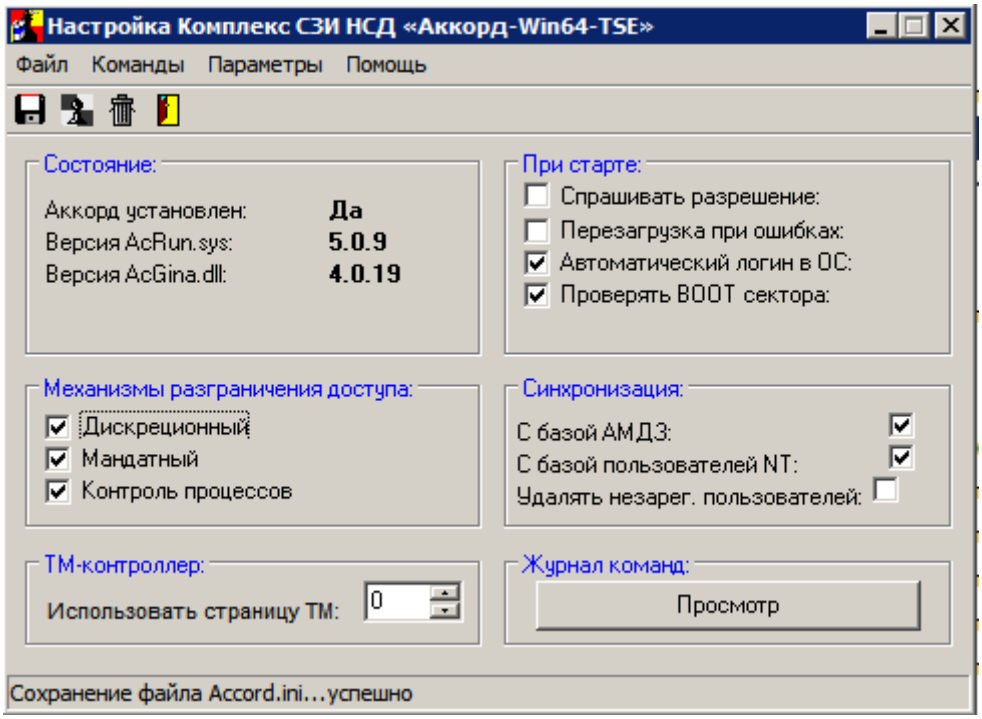

Рисунок 68 - Главное окно утилиты «Настройка комплекса Аккорд»

3) завершить работу приложения с сохранением изменений.

После включения в программе ACSETUP.EXE мандатного и/или дискреционного механизма разграничения доступа для процессов в окне

описания прав доступа пользователя к ресурсам СВТ (программа ACED32.EXE) кроме закладки «Объекты» появляется закладка «Процессы».

При первом запуске программы ACED32.EXE с включенной дисциплиной мандатного и/или дискреционного доступа в список процессов заносятся все процессы, которые в данный момент находятся в оперативной памяти.

Однако на момент старта редактора ACED32.EXE некоторые процессы уже завершают свою работу, поэтому более корректно выполнять формирование списка контролируемых процессов следующим образом:

- в программе настройки комплекса «Аккорд» установить дополнительную опцию «Мягкий режим», в редакторе ПРД для пользователя в поле «Детальность журнала» установить уровень детальности журнала «Высокий». Для отдельного пользователя можно также использовать режим сбора статистики;
- некоторое время предоставить пользователю возможность работать на компьютере в этом режиме, но обязательно с загруженным монитором разграничения доступа;
- с помощью программы AcProc.exe («Создание списка процессов из журналов регистрации») выбрать из журналов используемые при работе программы и сохранить в файле <Имя_пользователя>.PRD, также сохранить список объектов, к которым обращался пользователь во время выполнения должностных обязанностей в файле <Имя_пользователя>.HSH;
- импортировать в редакторе из файла .PRD набор исполняемых файлов;
- установить на динамический контроль целостности объекты из файла .HSH.
- выключить в настройках комплекса «Мягкий режим».

Следует отметить, что настройка контроля процессов с использованием мандатного механизма разграничения доступа имеет ряд важных особенностей, которые описаны в 7.12.2.

Общий алгоритм создания «белого» списка процессов с помощью мандатного и/или дискреционного механизмов разграничения доступа с контролем процессов и динамического контроля целостности файлов из этого списка приведен в 7.12.3.

7.12.2. Особенности настройки контроля процессов с использованием мандатного механизма разграничения доступа

После включения в программе ACSETUP.EXE мандатного механизма разграничения доступа для процессов (подробнее см. 7.12.1) в окне описания прав доступа пользователя к ресурсам СВТ (программа ACED32.EXE) кроме закладки «Объекты» появляется закладка «Процессы».

При первом запуске программы ACED32.EXE с включенной дисциплиной мандатного и/или дискреционного доступа в список процессов заносятся все процессы, которые в данный момент находятся в оперативной памяти. При использовании мандатного механизма РД для них устанавливается уровень доступа «Общедоступный», т.е. самый низкий.

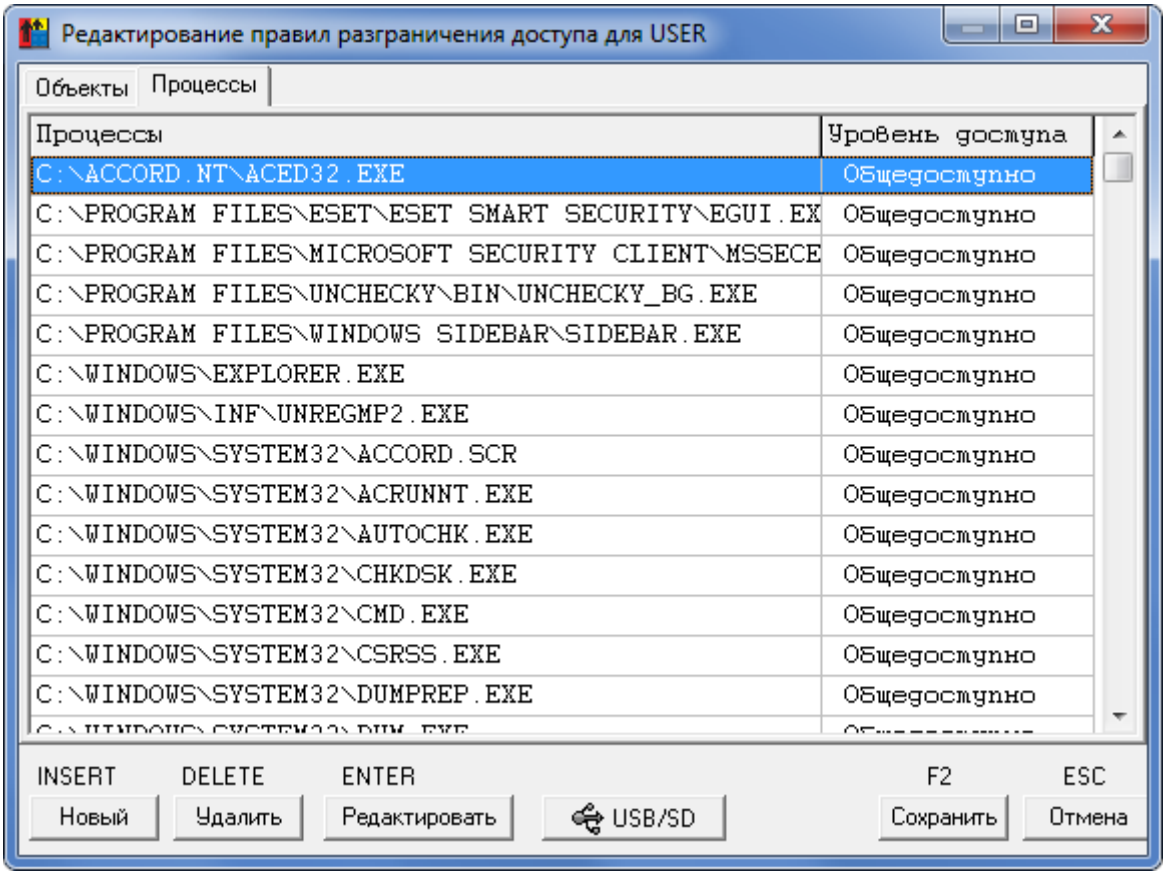

Рисунок 69 - Закладка «Процессы» при включенном механизме мандатного доступа для процессов

Если в списке процессов написать "*", это будет означать необязательное перечисление всех процессов.

Если необходимый процесс отсутствует в списке (рисунок 69), нажмите кнопку <Новый> или клавишу <Insert>.

На экран выводится окно установки уровня доступа (рисунок 70). Имя процесса вводится без указания пути, но с расширением. При установке в программе настройки СПО «Аккорд» параметра «Использовать полный путь процесса» список процессов будет формироваться и проверяться с учетом полного пути. Уровень доступа выбирается из списка.

Для сохранения изменений ПРД выделенного процесса нажмите кнопку <ОК>. Для изменения уровня доступа процесса в разделе «Процессы» выберите строку с нужным именем и нажмите кнопку <Редактировать> или клавишу <Enter>.

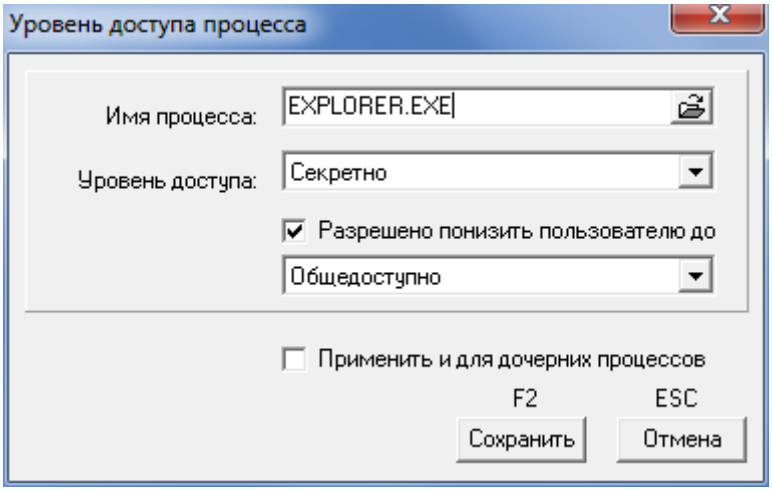

Рисунок 70 - Установка уровня доступа процесса

Часто в рамках работы одного процесса создается другой процесс, аналогичный первому. При этом между двумя процессами используется одна и та же среда окружения. В таком случае первый процесс называется родительским, а второй – дочерним[8].

Флаг **«Применить для дочерних процессов»** предназначен для того, чтобы при присвоении родительскому процессу определенного уровня доступа дочерним процессам автоматически присваивался такой же уровень доступа, как и у родительского (так как присвоение одного и того же уровня доступа большому количеству дочерних процессов является весьма трудоемкой задачей). Это сделано с целью исключения некорректной работы родительского процесса вследствие отсутствия нужного уровня доступа одного из дочерних процессов.

Администратор может для некоторых процессов установить флаг **«Разрешено понизить пользователю»**. Если этот флаг установлен, то при старте такого процесса выводится окно выбора текущего уровня процесса (конечно, при этом уровень доступа можно выбирать только с понижением). Это дает возможность пользователю в одном сеансе работать с документами разных грифов секретности с помощью одной программы (например, Winword), но четко соблюдать **правило запрета на «понижение» метки конфиденциальности документа**, т.к. процессу в системе мандатного контроля запрещается запись в любой ресурс с меньшей по уровню меткой допуска.

В рамках контроля процессов с использованием мандатного механизма разграничения доступа существует ограничение на запуск нескольких объектов, использующих один и тот же процесс. Данная ситуация наблюдается при установке режима доступа на понижение для работы процесса с объектами ниже установленного уровня.

[8)] Дочерними процессами могут быть драйверы, динамические библиотеки, приложения и т.д.

37222406.26.20.40.140.091 97

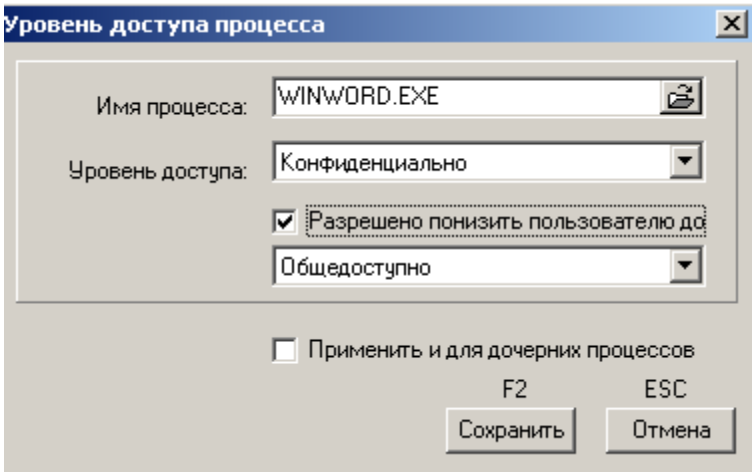

Рисунок 71 – Установка уровня доступа процесса

В случае запуска в рамках данного процесса двух объектов, имеющих разные уровни доступа, выводится предупреждающее сообщение (рисунок 72), которое остается на экране до тех пор, пока документ другого уровня доступа не будет закрыт.

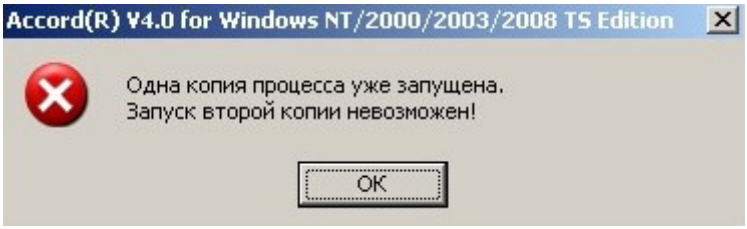

Рисунок 72 – Предупреждающее сообщение

Список процессов с установленными уровнями доступа в наиболее полном и наглядном виде отражает концепцию изолированной программной среды, т.к. доступ к соответствующим ресурсам получат только процессы из этого списка. При этом процесс не имеет доступа на запись информации в объекты нижестоящего уровня.

В реализации процедуры разграничения доступа СПО «Аккорд-Win64 K» исполняемый файл может выступать и как объект, и как субъект. Файл на жестком диске – это объект, которому установлена метка допуска, и запустить файл на исполнение может пользователь с соответствующим уровнем доступа. После запуска процесса он уже как субъект имеет установленный уровень доступа к объектам. В такой системе атрибутов возможна реализация такой политики безопасности, когда обработка объектов с определенной меткой допуска возможна только с помощью процессов соответствующего уровня доступа.

Управление потоками информации осуществляется по следующему алгоритму:

- конкретному процессу запись информации разрешена только в том ресурсе, чья метка допуска **равна** уровню доступа процесса;

- все ресурсы с более низкой меткой допуска открыты для этого процесса только на чтение и запуск программ (атрибуты RVOX).

Таким образом, пользователь не может понизить уровень секретности документа, т.е. скопировать секретный документ в несекретную папку с помощью «секретного» процесса, а для всех процессов, которые не имеют соответствующего уровня, объект «секретно» не доступен.

Теперь возникает новая проблема - в рамках сеанса одного пользователя невозможно корректировать документы с разными метками, т.к. матрица доступа загружается в момент начала сеанса и не меняется в процессе работы. Можно «исхитриться» и создать по нескольку копий одной программы с разными именами и назначить им разные уровни секретности. Для работы с документами «общедоступно» пользователь будет запускать программу Word_obsch, а для документов из папки «Конфиденциально» программу Word_conf. и т.д. Однако Microsoft Офис, как и любой современный программный пакет, - это достаточно сложный продукт, программы и библиотеки которого функционируют по правилам, которые задают разработчики, а не администраторы безопасности. Разные компоненты этого пакета открывают на чтение/запись массу временных, конфигурационных и прочих файлов независимо от воли пользователя и независимо от того, какая копия данного файла запускается. В результате мы приходим к тому, что, соблюдая дисциплину контроля потоков информации, нормально работать со сложным пакетом практически невозможно.

Разработчики ОКБ САПР для решения этой проблемы создали **механизм динамического присвоения уровня мандатного доступа запускаемому процессу**.

Администратор безопасности заранее устанавливает процессу максимально допустимый уровень доступа и флаг «Разрешено понизить пользователю до…». При старте этой задачи на экран выводится диалог, в котором пользователь выбирает тот уровень, который ему требуется для обработки документов с соответствующей меткой допуска. По окончании работы пользователь закрывает задачу и запускает ее заново уже с другим уровнем. При этом СЗИ контролирует буфер обмена, если в опциях установлен флаг «*Не контролировать UNC имена*».

Вторая необходимая подсистема – **метка допуска «ОБЩИЙ_РЕСУРС»**. Если администратор безопасности в редакторе ПРД присваивает эту метку какой-либо папке, то далее создается несколько копий этого объекта, и каждой копии присваивается одна из меток допуска, прописанных в конфигурационном файле системы защиты. Имена копий различаются на один символ, а в процессе работы монитор безопасности динамически перенаправляет ввод-вывод с объекта-оригинала на копию с нужной меткой допуска. Теперь наш сложный программный пакет «думает», что работает, например, с папкой Temp, а на самом деле взаимодействует с ее копией, у которой метка допуска совпадает с текущим уровнем процесса. Становится возможной нормальная работа программ с реальным выполнением дисциплины контроля потоков информации. По умолчанию, если список объектов с меткой «Общий ресурс» пуст, это означает, что установлен запрет на создание копий объектов с соответствующей меткой допуска, прописанной в конфигурационном файле.

В общем случае для работы Microsoft Office нужно назначить метку «ОБЩИЙ_РЕСУРС» следующим объектам:

- c:\documents and settings\all users\application data\
- c:\documents and settings\<имя_пользователя>\application data\
- c:\program files\microsoft office\office<nn>\~$normal.dot
- c:\windows\sti_trace.log

Если нет жестких ограничений по объему дискового пространства, то можно вместо добавления объектов со 2-го по 6-й назначить метку «ОБЩИЙ_РЕСУРС» на весь каталог:

- c:\documents and settings\<имя_пользователя>\application data\microsoft\

Дополнительные настройки администратор делает на основе информации в журналах регистрации событий.

Назначение метки «ОБЩИЙ_РЕСУРС» выполняется в следующей последовательности (на примере Microsoft Office 2009/2011 под Windows 10):

1)в программе настройки AcSetup.exe включить мандатный механизм с контролем процессов;

2)В редакторе ПРД установить уровень детальности журнала «Сбор статистики» для одного из пользователей, входящего в состав группы пользователей СПО «Аккорд», с использованием учетной записи которого будут формироваться списки. При этом пользователю автоматически присваивается высокий уровень детальности журнала, а его работа выполняется в мягком режиме;

3)осуществить от имени пользователя запуск и работу с приложениями, необходимыми для выполнения должностных обязанностей пользователя;

4)завершить сеанс пользователя, запустить от имени Администратора СПО «Аккорд» программу AcProc.exe из каталога Accord.NT (Accord.x64 – для 64-битных ОС) (Пуск –> Программы –> Аккорд -> Создание списка процессов из журналов регистрации) (рисунок 73);

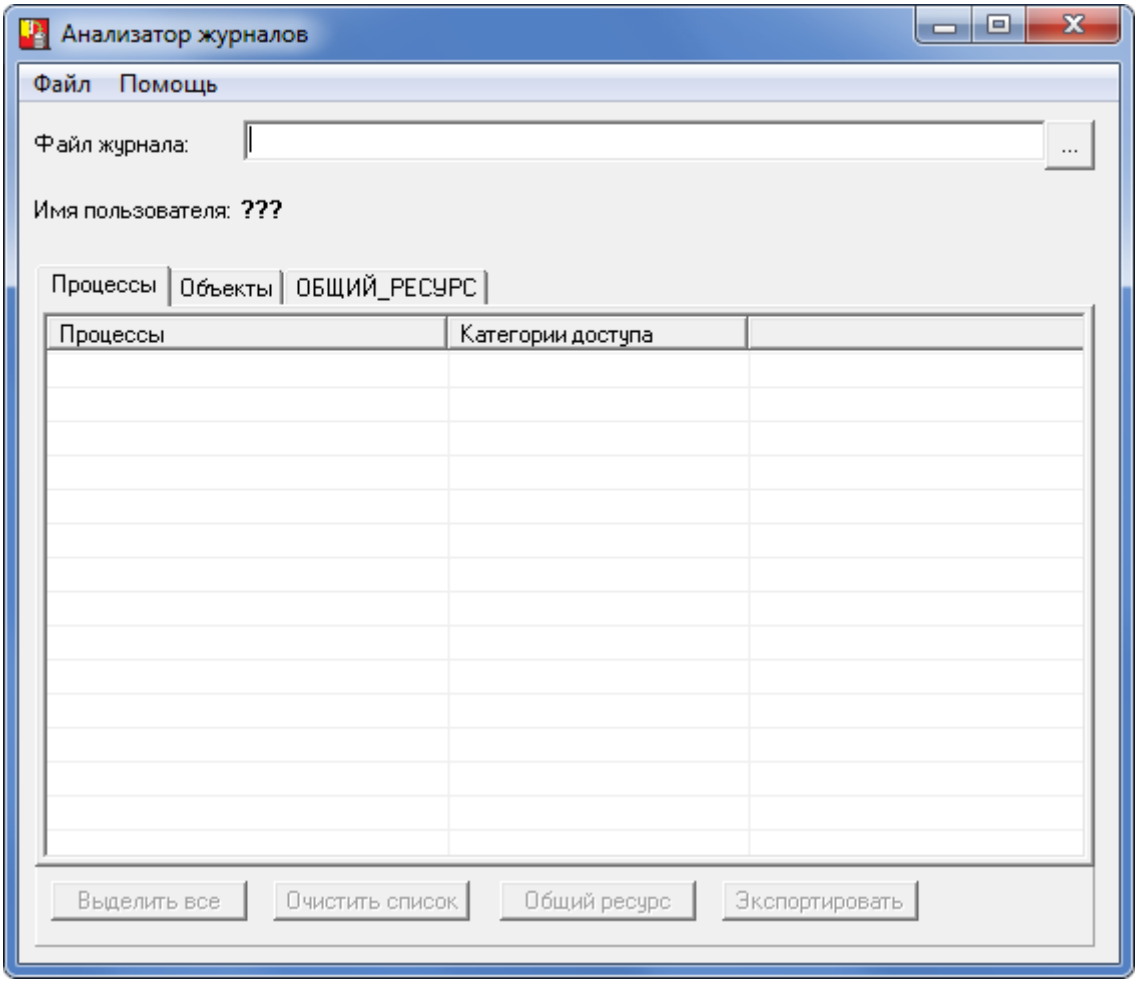

Рисунок 73 - Главное окно программы AcProc.exe

5) во вкладке «Процессы» загрузить журнал последнего сеанса работы пользователя: в окне программы AcProc.exe (рисунок 73) нужно нажать на раскрывающийся список в поле «Файл журнала», далее в появившемся окне (рисунок 74) выбрать файл журнала (или несколько файлов);

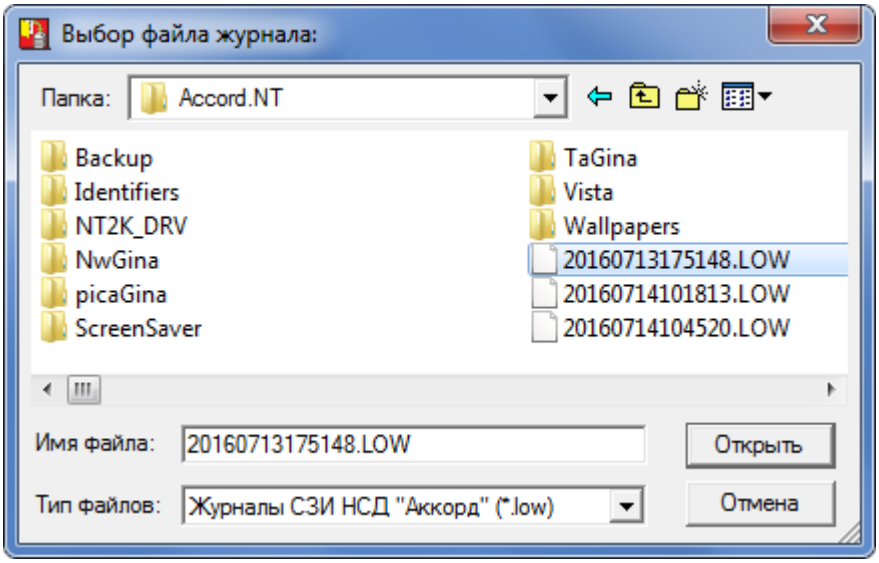

Рисунок 74 - Выбор файла журнала регистрации событий

6)в главном окне программы AcProc.exe выбрать процессы, которые необходимы для выполнения должностных обязанностей пользователя (рисунок 75);

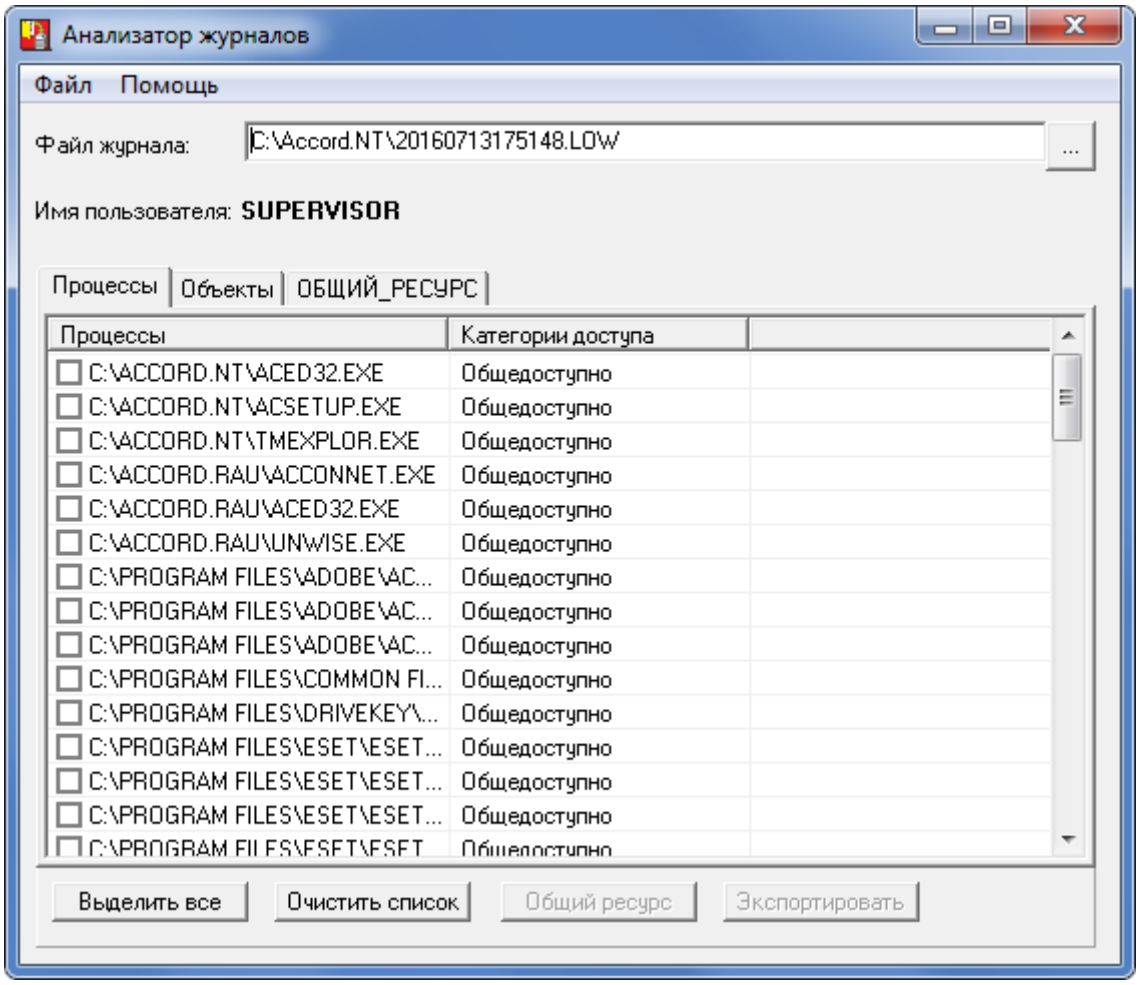

Рисунок 75 - Главное окно программы AcProc.exe. Выбор процесса

7)проанализировать, к каким объектам производилось обращение со стороны процессов с запросами на создание, открытие на запись или на чтение/запись. Для этого следует нажать кнопку «Общий ресурс» и просмотреть необходимые объекты (короткие имена объектов учитывать не нужно) (рисунок 76);

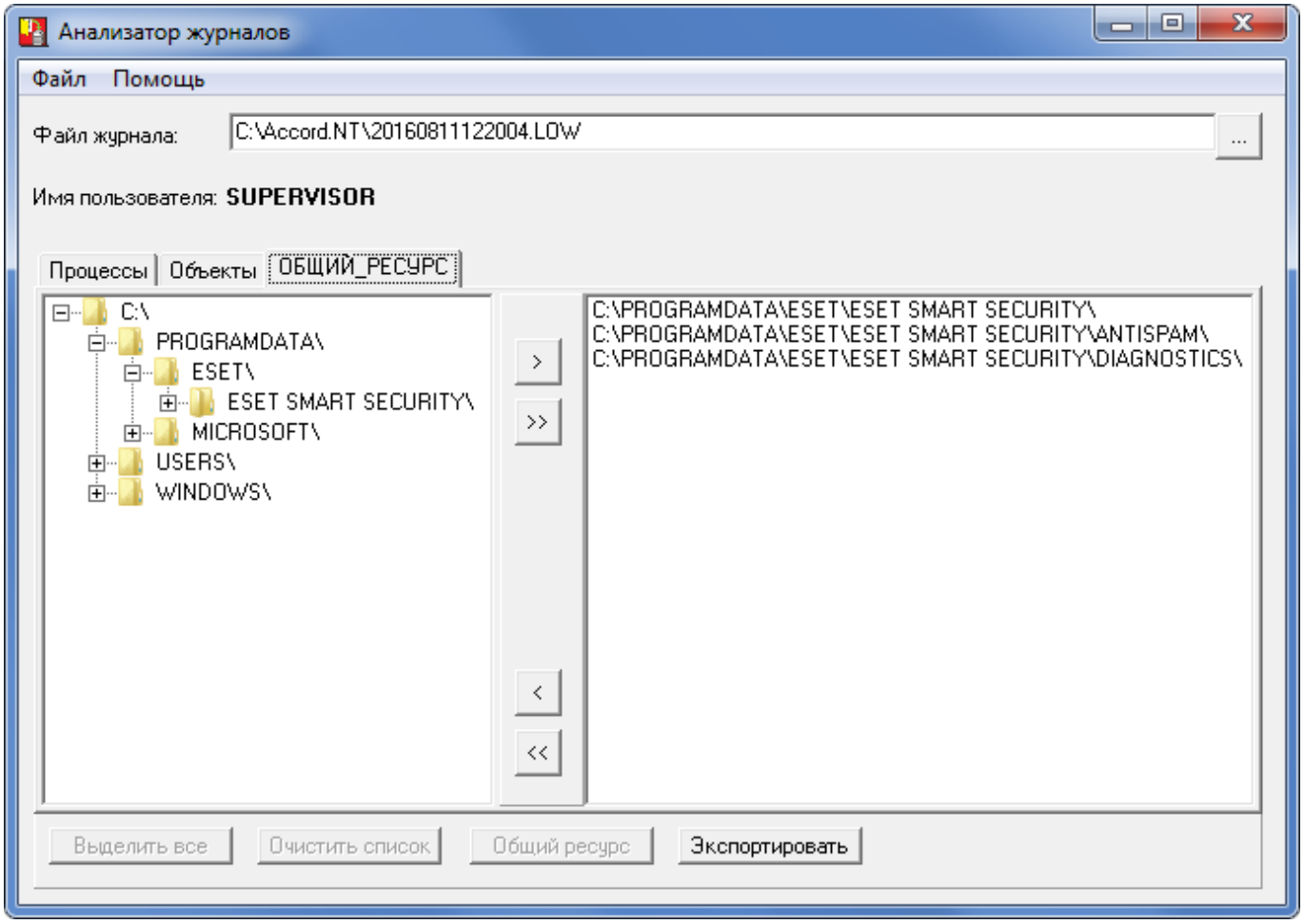

Рисунок 76 - Выбор имени процесса для анализа

8) сохранить объекты, к которым обращались процессы. Для этого нужно нажать кнопку <Экспортировать> (рисунок 76). При нажатии кнопки на экране появляется окно, в котором нужно указать путь, имя файла (например, «SUPERVISOR.PRD») и нажать кнопку <Сохранить> (рисунок 77).

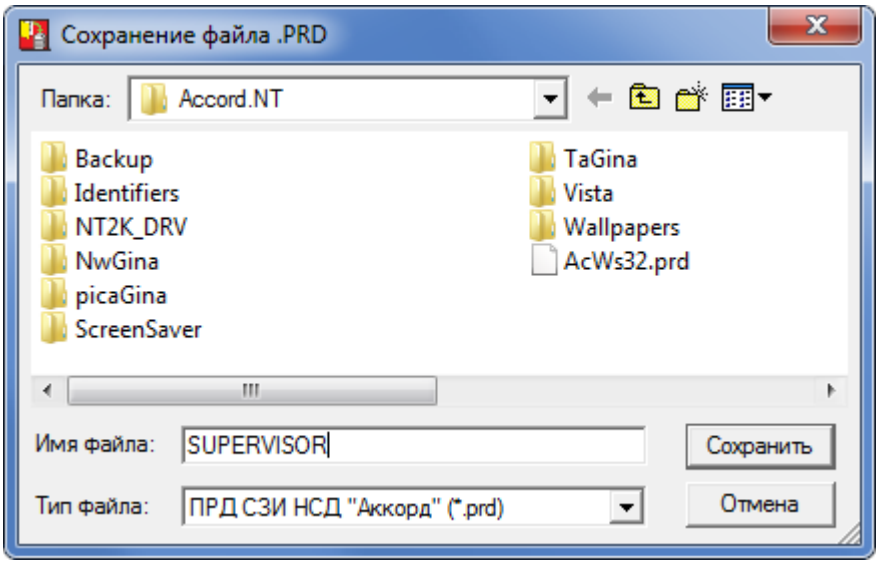

Рисунок 77 - Сохранение файла объектов, к которым обращался процесс Winword.exe

9)запустить редактор прав доступа Aced32.exe (Пуск\Программы\Аккорд\Редактор прав доступа\ Команды \Импортировать мандатные метки), затем выбрать файл «SUPERVISOR.PRD»;

10) на экране появляется окно, в котором отображается список каталогов и файлов, к которым обращались выбранные процессы (рисунок 78);

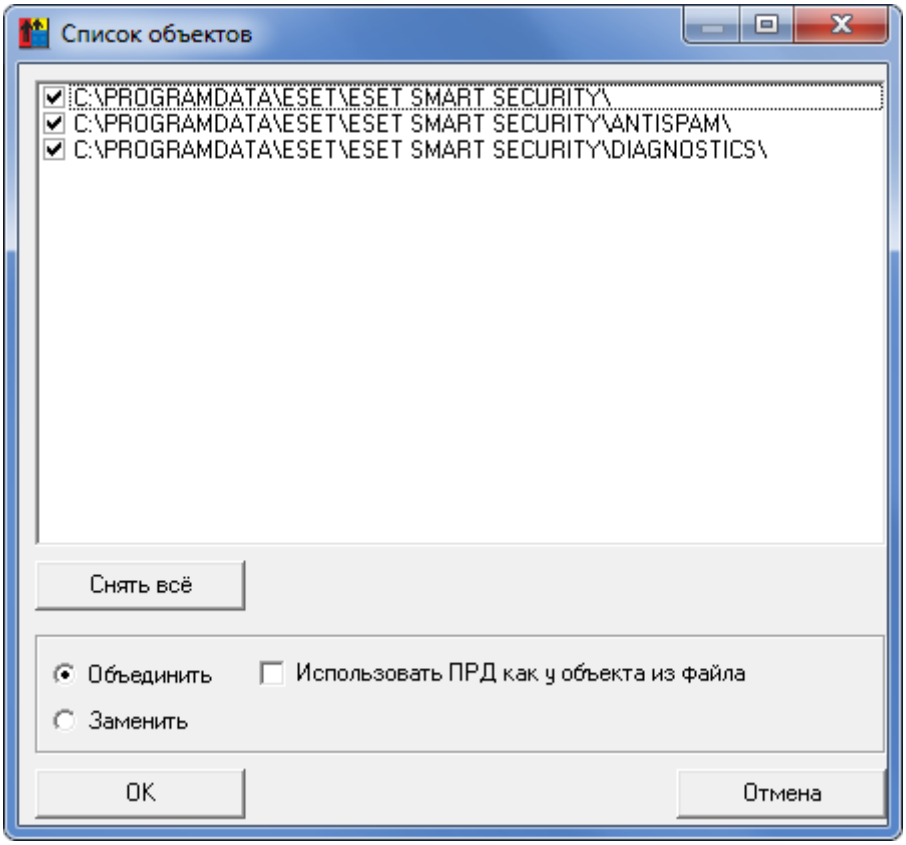

Рисунок 78 - Список объектов, к которым обращались анализируемые процессы

11) в окне 78 необходимо нажать кнопку <Снять все>, отметить объекты с учетом вложенности каталогов и нажать кнопку <OK>.

Для Microsoft Office 2007, например, это следующие объекты:

- C:\PROGRAMDATA\MICROSOFT\OFFICE\DATA\OPA12.DAT;
- C:\USERS\TEST\APPDATA\LOCAL\MICROSOFT\OFFICE\;
- C:\USERS\TEST\APPDATA\LOCAL\MICROSOFT\WINDOWS\CACHES\;
- C:\USERS\TEST\APPDATA\LOCAL\MICROSOFT\WINDOWS\EXPLORER\;
- C:\USERS\TEST\APPDATA\LOCAL\MICROSOFT\WINDOWS\WINDOWSUPDATE.LOG;
- C:\USERS\TEST\APPDATA\ROAMING\;
- C:\WINDOWS\DEBUG\WIA\WIATRACE.LOG;
- C:\USERS\TEST\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET FILES\CONTENT.MSO.

Для Microsoft Office 2010:

- C:\USERS\TEST\APPDATA\LOCAL\MICROSOFT\OFFICE\;

- C:\USERS\TEST\APPDATA\LOCAL\MICROSOFT\WINDOWS\CACHES\;
- C:\USERS\TEST\APPDATA\LOCAL\MICROSOFT\WINDOWS\EXPLORER\;
- C:\USERS\TEST\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET FILES\;
- C:\USERS\TEST\APPDATA\LOCAL\TEMP\;
- C:\USERS\TEST\APPDATA\ROAMING\MICROSOFT\OFFICE\;
- C:\USERS\TEST\APPDATA\ROAMING\MICROSOFT\TEMPLATES\;
- C:\USERS\TEST\APPDATA\ROAMING\MICROSOFT\UPROOF\.

12) в редакторе ПРД для пользователя необходимо в поле «Детальность журнала» установить уровень детальности журнала, назначенный для пользователя до момента установки уровня «Сбор статистики» (в общем случае рекомендуется установить уровень – «Низкий»).

В том случае, когда администратор не имеет возможности собрать полный список процессов, но точно знает, какая программа будет работать со сведениями ограниченного доступа, он может добавить в список процесс «*» (звездочка). При проверке грифа, если процесс явно не прописан в списке, ему будет присвоен тот уровень, что установлен для объекта «*». В общем случае это будет самый низкий гриф.

В ряде случаев возникает необходимость добавления в «белый» список часто обновляющихся процессов, версии которых имеют однотипные названия (например, отличающиеся только цифрой). Чтобы добавить процессы с похожими именами в «белый» список, необходимо в конце имени процесса добавить знак «*».

Таким образом, при добавлении в «белый» список процесса «Process Name*» в список процессов автоматически добавляются все процессы, имена которых начинаются с «Process Name». При этом расширение процессов может быть любым.

При добавлении в список процессов элемента «Process Name*.exe» в список процессов автоматически добавляются все процессы, имена которых начинаются с «Process Name» и имеют расширение .exe.

Еще один вариант работы с разными уровнями процессов – это **выбор уровня доступа сессии пользователя**. При задании уровня доступа пользователя (рисунок 65) Администратор БИ может установить флаг «Предлагать выбор уровня конфиденциальности сессии». Действует этот флаг так же, как выбор уровня для отдельных процессов, но запрос выводится при начале сеанса работы пользователя. Если не включен флаг «Строгая установка уровня сессии», то пользователь может отказаться от выбора уровня сессии и в процессе работы выбирать только уровень отдельных программ при их запуске. Выбор уровня сессии в таком «мягком» режиме определяет фиксацию уровня только тех процессов, для которых администратор включил флаг «Разрешено понизить пользователю» на уровне сессии. Для остальных процессов уровни доступа не меняются и будут соответствовать фиксированным значениям, прописанным в списке процессов редактора ПРД.

Если включен флаг «Строгая установка уровня сессии», то пользователь обязан выбрать уровень сессии в начале сеанса работы, и ВСЕМ ПРОЦЕССАМ присваивается уровень доступа не выше уровня сессии. Так, например, пользователю <USER01> присвоен уровень доступа «Секретно», основной массе процессов установлен уровень «Общедоступно», а некоторым процессам – уровень «Секретно». При выборе уровня сессии «Конфиденциально» процессы уровня «Секретно» получат уровень «Конфиденциально», а для всех остальных процессов уровень не изменится.

Флаги «Предлагать выбор уровня конфиденциальности сессии» и «Строгая установка уровня сессии» доступны в окне выбора уровня доступа пользователя только при включенном механизме контроля процессов.

В СПО «Аккорд» имеется **возможность отмены проверки ПРД для 0 сессии**, т.е. для учетной записи пользователя, в чьи обязанности входит процедура запуска СВТ (например, пользователь Boot-start или Startup-пользователь).

Чтобы отменить проверку ПРД для 0 сессии, необходимо в файле Accord.ini ключу Check0Session в секции [Terminal Server] установить значение «No».

Отменить проверку ПРД для 0 сессии можно как в терминальном режиме, так и в локальном.

7.12.3. Создание «белого» списка процессов с помощью мандатного и/или дискреционного механизма разграничения доступа с контролем процессов и динамического контроля целостности файлов из этого списка

7.12.3.1. Формирование списков процессов с помощью мандатного и/или дискреционного механизма разграничения доступа с контролем процессов

Формирование списков процессов выполняется в соответствии со следующим порядком:

1)запустить утилиту «Настройка комплекса «Аккорд» (Программы\Аккорд\Настройка комплекса Аккорд);

2)в главном окне программы установить необходимые флаги («Контроль процессов», «Дискреционный» и/или «Мандатный») (рисунок 79);

ВНИМАНИЕ! Контроль процессов может осуществляться только совместно с одним или несколькими механизмами разграничения доступа (дискреционным и/или мандатным).

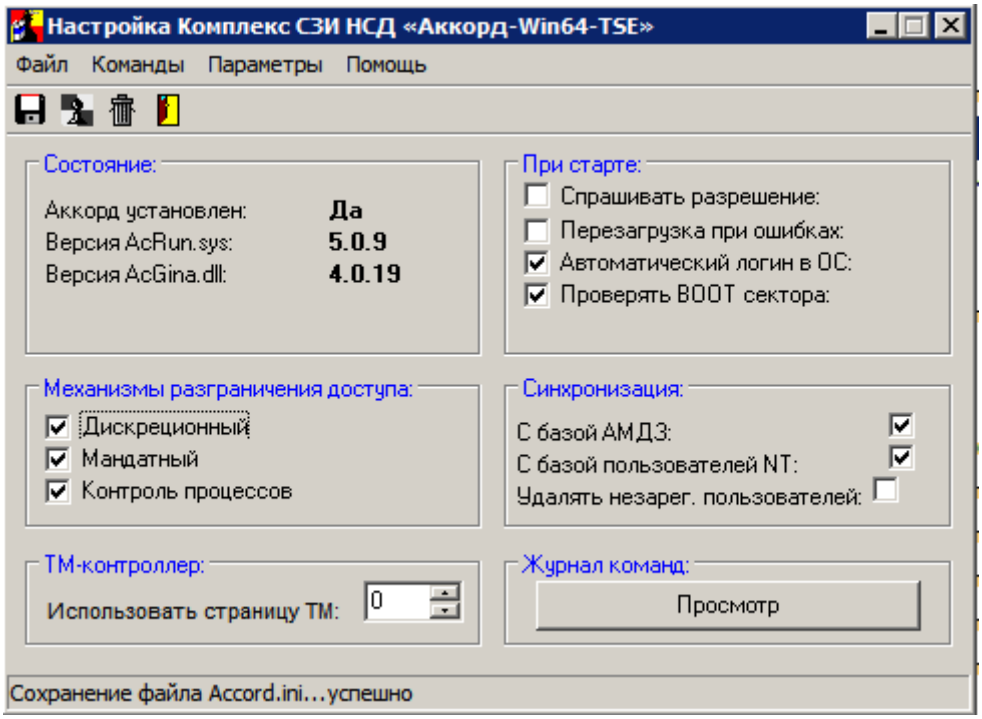

Рисунок 79 – Главное окно утилиты «Настройка комплекса Аккорд»

3) завершить работу приложения с сохранением изменений;

4) запустить утилиту «Редактор прав доступа» (Программы\Аккорд\Редактор прав доступа), в которой установить уровень детальности журнала «Сбор статистики» для одного из пользователей, входящего в состав группы пользователей СПО «Аккорд», с использованием учетной записи которого будут формироваться списки. При этом пользователю автоматически присваивается высокий уровень детальности журнала, а его работа выполняется в мягком режиме;

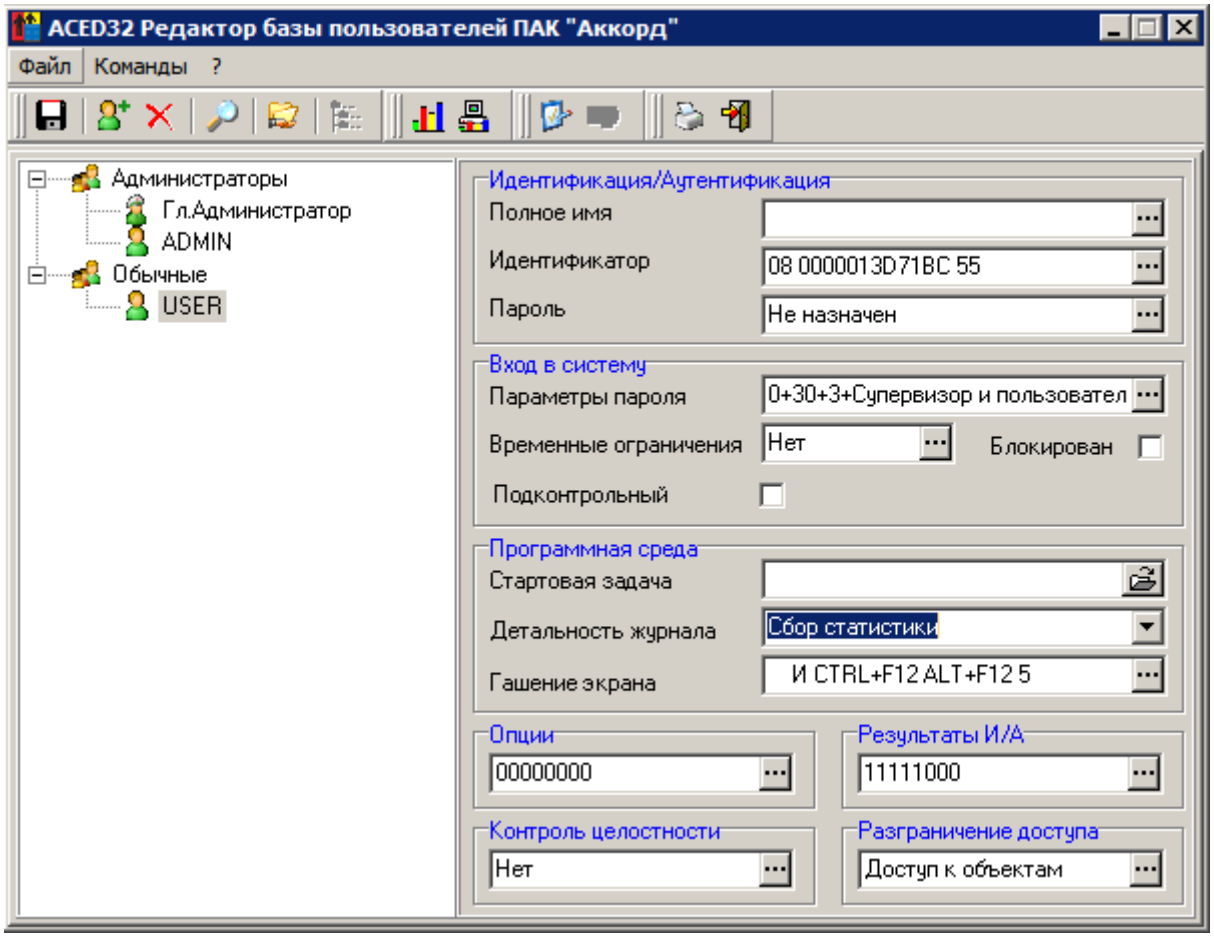

Рисунок 80 - Установка уровня детальности журнала «Сбор статистики»

Вместо уровня «Сбор статистики» можно установить уровень детальности «Высокая». Однако **в этом случае необходимо установить флаг «Мягкий режим»** в программе настройки комплекса «Аккорд».

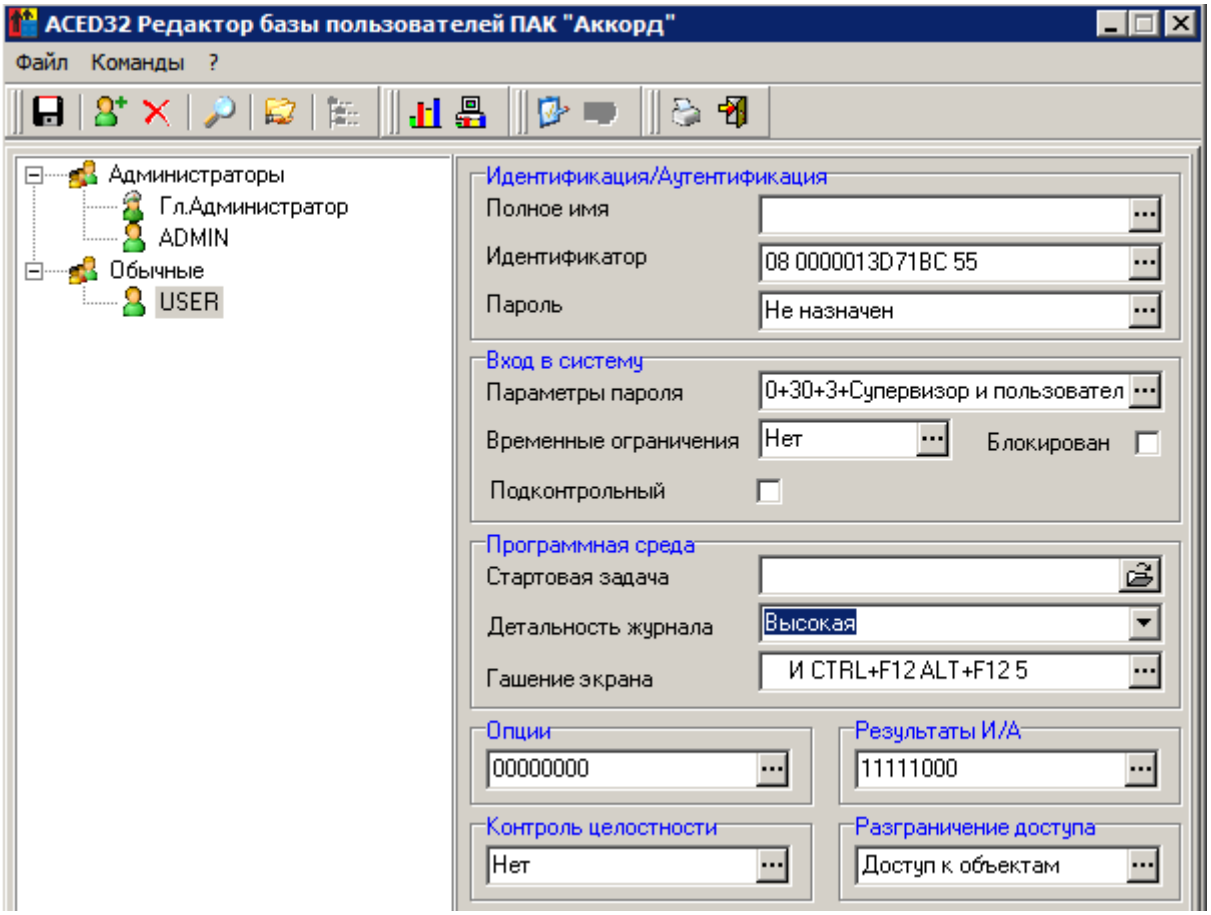

Рисунок 81 - Установка уровня детальности журнала «Высокая»

Для этого в главном окне программы настройки комплекса «Аккорд» необходимо в меню «Параметры» выбрать пункт «Дополнительные опции...».

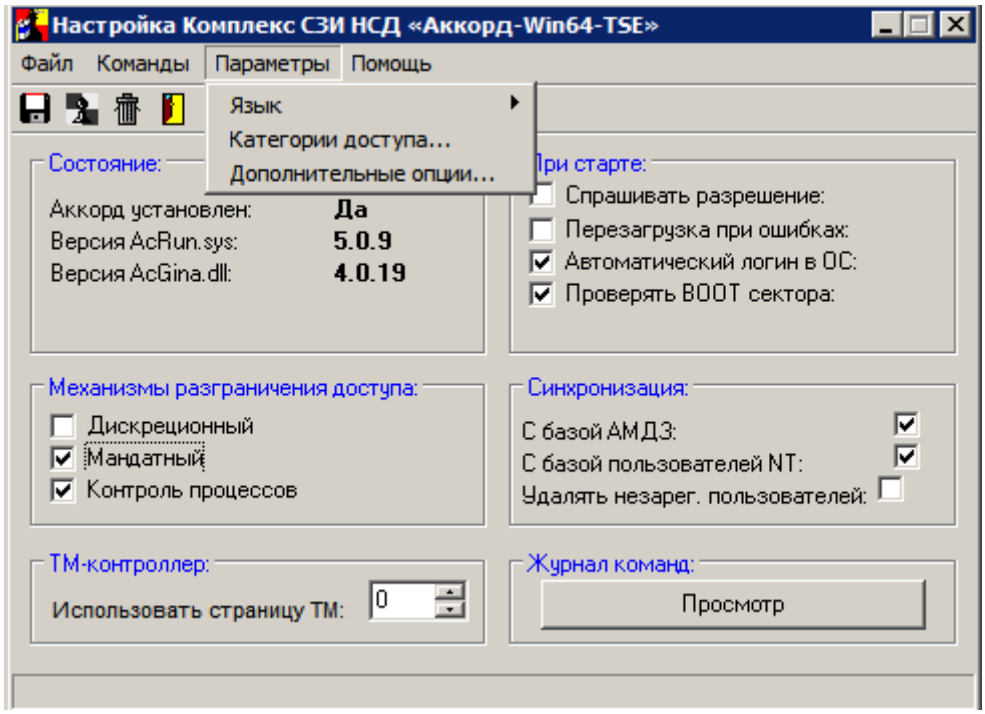

Рисунок 82 - Главное окно программы настройки комплекса «Аккорд»

На вкладке «Разное» открывшегося окна установки дополнительных опций следует установить флаг «Мягкий режим».

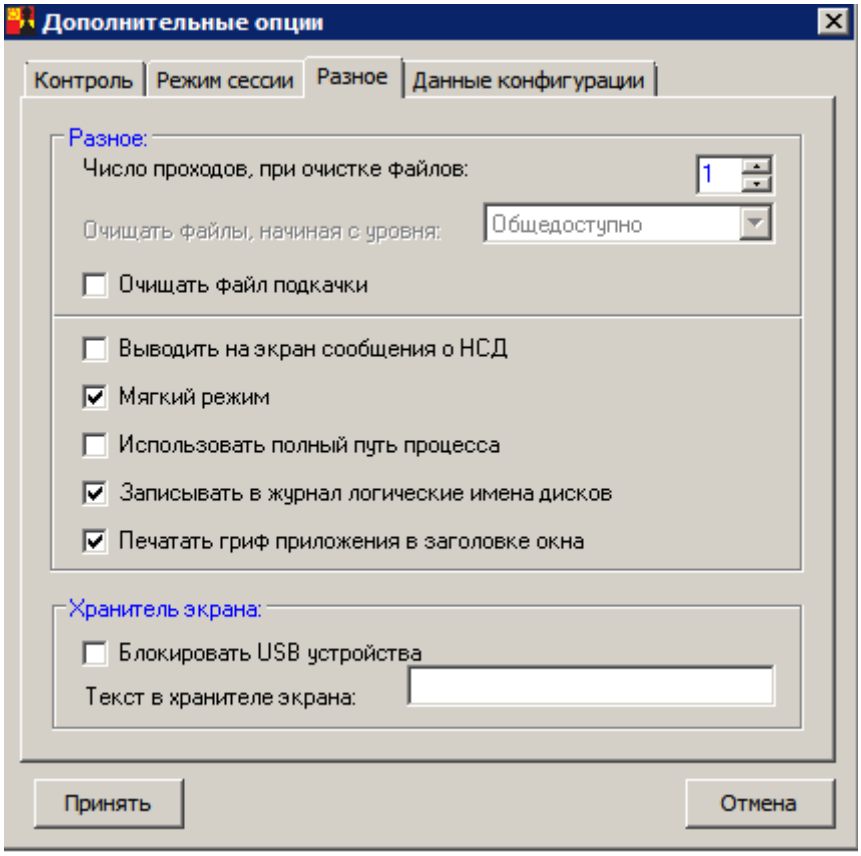

Рисунок 83 - Установка опции «Мягкий режим»

5)запустить сеанс работы от имени пользователя, для которого проводились описанные выше настройки. При использовании режима «Сбор статистики» после успешного выполнения процедуры аутентификации на экран выводится дополнительное сообщение. По истечении времени, указанного в данном окне, необходимо нажать кнопку <OK>, которая станет активна;

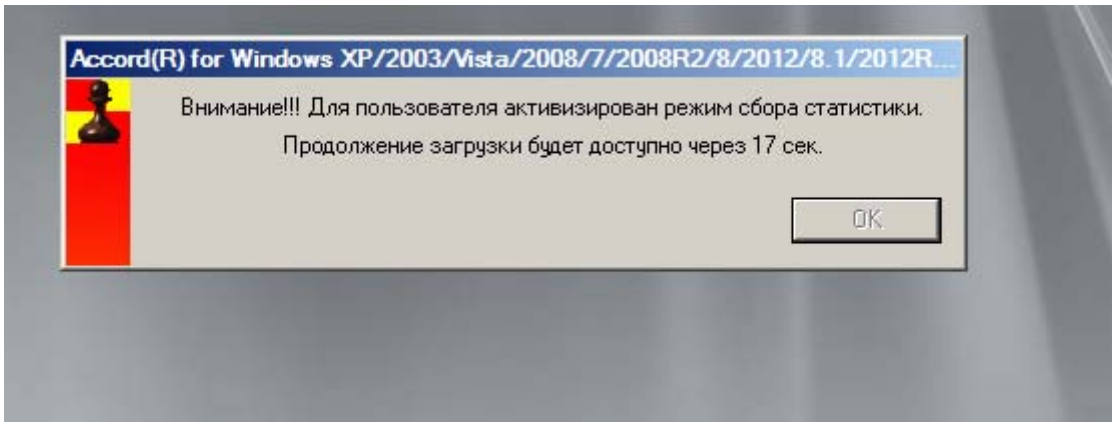

Рисунок 84 - Информационное сообщение

6)выполнить работу с приложениями (запустить все необходимые процессы), необходимыми для выполнения должностных обязанностей пользователя;

7)завершить сеанс пользователя[9], запустить от имени Администратора СПО «Аккорд» программу AcProc.exe (Программы\Аккорд\Создание списка процессов из журналов регистрации, рисунок 85);

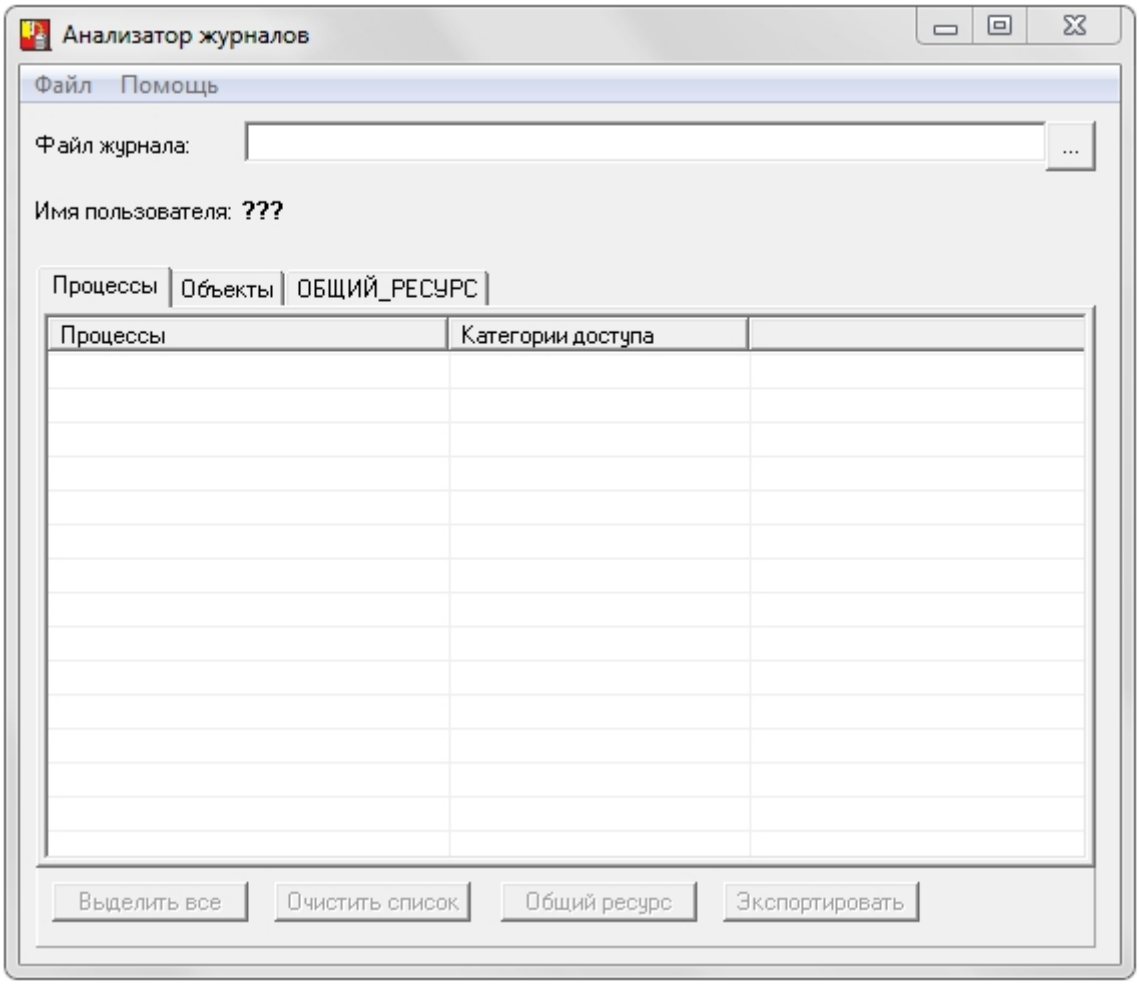

Рисунок 85 – Главное окно утилиты AcProc.exe

8)во вкладке «Процессы» загрузить журнал последнего сеанса работы пользователя: в окне программы AcProc.exe (рисунок 85) нажать на раскрывающийся список в поле «Файл журнала», далее в появившемся окне (рисунок 86) выбрать файл журнала (или несколько файлов);

[9)] По завершении сеанса работы пользователя на данном этапе можно вернуть для него первоначальные настройки уровня детальности журнала, установленные до начала процедуры формирования белого списка процессов (в общем случае рекомендуется установить уровень – «Низкий»)

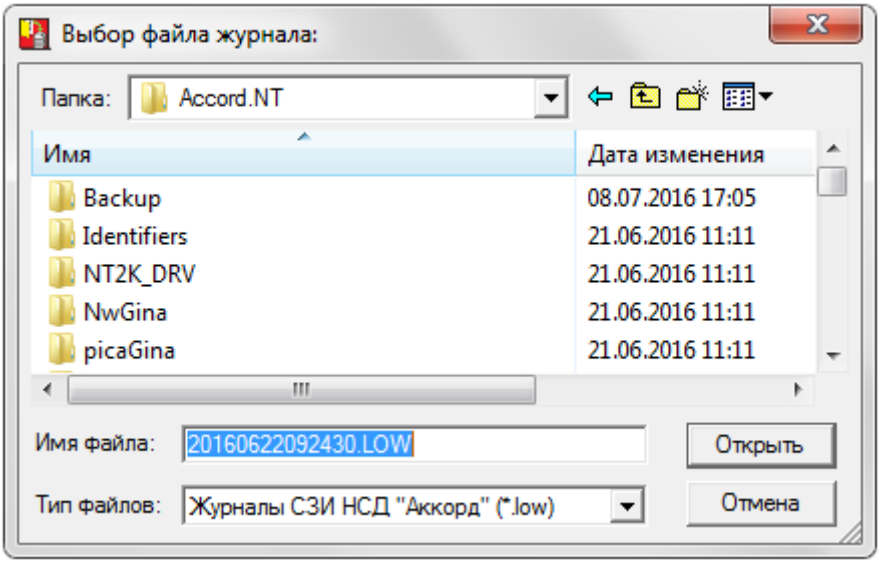

Рисунок 86 - Выбор файла журнала регистрации событий

9)в главном окне программы AcProc.exe выбрать процессы, которые необходимы для выполнения должностных обязанностей пользователя, и нажать кнопку <Экспортировать> (рисунок 87);

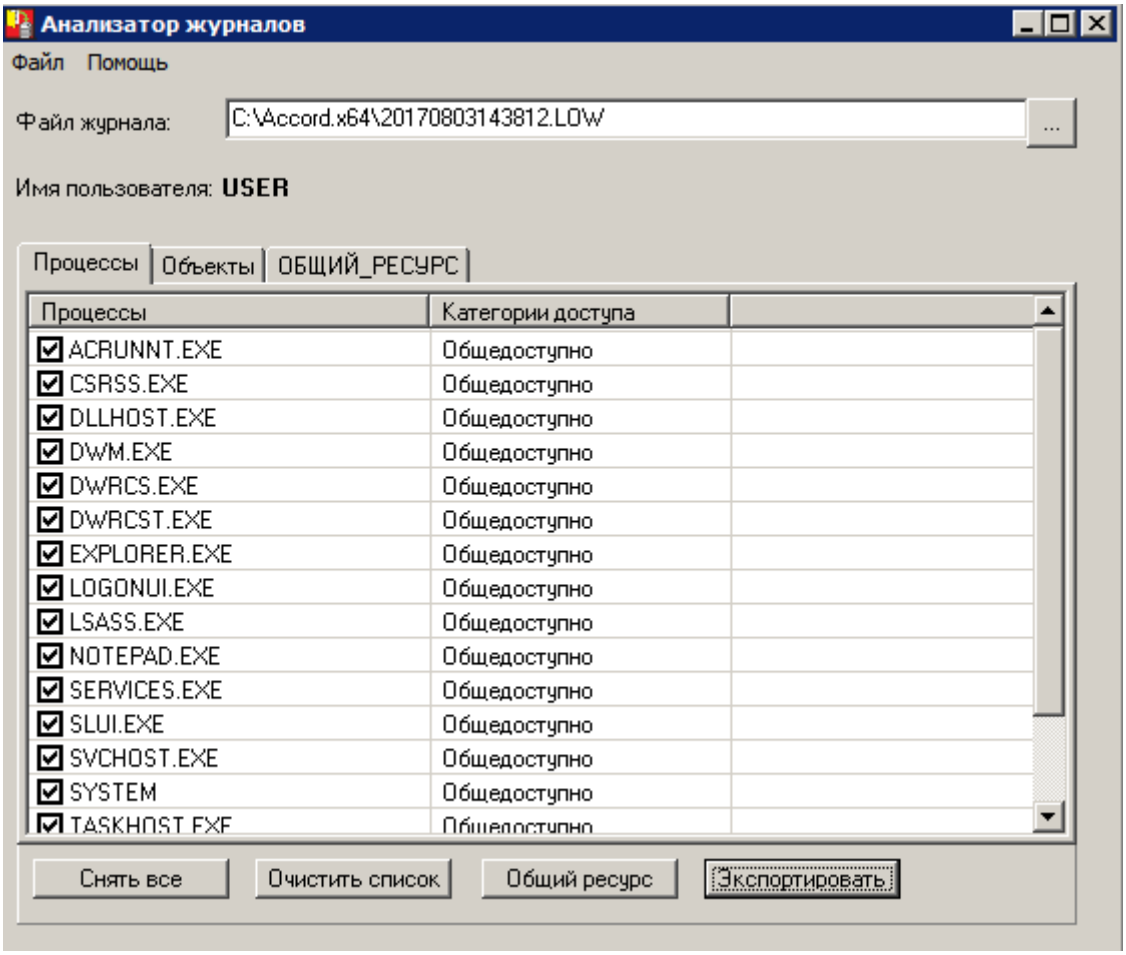

Рисунок 87 - Главное окно программы AcProc.exe. Выбор процессов

10) в появившемся окне нажать кнопку <Сохранить> (по умолчанию имя файла соответствует имени учетной записи пользователя, для которого формируется список процессов, однако при необходимости можно изменить имя файла, рисунок 88);

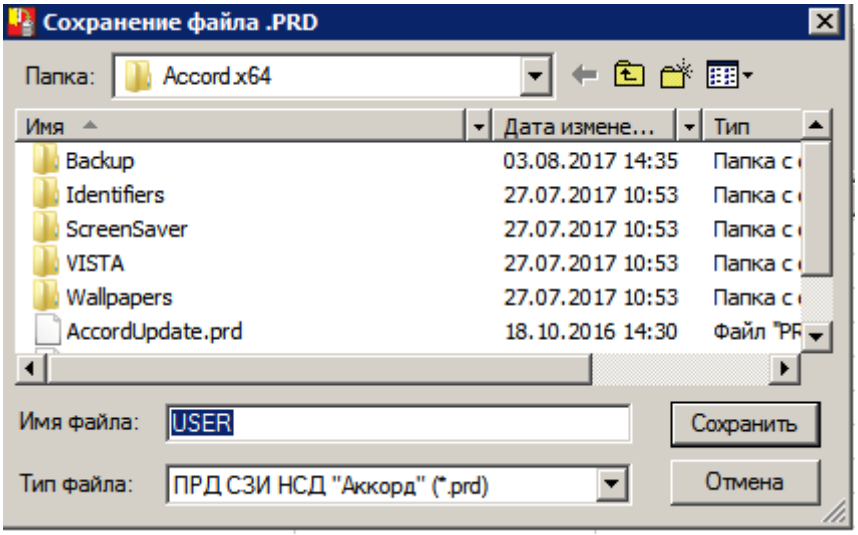

Рисунок 88 – Сохранение процессов в файл .prd

11) в главном окне программы AcProc.exe перейти во вкладку «Объекты» и сохранить список объектов, к которым обращался пользователь во время выполнения должностных обязанностей, нажав кнопку <Экспортировать> (рисунок 89);

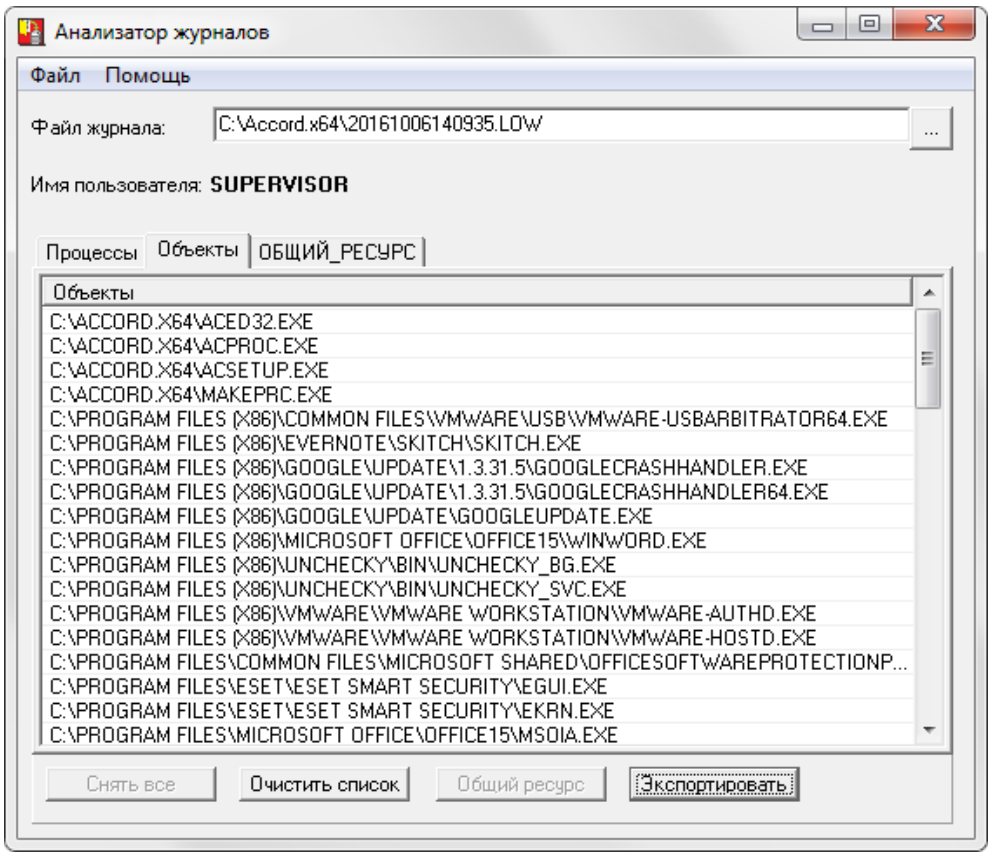

Рисунок 89 – Главное окно программы AcProc.exe. Вкладка «Объекты»

12) в появившемся окне следует нажать кнопку <Сохранить> (по умолчанию имя файла соответствует имени учетной записи пользователя, для которого формируется список объектов, однако при необходимости можно изменить имя файла, рисунок 90);

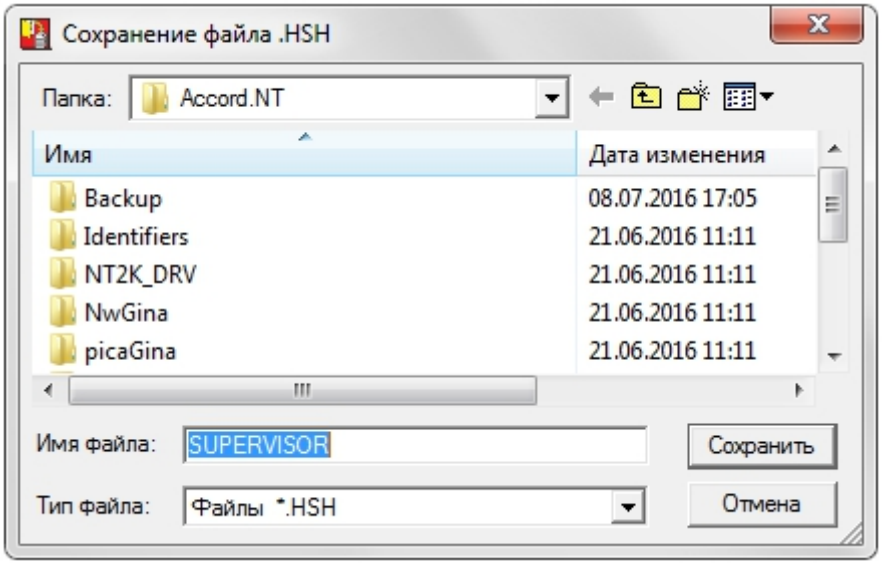

Рисунок 90 – Сохранение объектов в файл .hsh

13) затем необходимо вновь запустить утилиту «Редактор прав доступа» (Программы\Аккорд\Редактор прав доступа) и выбрать меню Файл\Импорт ПРД (рисунок 91);

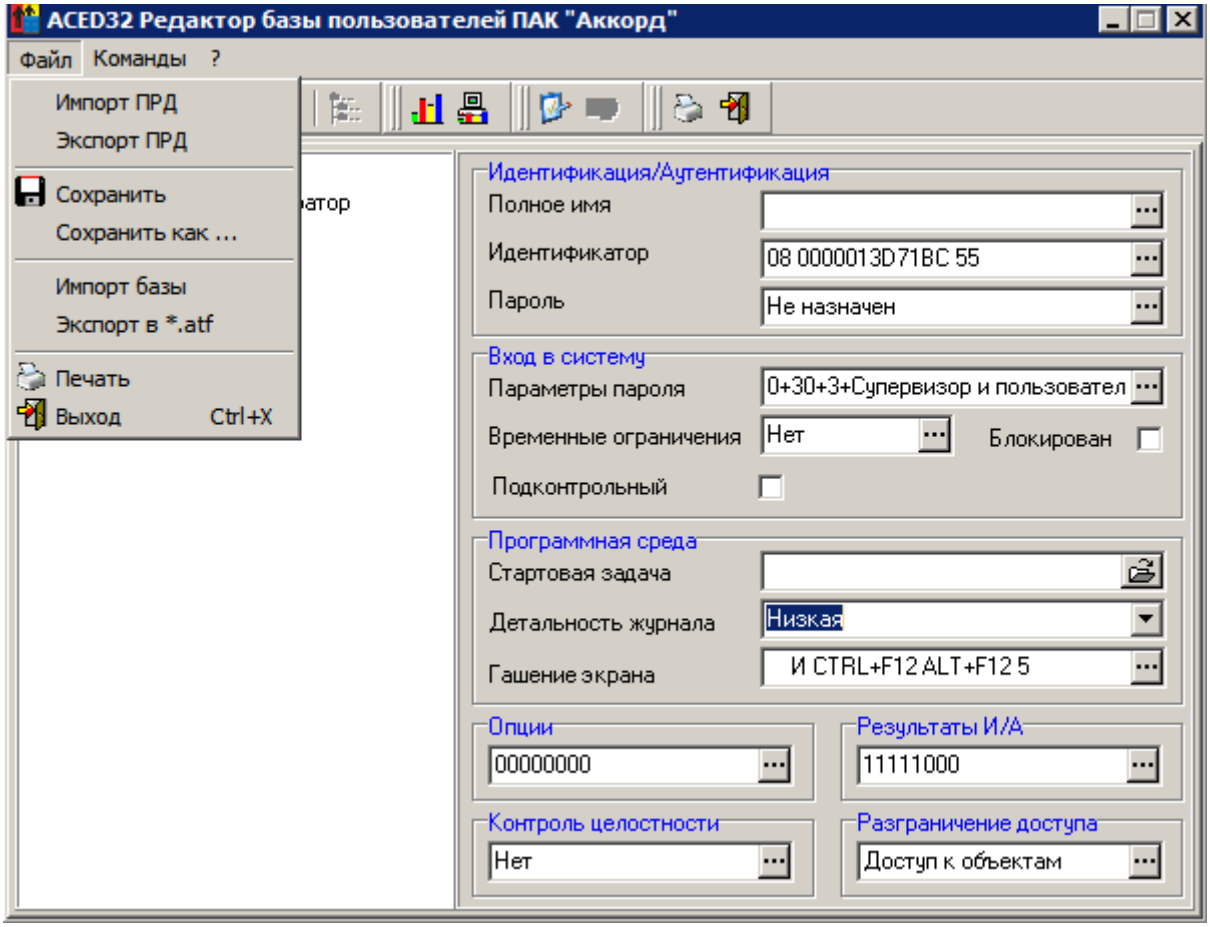

Рисунок 91 – Импорт ПРД

14) после этого на экране появляется окно выбора файла со списком процессов (рисунок 92);

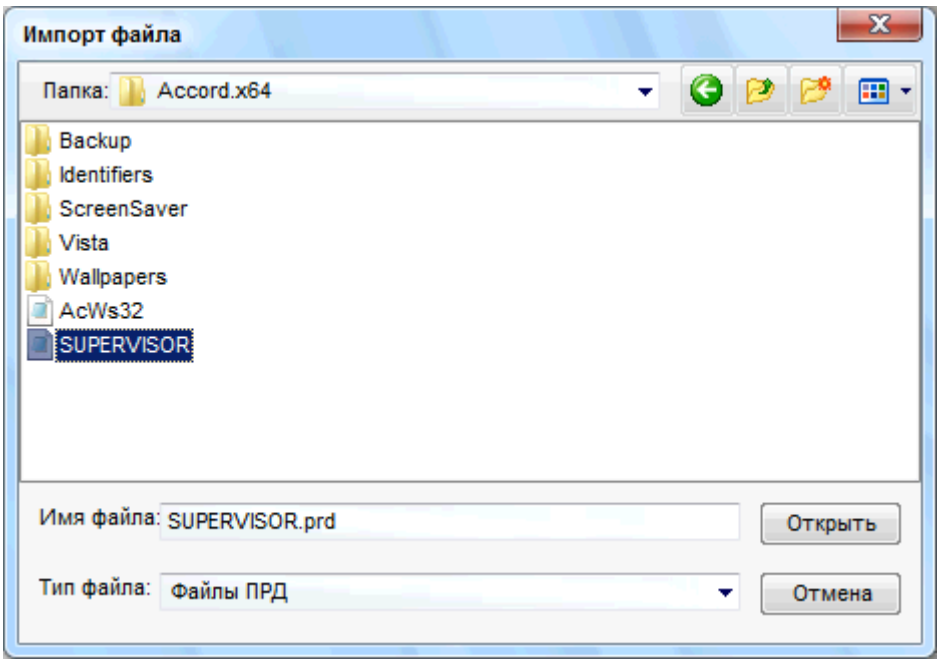

Рисунок 92 – Окно выбора файла со списком процессов

15) необходимо выбрать файл (рисунок 92) и нажать кнопку <Открыть>;

16) в появившемся окне следует установить флаг «Для процессов» и нажать кнопку <Импорт> (рисунок 93);

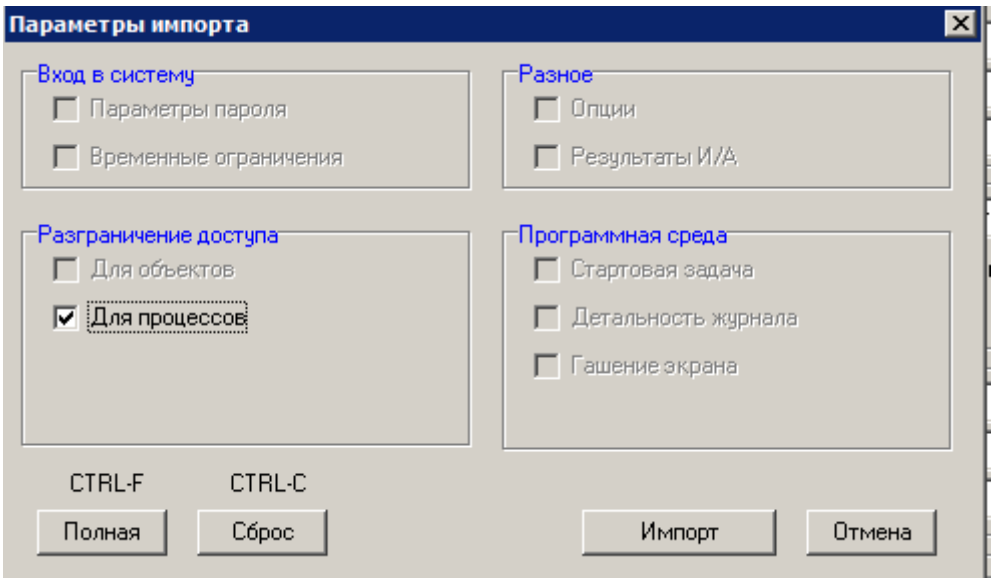

Рисунок 93 – Параметры импорта

17) в появившемся далее окне со списком импортированных процессов (рисунок 94) следует отметить необходимые (или же выбрать все процессы, нажав кнопку <Выбрать все>), а также (в случае необходимости) отметить флаги, показанные внизу окна на рисунке 94, и нажать кнопку <OK>. Убедиться в корректности выполнения процедуры импорта, нажав на кнопку <...> в поле «Разграничение доступа» главного окна программы ACED32;

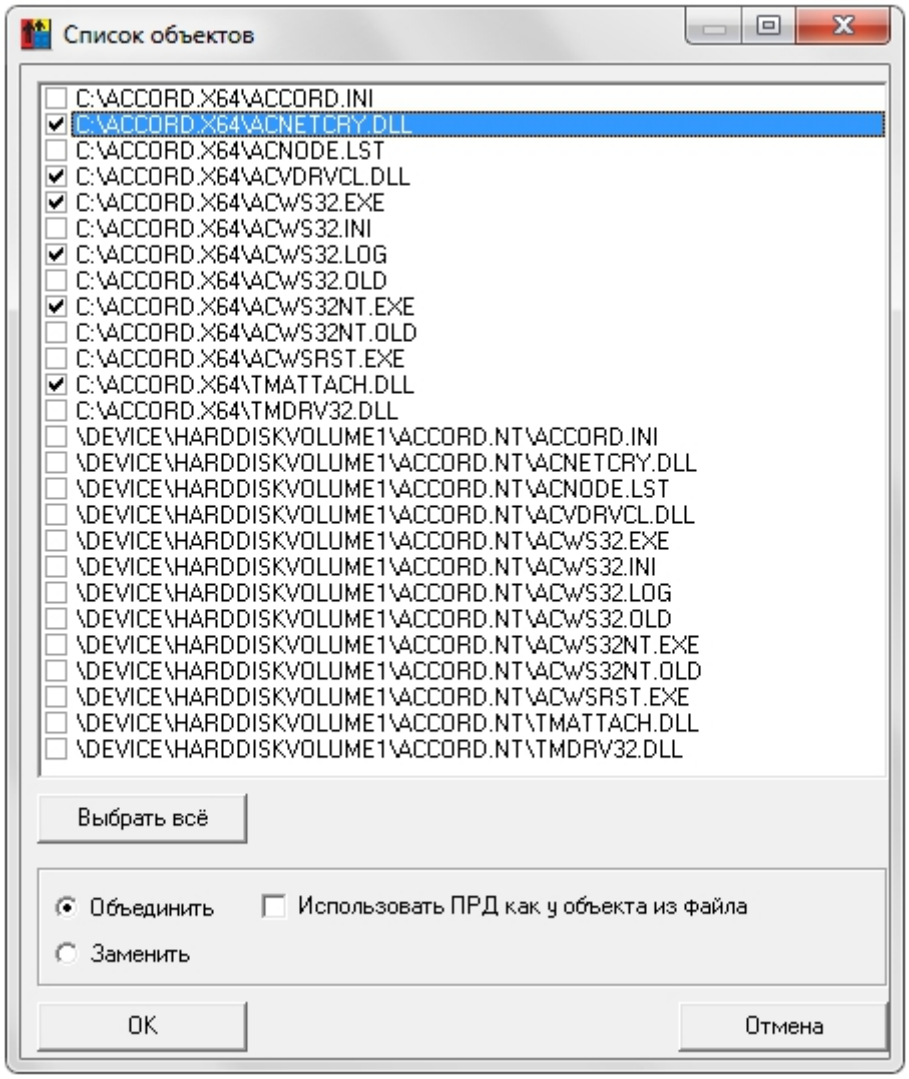

Рисунок 94 – Список импортированных процессов

18) в меню разграничения доступа для пользователя следует установить импортированным процессам соответствующие уровни доступа (при выполнении мандатного механизма разграничения доступа, рисунок 95), а также убедиться, что все необходимые процессы включены в список для контроля (при выполнении дискреционного механизма разграничения доступа, рисунок 96);

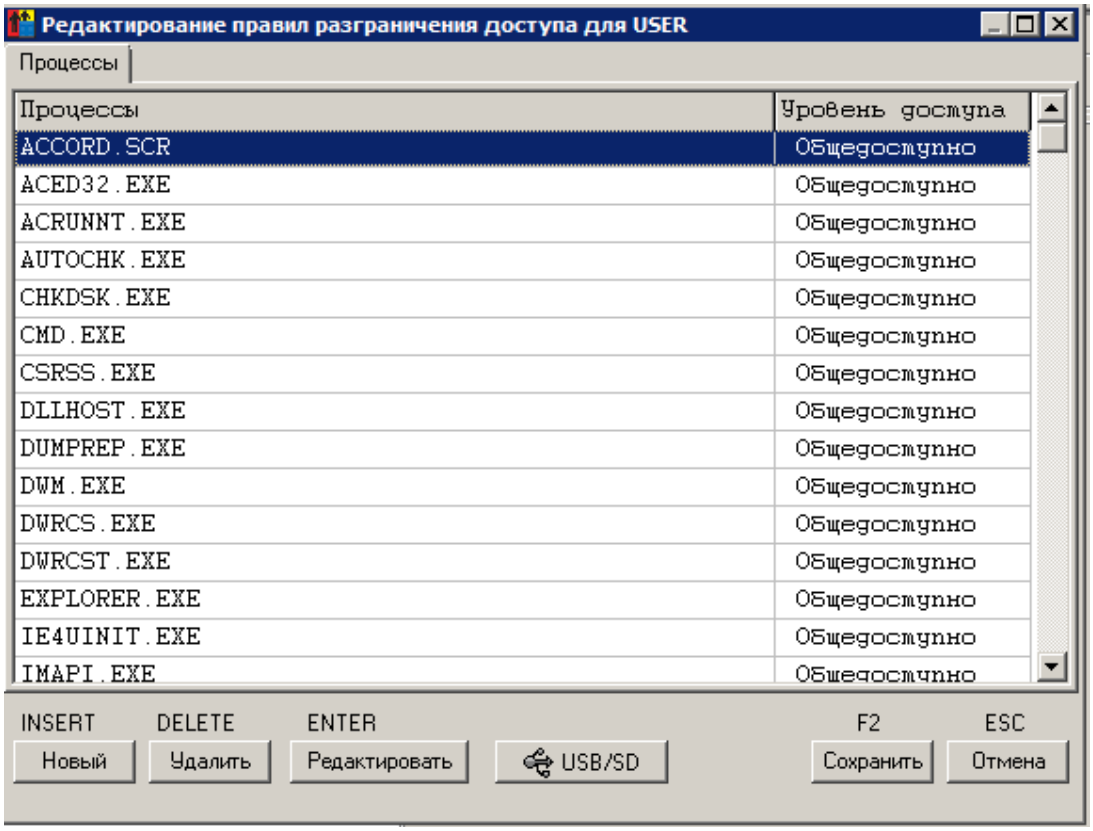

Рисунок 95 – Список импортированных процессов (мандатный механизм разграничения доступа)

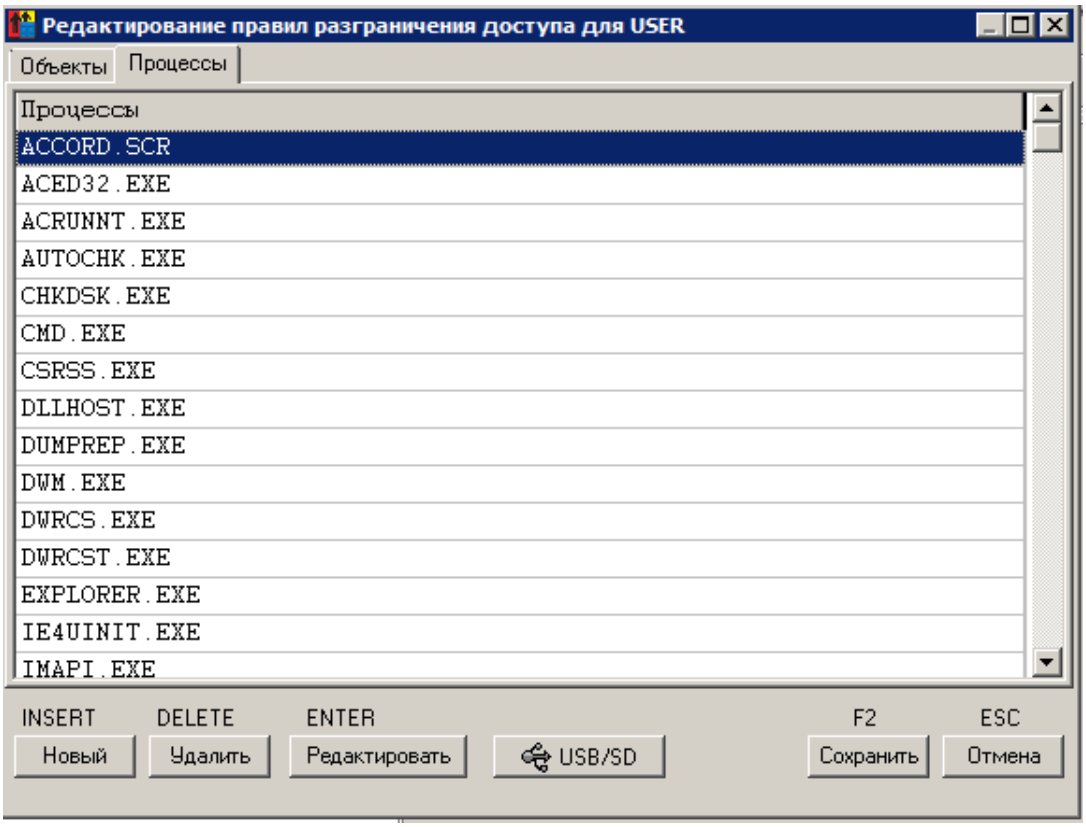

Рисунок 96 - Список импортированных процессов (дискреционный механизм разграничения доступа)

7.12.3.2. Установка динамического контроля целостности файлов из сформированного списка

19) в главном окне редактора прав доступа перейти в меню «Контроль целостности»;

20) в появившемся окне перейти во вкладку «Динамический» и нажать кнопку <Загрузить> (рисунок 97);

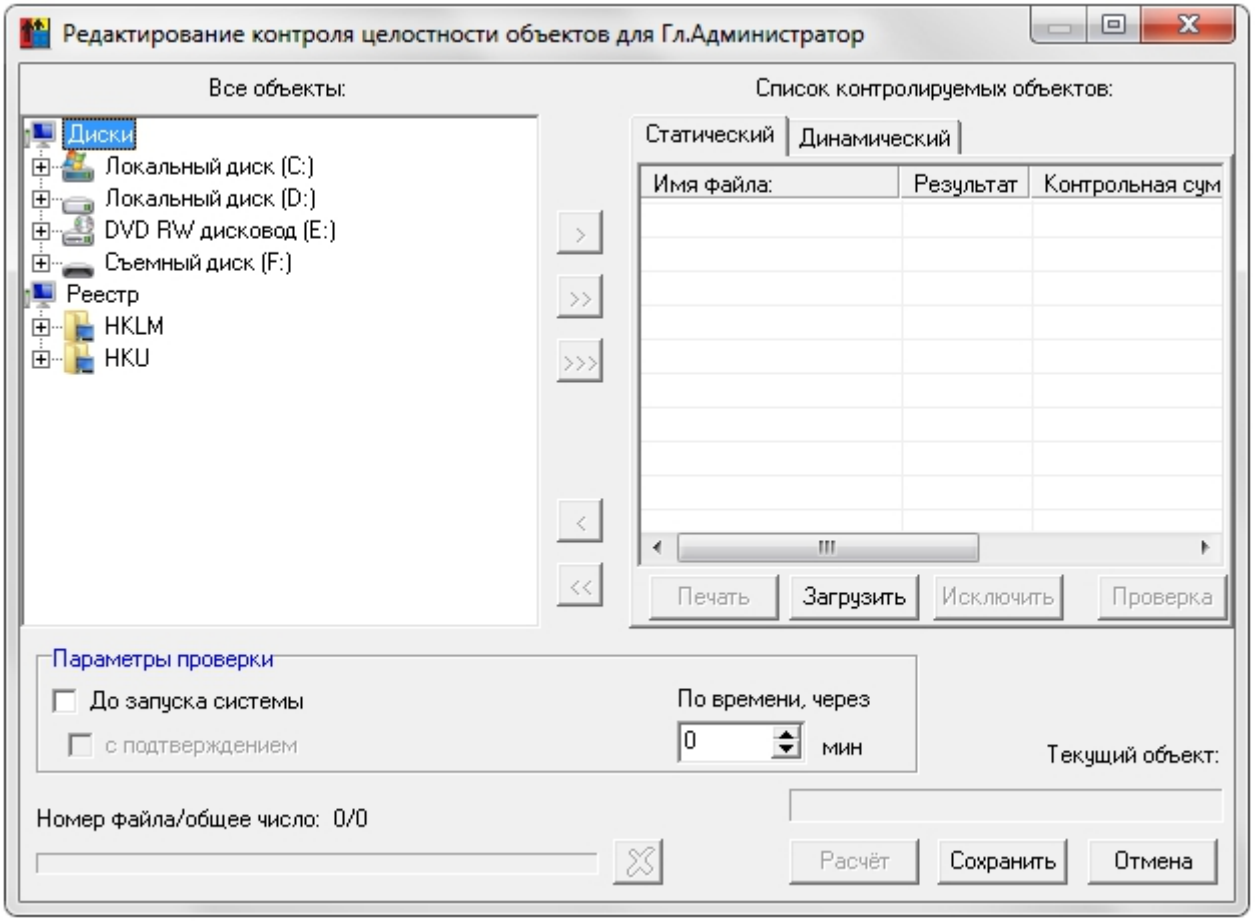

Рисунок 97 – Редактирование списков для контроля целостности пользователя

21) при нажатии кнопки появляется окно выбора файла (рисунок 98). Необходимо выбрать файл со списком импортированных объектов, с которыми работал пользователь при выполнении должностных обязанностей (файл .hsh), и нажать кнопку <Открыть>;

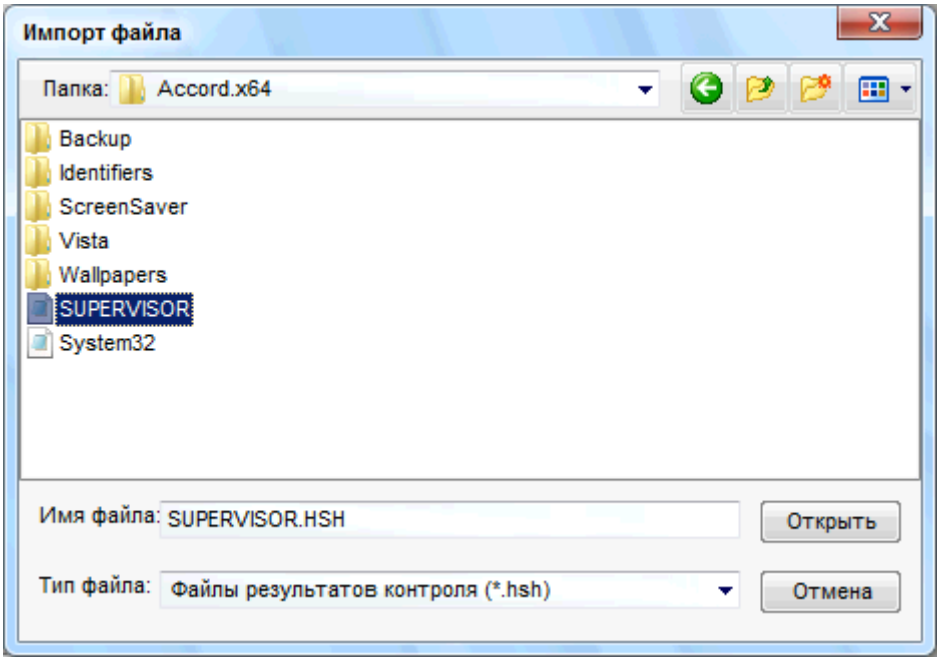

Рисунок 98 – Импорт файла со списком импортированных объектов

22) окно для редактирования списков для контроля целостности примет следующий вид (рисунок 99):

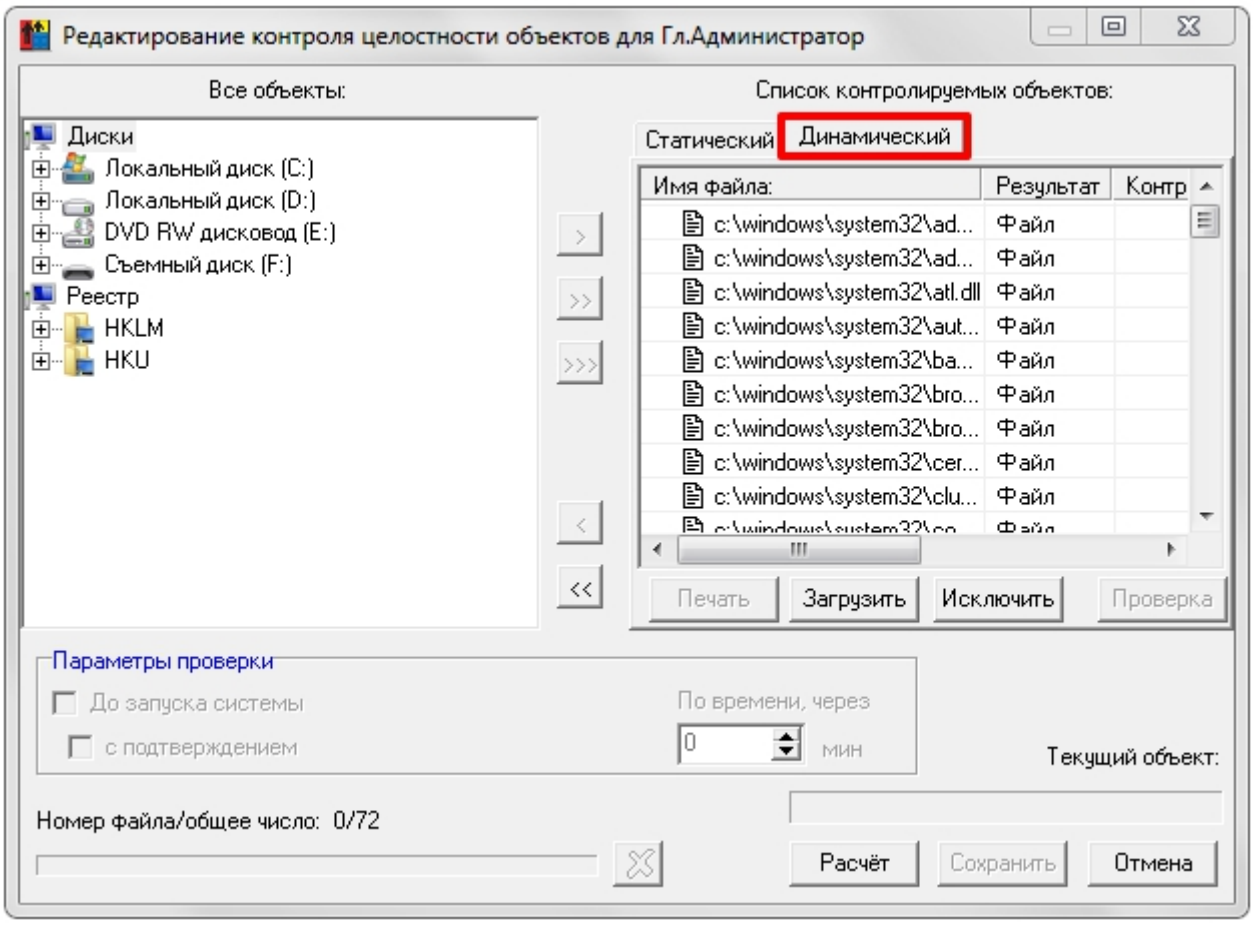

Рисунок 99 - Редактирование списков для контроля целостности. Импорт списка контролируемых объектов

23) необходимо выбрать объекты и нажать кнопку <Расчет> (рисунок 99);

24) на запрос идентификатора предъявить идентификатор пользователя, для которого выполняется процедура редактирования контроля целостности объектов;

25) в графе «Контрольная сумма» появляются эталонные значения КС (рисунок 100);

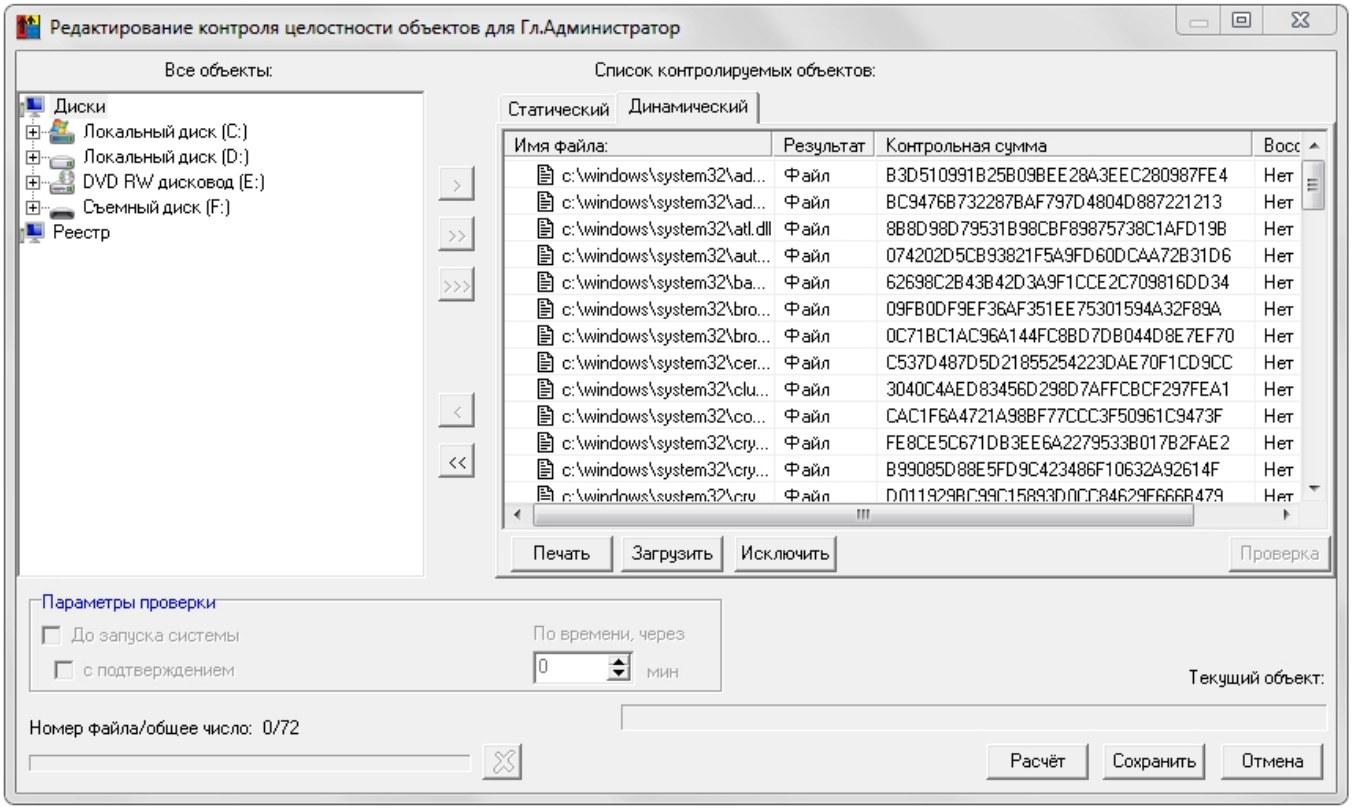

Рисунок 100 - Редактирование списков для контроля целостности. Контрольные суммы рассчитаны

26) по завершении процедуры расчета КС нажать кнопку <Сохранить> (рисунок 100).

По окончании всех настроек убедитесь в том, что в программе настройки комплекса «Аккорд» **снят флаг «Мягкий режим»** (рисунок 83).

После выполнения описанной последовательности действий для пользователя создается список разрешенных процессов, необходимых для выполнения его должностных обязанностей. Для каждого из процессов рассчитывается контрольная сумма и сохраняется в памяти идентификатора пользователя.

После запуска монитора разграничения доступа пользователю будут доступны только процессы из «белого» списка.

В случае несанкционированной модификации имени (при замене имени неразрешенного процесса именем разрешенного) процесс не запустится, так

как КС модифицированного процесса не совпадет с эталонным значением КС исходного, добавленного в список разрешенных, процесса.

Таким образом, возможность несанкционированного доступа к процессам исключается.

7.13.Установка опций настройки

В списке пользователей с помощью мыши или клавиатуры выделите пользователя.

В поле «Опции» окна «Параметры пользователя» (рисунок 2) отображается информация о том, какие дополнительные опции настройки системы «Аккорд» установлены у выделенного пользователя. Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «Опции», или клавишу <Enter>. На экран выводится окно «Опции» (рисунок 101).

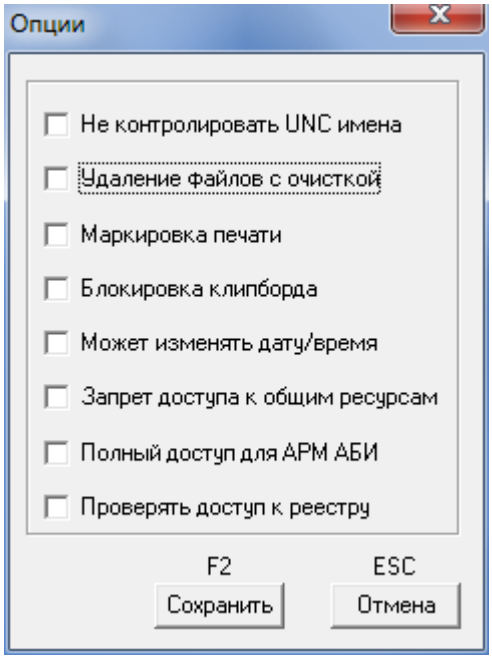

Рисунок 101 - Опции настройки

Дополнительные опции работы пользователя в СПО «Аккорд-Win64 K»:

- *Не контролировать UNC имена* – контроль уровня секретности информации, помещенной в буфер обмена при использовании мандатного доступа процессов;
- *удаление файлов с очисткой* – в процессе удаления файлов физическое место файла на жестком диске прописывается последовательностью случайных чисел. Следует учитывать, что при удалении файлов способом, подразумевающим перемещение их в корзину, невозможность их дальнейшего восстановления будет гарантирована только при последующем удалении их из корзины. Если требуется удаление с очисткой не всех файлов, а только с определенного уровня конфиденциальности, в главном окне программы настройки комплекса «Аккорд» в меню «Параметры» следует выбрать пункт «Дополнительные опции...», в котором на

закладке «Разное» (рисунок 83) активировать опцию «*Очищать файлы, начиная с уровня*» (работает при включенном механизме мандатного доступа);

- *маркировка печати* – включить для данного пользователя процедуру контроля вывода на печать и маркировки документов. Формат и состав параметров, выводимых на печатную копию, выполняется в программе «Настройка комплекса Аккорд»;
- *блокировка клипборда* – установка этого параметра позволяет блокировать буфер обмена в целях защиты информации от копирования;
- *может изменять дату/время* - разрешено ли пользователю изменять дату/время;
- *запрет доступа к общим ресурсам* – установка этого параметра запрещает доступ из сети к ресурсам данного компьютера, даже если они описаны в ОС как общие ресурсы;
- *полный доступ для АРМ АБИ* - при использовании подсистемы распределенного аудита и управления разрешать ли полный доступ к файлам и папкам данного компьютера администратору безопасности информации;
- *проверять доступ к реестру* - использовать ли разграничение доступа к разделам и ключам системного реестра.

Остальные флаги в разделе «Опции настройки» не используются (зарезервированы для дальнейших разработок). Для выхода из режима редактирования с сохранением нажмите кнопку <Сохранить> или клавишу <F2>, без сохранения – <Отмена> или <Esc>.

7.14.Установка фиксированных сетевых имен ресурсов общего пользования

В составе СПО «Аккорд» реализована дополнительная функция, существенная для работы защищенного СВТ в составе ЛВС. Эта функция регламентирует процедуру выделения локальных ресурсов данного компьютера в общее пользование для остальных компьютеров локальной сети. Для вызова этой функции можно щелкнуть мышью на иконке с изображением «общего» ресурса на панели задач или выбрать команду «Имена общих ресурсов» в меню <Команды>. Откроется окно, представленное на рисунке 102.

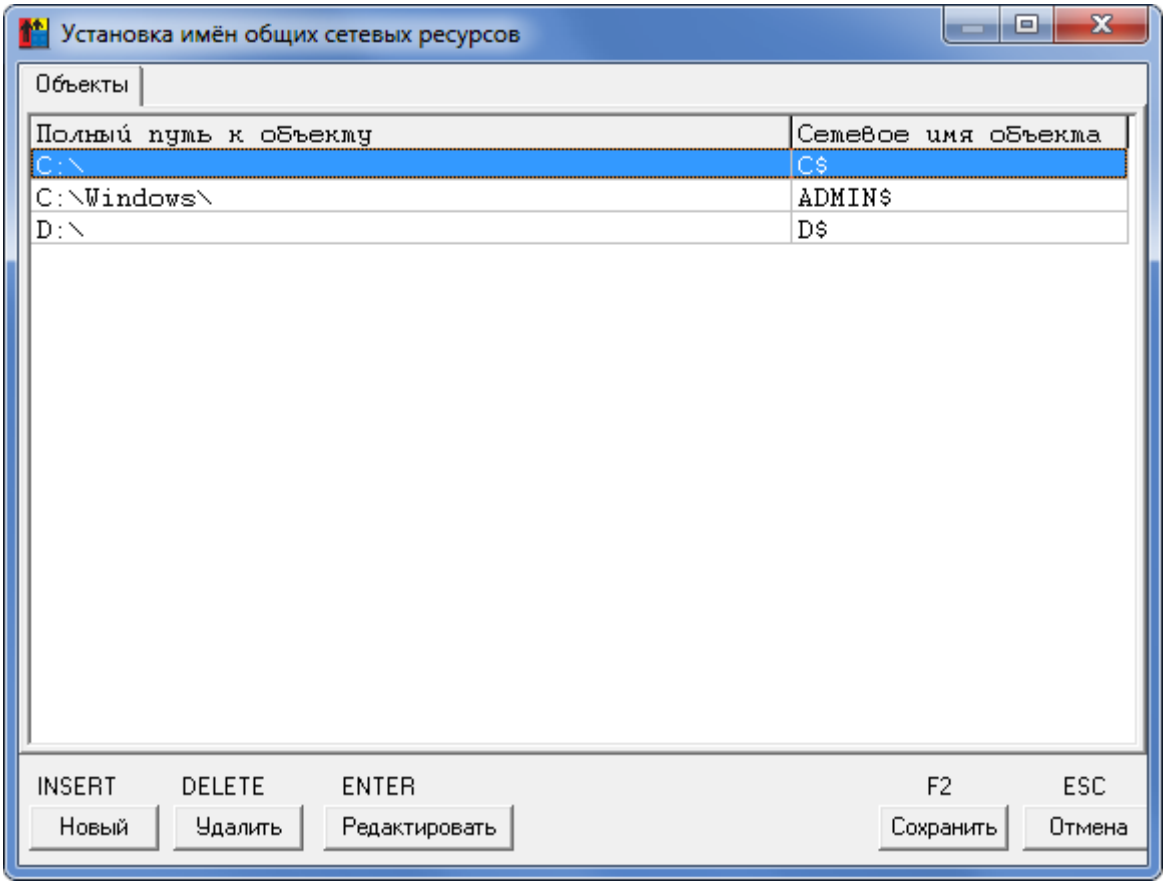

Рисунок 102 - Список ресурсов, выделяемых для общего доступа

В этом списке можно описать ресурсы (с полным именем), которые находятся на жестком диске данного компьютера, и задать сетевое имя, под которым ресурс будет доступен другим пользователям в сети. Для изменения сетевого имени объекта нужно выделить соответствующую строку и нажать <Enter> или щелкнуть мышью на кнопке <Редактировать>. Для добавления ресурсов в список служит кнопка <Новый>. Для чего предназначена данная функция? Во-первых, администратор полностью контролирует ресурсы, которые будут предоставлены для общего доступа, т.е. пользователь не сможет несанкционированно открыть доступ к конфиденциальной информации для других компьютеров в сети, а во-вторых, даже разрешенный ресурс предоставляется с фиксированным сетевым именем. Это важно, если в сети функционируют другие компьютеры с установленным СПО «Аккорд», и на этих компьютерах описан доступ к сетевым ресурсам. Поскольку этот доступ проверяется по полному сетевому пути, то администратор получает однозначное выполнение заданной политики безопасности.

Если производится попытка предоставить общий доступ ресурсу, не указанному в списке имен общих сетевых ресурсов, то такое действие считается НСД и заносится в журнал в виде «Attempt shared ObjectPath as ObjectName».

7.15.Экспорт/импорт базы данных пользователей и правил разграничения доступа

В программе ACED32.EXE предусмотрены процедуры сохранения и загрузки базы данных пользователей и правил разграничения доступа.

7.15.1. Сохранение/загрузка базы данных пользователей

Для сохранения базы данных пользователей выберите команду «Сохранить как» в меню «Файл» в главном окне программы (рисунок 103).

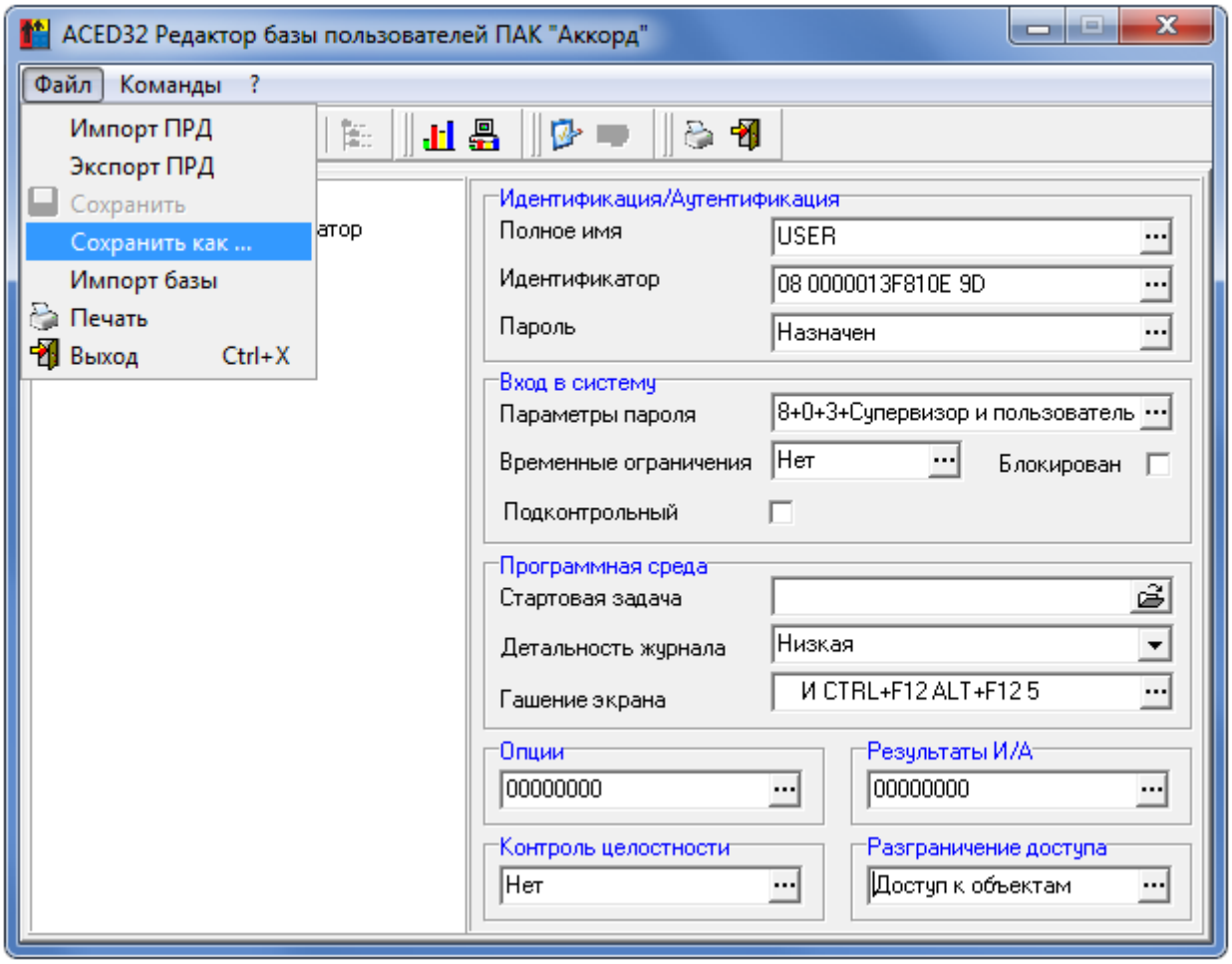

Рисунок 103 - Команды работы с базой данных пользователей

На экран выводится окно «Сохранить как» для выбора имени файла, показанное на рисунке 104.

Расширение файла .amz задается по умолчанию, и изменить его нельзя. После задания имени файла нажмите кнопку <Сохранить>. Параметры пользователей запишутся в виде файла на жесткий диск. Этот файл можно скопировать на съемный носитель и хранить как средство восстановления данных.

Восстановить настройки пользователей можно, скопировав резервную базу в папку Accord.NT (Accord.x64 – для 64-битных ОС) под именем accord.amz. После копирования достаточно запустить редактор ПРД и сделать

любое изменение в настройках любого пользователя, например, изменить время срабатывания Screen Saver. При выходе из программы подтвердить сохранение изменений.

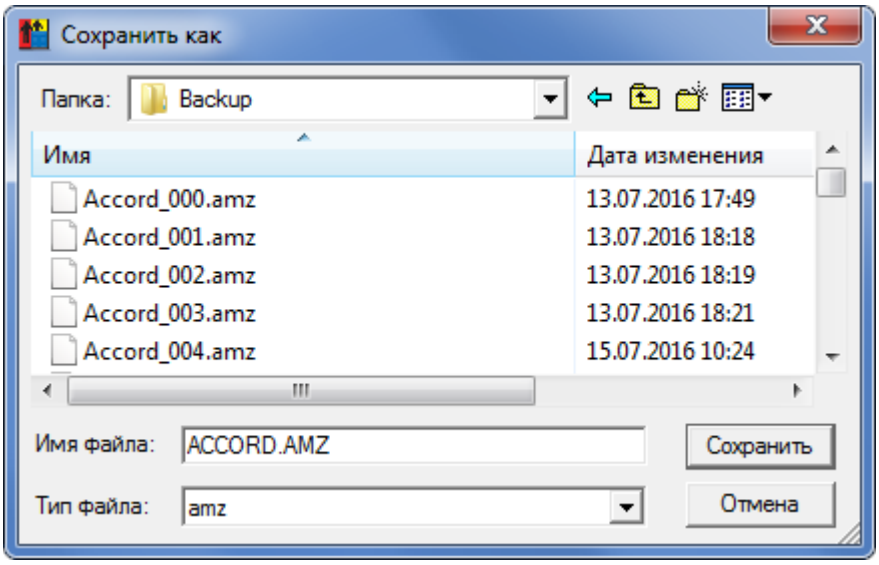

Рисунок 104 - Выбор имени файла для сохранения

Для корректировки настроек пользователей или просмотра базы данных пользователей в файле, в котором не зарегистрирован идентификатор Администратора БИ, предназначена команда «Импорт базы» в меню «Файл». После вызова этой команды на экран выводится окно выбора имени файла (рисунок 105).

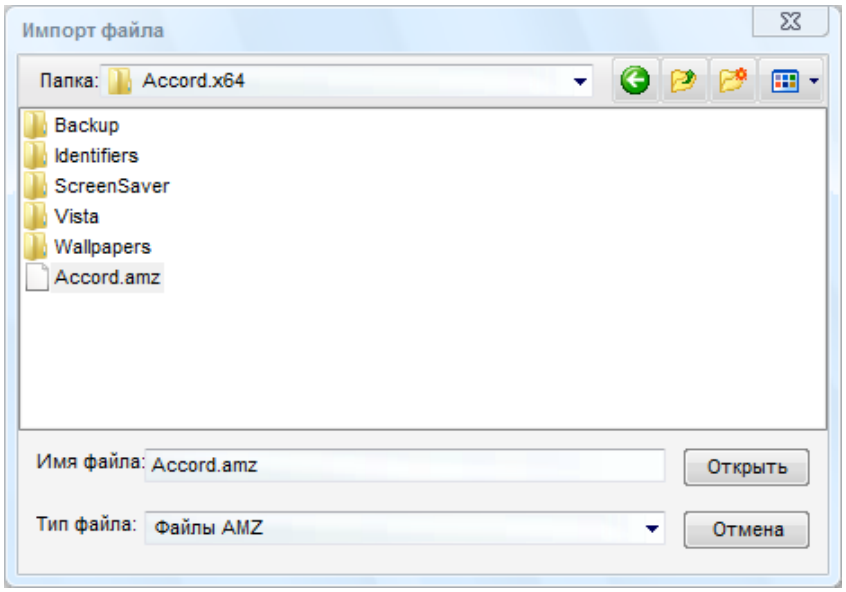

Рисунок 105 - Выбор файла для импорта базы данных пользователей

После ввода имени файла нажмите кнопку <Импорт>.

ВНИМАНИЕ! Изменения, которые внесены в импортированную базу, сохраняются по умолчанию в том же файле, из которого были импортированы. Такой режим работы с базой ПРД может быть полезен в том случае, когда администратору необходимо скорректировать настройки для удаленного компьютера, но подсистема удаленного аудита и управления не установлена. Администратор на своем компьютере выполняет импорт базы, вносит изменения, сохраняет настройки и отправляет полученный файл по электронной почте или сохраняет на дискете. После получения файла пользователь, выполняющий обязанности администратора удаленного компьютера, копирует его на жесткий диск.

7.15.2. Экспорт/импорт правил разграничения доступа

Программа ACED32.EXE позволяет сохранять в отдельных файлах правила разграничения доступа (ПРД) пользователя. Для этого следует выбрать пользователя и команду «Экспорт ПРД» в меню «Файл». На экран выводится окно выбора параметров, которые предполагается сохранить (рисунок 106).

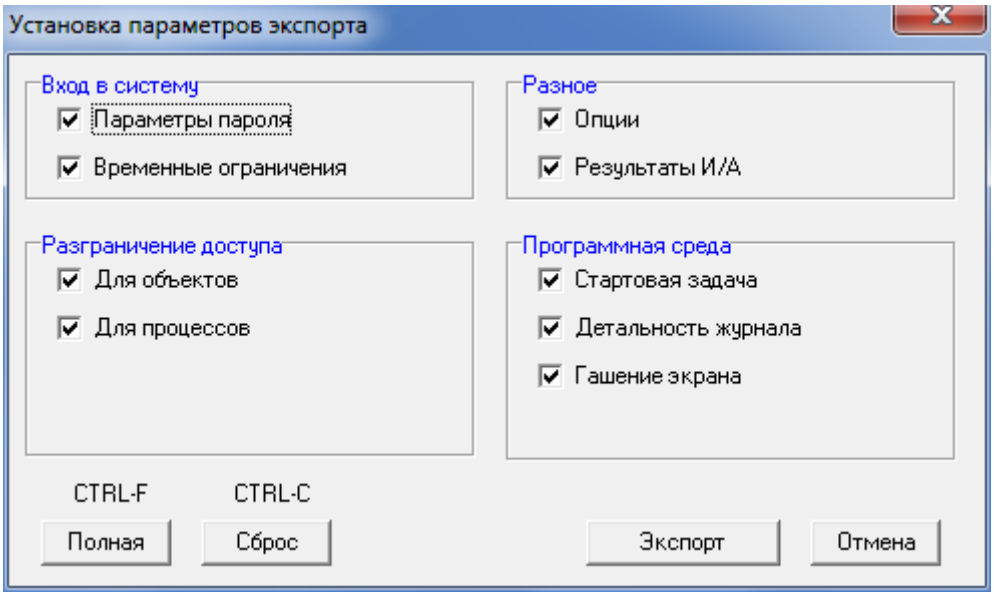

Рисунок 106 - Выбор параметров ПРД для экспорта

После выбора необходимого перечня экспортируемых параметров нажмите кнопку <Экспорт>. Выводится окно ввода имени файла для сохранения (рисунок 107).

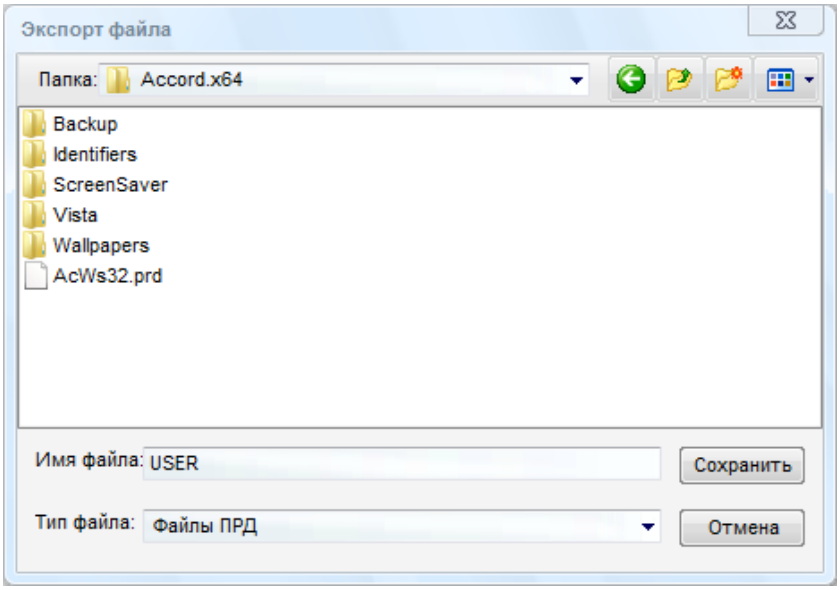

Рисунок 107 - Выбор имени файла для экспорта ПРД

Программа предлагает для сохранения имя файла, совпадающее с именем пользователя, но это не является обязательным условием, а сделано для удобства администратора безопасности. После ввода имени файла нажмите кнопку <Экспорт>. Файл запишется на диск.

Для импорта ПРД из файла следует отметить пользователя и выбрать команду «Импорт ПРД» в меню «Файл». Выводится окно выбора файла для импорта (рисунок 108).

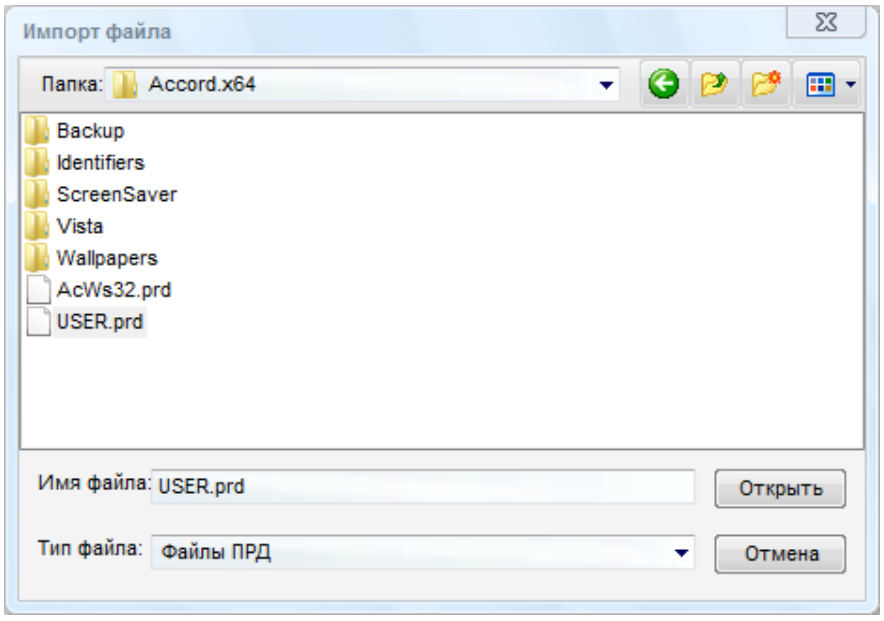

Рисунок 108 - Выбор имени файла для импорта ПРД

После ввода имени файла нажмите кнопку <Импорт>. На экран выводится окно выбора параметров, которые предполагается импортировать данному пользователю (рисунок 109).

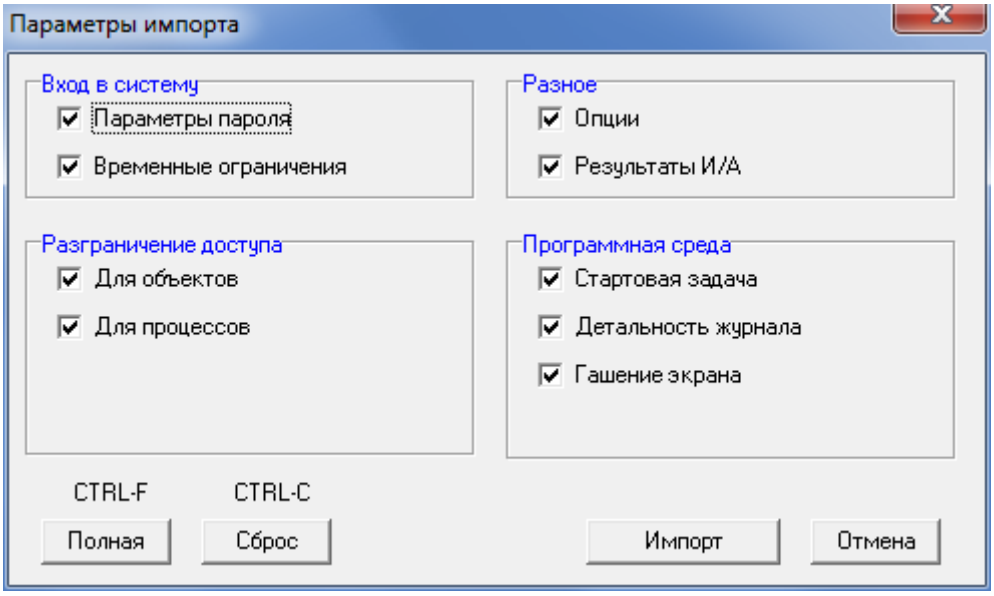

Рисунок 109 - Выбор параметров для импорта

Мышью следует выбрать параметры и нажать кнопку <Импорт>. На экран выводится окно выбора процедуры включения ПРД в настройки пользователя (рисунок 110).

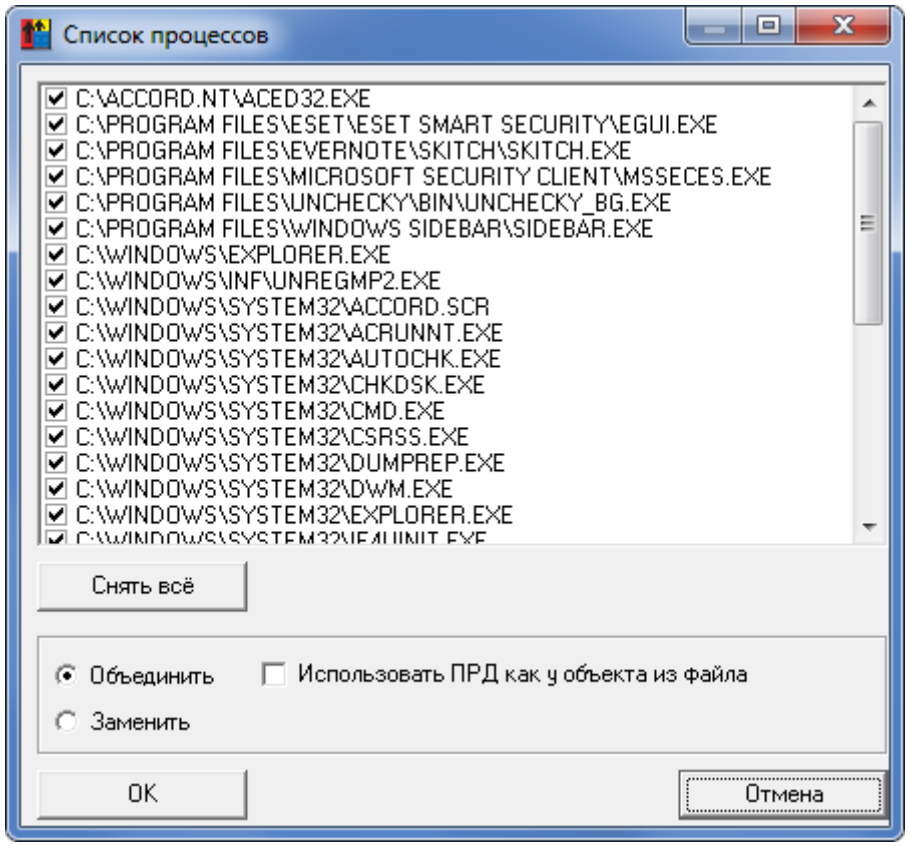

Рисунок 110 - Выбор процедуры формирования нового списка ПРД

В верхней части окна выводится список процессов (если флаг разграничения доступа для процессов включен в предыдущем окне), и можно выбрать те процессы, которые предполагается включить в ПРД данного пользователя.

Если выбран параметр «Объединить», то импортируемые ПРД добавляются в настройки пользователя. Флаг «Использовать ПРД, как у объекта из файла» позволяет при объединении списков включать в основные ПРД объект с теми атрибутами доступа, которые записаны в импортируемом файле. Если выбран параметр «Заменить», то настройки пользователя очищаются, и записываются только новые объекты и их ПРД из файла.

Например, при установке на защищаемый АРМ подсистемы распределенного аудита и управления «Аккорд» программа-клиент запускается из каталога Accord.NT (Accord.x64 – для 64-битных ОС) и выполняет запись в файл регистрации событий. В ПРД пользователя по умолчанию запрещен доступ к каталогу Accord.NT (Accord.x64), чтобы пользователь не мог нарушить настройки системы защиты. В файле acws32.prd прописан набор правил доступа к тем файлам в каталоге Accord.NT (Accord.x64), которые необходимы для работы клиента РАУ. Администратор безопасности может импортировать ПРД группе пользователей, а потом выполнить синхронизацию пользователей с групповыми политиками.

Аналогично выполняется экспорт/импорт меток мандатного доступа для объектов. Для этого нужно выбрать соответствующие пункты в меню «Команды».

В состав СПО «Аккорд» входят две программы, которые позволяют сформировать файл правил разграничения доступа (файл с расширением .prd) на основе записей в журнале регистрации событий. Программа LogToPRD.exe формирует список объектов, а программа AcProc.exe формирует список процессов. Подробно работа с этими программами описана в документе "Подсистема регистрации. Программа работы с журналами регистрации «LogView». Из полученных в результате работы программ файлов .prd можно импортировать правила доступа отдельному пользователю или группе пользователей. Такая технология формирования ПРД избавляет администратора безопасности от необходимости вручную вводить список объектов.

7.16. Формирование списка разрешенных USB-устройств и SD-карт

ВНИМАНИЕ! В СПО «Аккорд-Win64 K» управление доступом к устройствам и контроль USB и SD выполняются только для сессии консоли, т.е. на основе ПРД, назначенных тому пользователю, который загружает терминальный сервер. Для всех пользователей удаленного рабочего стола индивидуальные списки устройств действовать не будут.

Если в ПРД пользователя описать доступ к съемному диску, будет доступен флэш-диск, подключенный к серверу в рамках сессии консоли.

Большинство современных компьютеров имеют в своем составе USB-шину и устройства для чтения Secure Digital карт. Программа-редактор ACED32 позволяет администратору безопасности сформировать список USB-устройств и SD-карт, с которыми разрешено работать данному пользователю.

По умолчанию для обычных пользователей в список объектов уже включена запись «USB, Vid=*, Pid=*, Sn=*, -, Allowed all USB devices!».

Это означает, что любое USB-устройство разрешено для доступа.

Если администратора безопасности не устраивает такая ситуация, ему необходимо удалить эту строчку из списка объектов доступа и назначить конкретные устройства, к которым доступ будет разрешен. Для выполнения данной операции нужно в окне редактирования правил доступа пользователя (рисунок 55) щелкнуть мышью по клавише <USB/SD>. Открывается окно редактирования списка устройств (рисунок 111).

ВНИМАНИЕ! Если удалена запись «USB, Vid=*, Pid=*, Sn=*, -, Allowed all USB devices!», то для нормальной работы клавиатуры и мыши, подключенных по USB, запись о них нужно добавить в список.

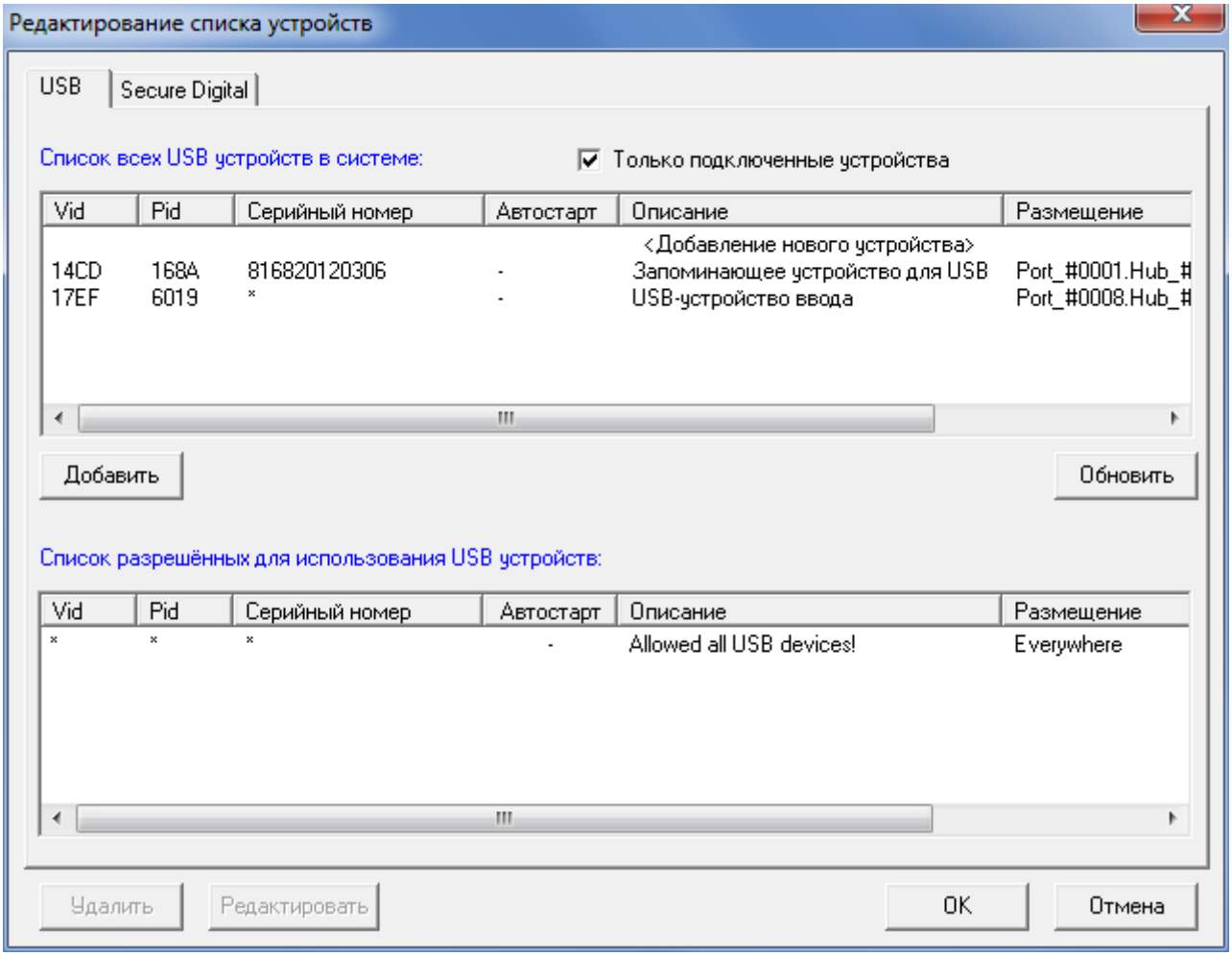

Рисунок 111 - Окно редактирования списка разрешенных USB-устройств

В верхней части окна по умолчанию включен флаг «Только подключенные устройства». В этом режиме в списке доступных устройств отображаются только те, которые в данный момент подключены к компьютеру. Если в списке нет устройства, щелкните мышью по кнопке <Обновить>. По этой команде выполняется поиск подключенных USB-устройств, и они появляются в верхней половине окна в списке устройств. Установите курсор на то устройство, доступ к которому Вы хотите разрешить данному пользователю. Нажмите кнопку <Добавить>, и USB-устройство появится в нижней половине окна в списке разрешенных для использования (рисунок 112). Чтобы включить несколько устройств, нужно повторить операцию выбора и добавления устройств. Для

завершения процедуры выбора нажмите кнопку <Ок>, и выбранные устройства появятся в списке объектов (рисунок 55).

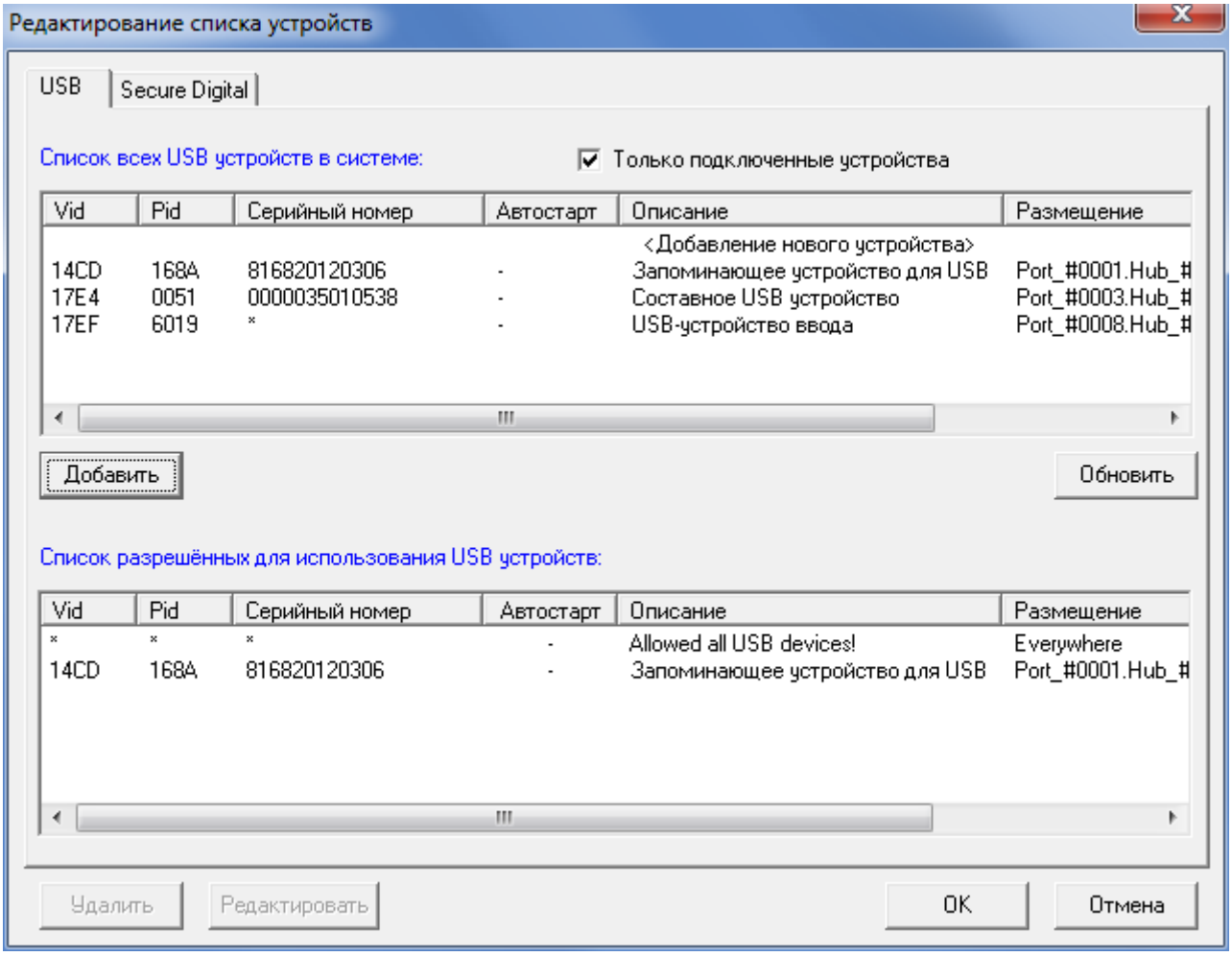

Рисунок 112 – USB-устройство добавлено в список разрешенных

Можно использовать другой режим добавления устройств, когда снят флаг «Только подключенные устройства». В этом случае в списке выводятся идентификационные параметры устройств, которые подключены к компьютеру в данный момент и подключались ранее - эти сведения сохраняются операционной системой. Пользоваться этим режимом следует с осторожностью, только в том случае, когда Вам точно известен серийный номер того устройства, доступ к которому будет разрешен.

При необходимости ограничения доступа к USB-устройствам пользователей группы «Администраторы» в программе ACED32.EXE во вкладке Разграничение доступа\Редактирование списка устройств следует удалить строку «Allowed all USB devices». При этом пользователю будут доступны только USB-устройства, добавленные в список разрешенных[10].

---

[10] Такие правила разграничения доступа будут действовать, если у пользователя в привилегиях Администраторов снят хотя бы один из четырех первых флагов: «Редактирование пользователей», «Редактирование контроля», «Управление журналом», «Редактирование настроек». Снятие флага «Контролер» на доступ Администраторов к USB-устройствам не влияет.

В закладке Secure Digital точно так же можно сформировать список разрешенных для использования карт памяти. Процесс регистрации SD-карт имеет одну особенность - если устройство считывания карт подключено к USB-порту, то в списке устройств в ОС отображается одно-единственное устройство, а серийные номера карт будут недоступны. Администратор не сможет формировать список SD-карт по уникальным номерам. Поэтому в АС, в которых обрабатывается конфиденциальная и секретная информация, следует избегать подключения считывателя карт через USB.

ВНИМАНИЕ! Если USB-устройство – это съемный диск (флоппи, Zip, CD, флэш – не важно), то после включения его в список разрешенных устройств следует описать правила доступа к тому логическому съемному диску, который монтируется в системе после подключения физического устройства к компьютеру. Если такую операцию не выполнить, то съемный диск останется недоступным после подключения к компьютеру, т.к. все логические диски, не включенные в список ПРД, запрещены. Атрибуты доступа устанавливаются стандартным образом, эта процедура описана в пункте 7.11.1.3 настоящего Руководства.

ВНИМАНИЕ! Для корректной работы функции проброса USB-устройств на платформе виртуализации VMware vSphere Client необходимо:

1) запустить утилиту «Редактор прав доступа» под учетной записью Администратора СПО «Аккорд» (Программы\Аккорд\Редактор прав доступа);

2) из списка учетных записей пользователей выбрать учетную запись Администратора инфраструктуры виртуализации (Администратора ИВ);

3) затем выбрать меню «Разграничение доступа» и в появившемся окне нажать кнопку <USB/SD>;

4) далее в окне редактирования списка устройств необходимо добавить в список разрешенных устройство VMware USB Device с VID=0E0F, PID=0001 и серийным номером =*.

В случае необходимости следует повторить описанную последовательность действий для каждого из Администраторов ВИ.

Устройство VMware USB Device заменяет USB-устройство, подключенное к локальному СВТ, на время его подключения к платформе виртуализации.

7.17. Формирование правил доступа для отдельных программ (процессов)

В состав СПО «Аккорд» входит программа, которая позволяет сформировать файл правил разграничения доступа для отдельных программ (файл с расширением .prc). Программа MakePrc.EXE использует тот же набор атрибутов доступа, что и редактор ACED32.EXE, поэтому логично привести ее описание в данном документе. После запуска программы на экран выводится главное окно (рисунок 113).

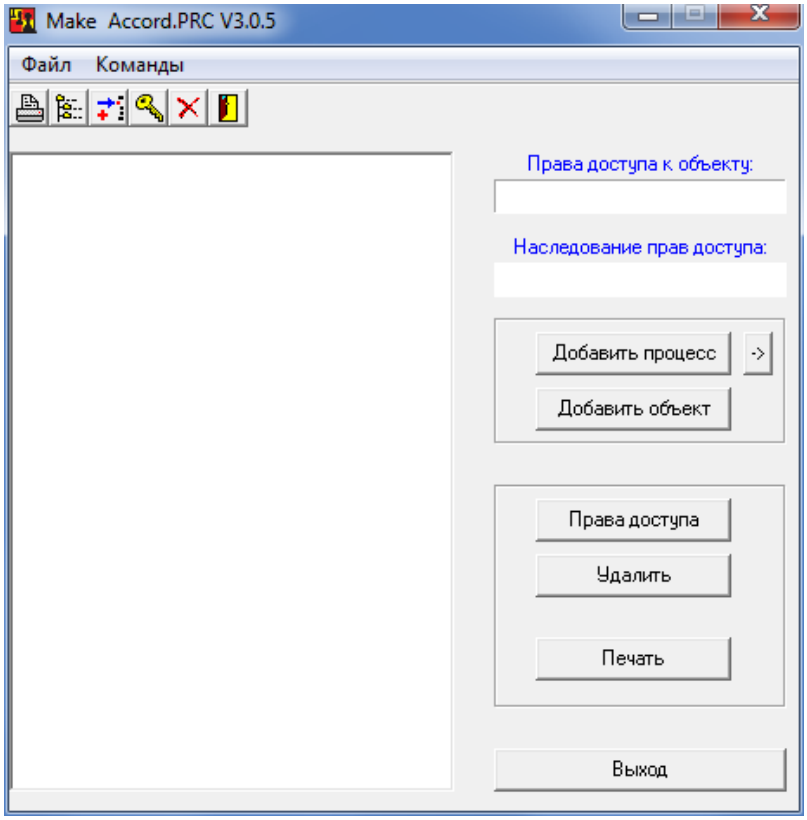

Рисунок 113 - Главное окно программы MakePrc

Вначале необходимо добавить программу (процесс), для которого будут устанавливаться правила доступа. Для этого на панели инструментов нужно нажать кнопку с изображением дерева каталогов или в меню «Команды» выбрать команду «Добавить процесс». На экран выводится окно выбора процесса (рисунок 114).

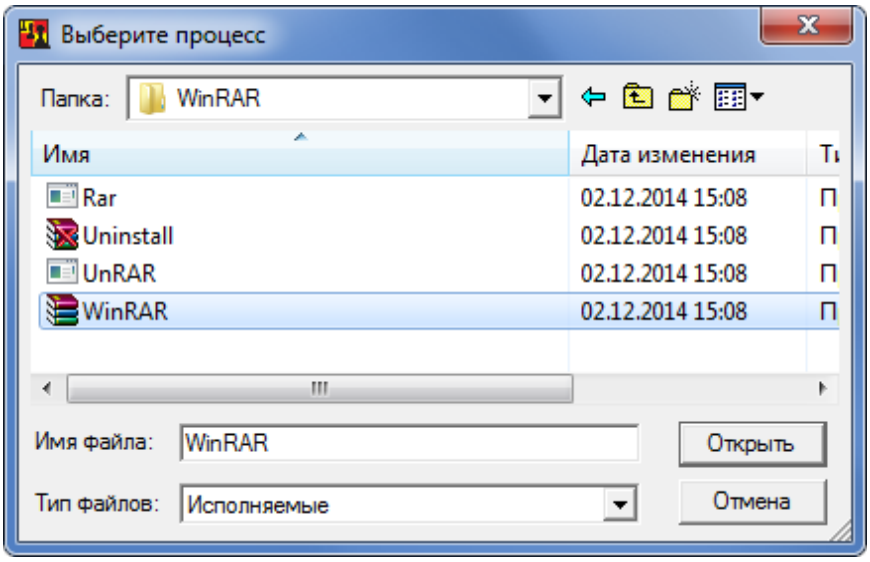

Рисунок 114 - Выбор процесса, для которого будут устанавливаться ПРД

Отметьте нужный исполняемый файл (.exe или .dll) и нажмите кнопку <Открыть>. Выбранный файл появится в списке процессов в левой половине главного окна. При необходимости процедуру выбора файла можно повторить,

т.е. в системе защиты «Аккорд» можно создать целый список процессов, для которых задаются правила доступа, не зависящие от ПРД текущего сеанса пользователя.

Теперь каждому процессу, включенному в список, нужно назначить список объектов. Для этого мышью отмечается процесс, после чего становится доступной кнопка на панели «Добавить объект». При нажатии этой кнопки открывается окно выбора файлов и каталогов (рисунок 115).

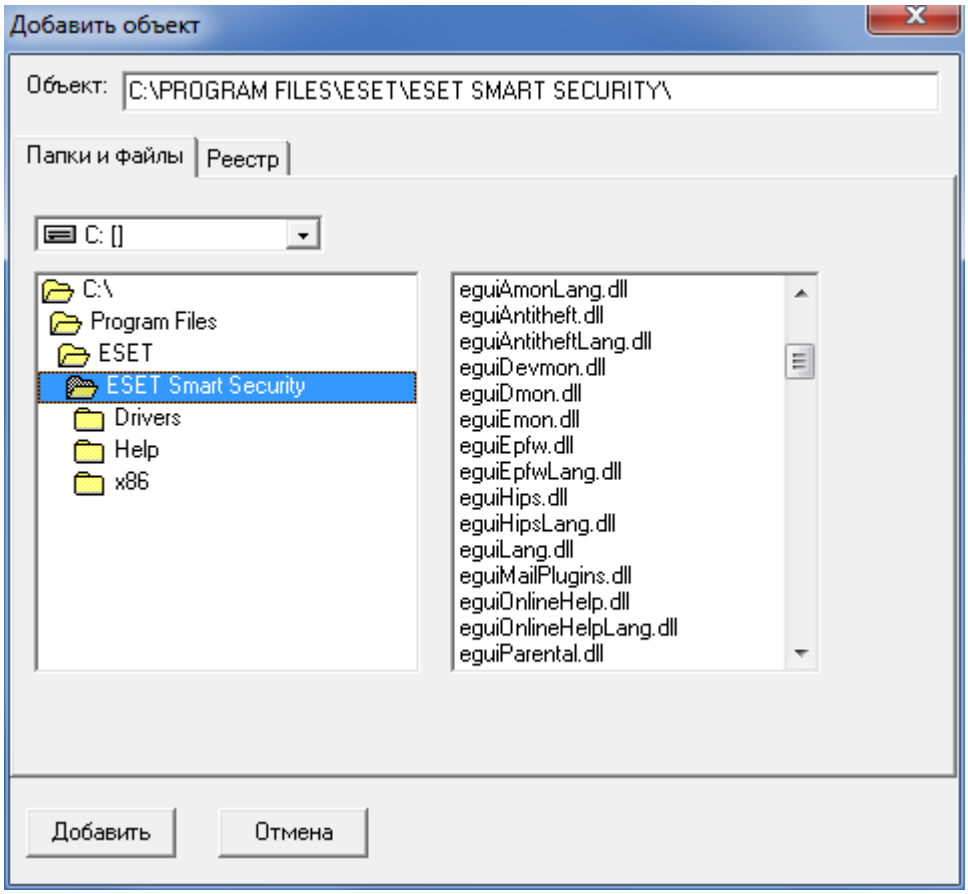

Рисунок 115 - Окно выбора файлов и каталогов

Отметьте необходимый каталог, нажмите кнопку <Добавить>. Выбранный объект появляется в списке под именем процесса. Для выбора конкретного файла из каталога нужно предварительно два раза щелкнуть мышью на каталоге в левом поле. В правом поле окна появится список файлов. Установите мышью курсор на нужном файле, нажмите кнопку <Добавить>. Если одному процессу необходимо назначить доступ к нескольким объектам, то операцию выбора нужно повторить. Теперь для каждого объекта из списка можно поменять ПРД (по умолчанию установлен полный доступ). Выберите мышью нужный объект. По двойному щелчку мышью или при нажатии кнопки <Права доступа> открывается окно установки атрибутов доступа. Атрибуты доступа полностью соответствуют дискреционным ПРД, которые устанавливаются с помощью редактора ACED32.EXE.

После того как установлены ПРД для выбранного объекта, нажмите клавишу <Сохранить>. Повторите операцию для других объектов. После того как всем объектам назначены правила доступа, следует сохранить настройки в файл на жестком диске. Нажмите кнопку <Выход>, подтвердите сохранение

файла (рисунок 116). Запись производится в файл accord.prc. При старте монитора разграничения доступа AcRun.SYS выполняется проверка наличия файла accord.prc. Если файл обнаруживается, то при запуске процессов, описанных в этом файле, будут выполняться заданные для них ПРД.

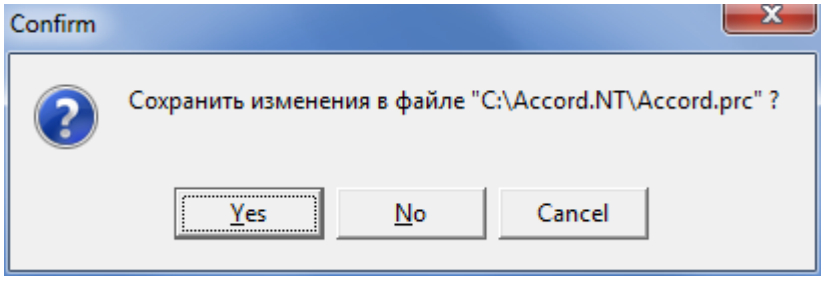

Рисунок 116 - Сохранение файла ПРД для выделенных процессов

Имеется возможность редактирования файла привилегированных процессов (*.PRC) в рамках работы программы ACED32.EXE. Для этого необходимо нажать кнопку <Редактирование списка привилегированных процессов>[11] на панели инструментов в главном окне программы ACED32.EXE (рисунок 2).

ВНИМАНИЕ! ПРД, загружаемые из файла accord.prc, действуют только для заданных процессов и не зависят от настроек правил доступа текущего пользователя. Важно понимать, что для выделенного процесса будет предоставлен доступ ТОЛЬКО к тем объектам, которые включены в список объектов в файле accord.prc!

Для каких целей используется данная технология? Предположим, что в составе АРМ имеются ресурсы, доступ к которым должен предоставляться независимо от настроек пользователя и только выделенными процессами. Самому пользователю, как правило, эти ресурсы недоступны.

7.18. Групповая политика и особенности установки ПРД на контроллере домена Windows

В данном Руководстве уже упоминалось, что при создании новой группы пользователей можно указать группу в составе ОС, в которую будут включаться пользователи СЗИ «Аккорд». Для того чтобы эта технология работала, в настройках СПО «Аккорд» должен быть установлен флаг «Синхронизация с базой пользователей NT». При установке СПО «Аккорд» этот флаг включен по умолчанию. Соответствие группы пользователей СЗИ «Аккорд» группам в составе ОС устанавливается нажатием кнопки <NT группы»> в главном окне программы после выбора нужной группы. Открывается окно выбора из списка существующих групп в составе ОС (рисунок 117).

---

[11] Кнопка <Редактирование списка привилегированных процессов> на панели инструментов в главном окне программы ACED32.EXE активна только при наличии файла *.PRC.

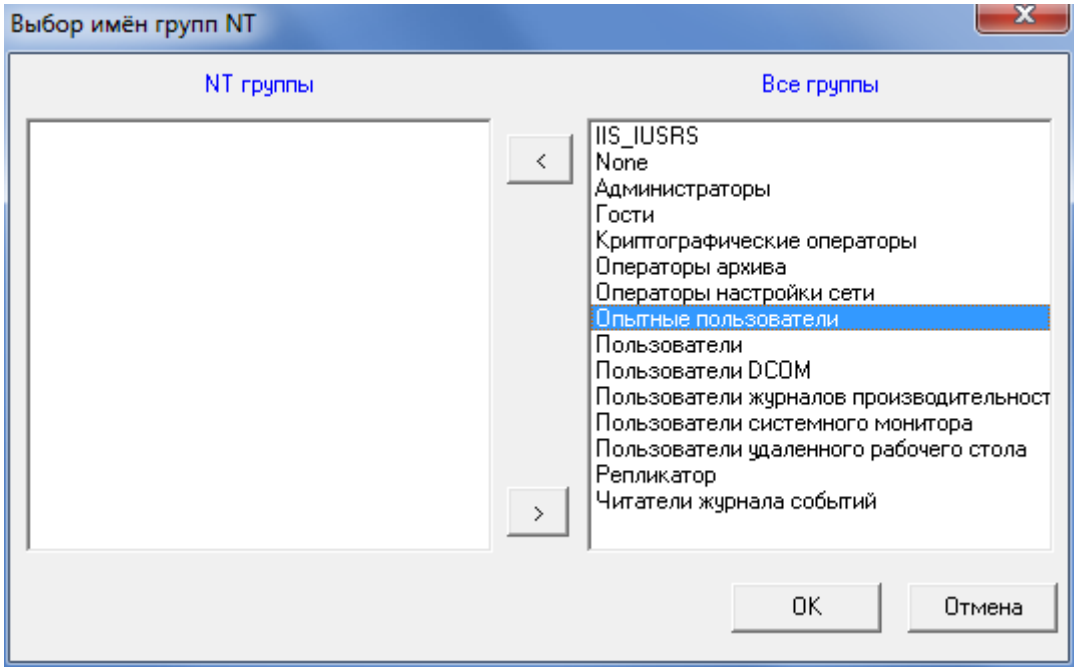

Рисунок 117 - Окно выбора групп пользователей

В правой половине окна перечислены все группы, в левую часть можно перенести одну или несколько групп, к которой должны принадлежать пользователи СПО «Аккорд». Такой вариант показан на рисунке 118. Изменить привязку к группам в составе ОС можно и для двух создаваемых по умолчанию групп СЗИ «Аккорд» - «Администраторы» и «Обычные». При установке подсистемы разграничения доступа «Администраторы» соответствуют группе «Administrators/Администраторы», «Обычные» соответствуют группе «Users/Пользователи» в зависимости от основного языка установленной ОС.

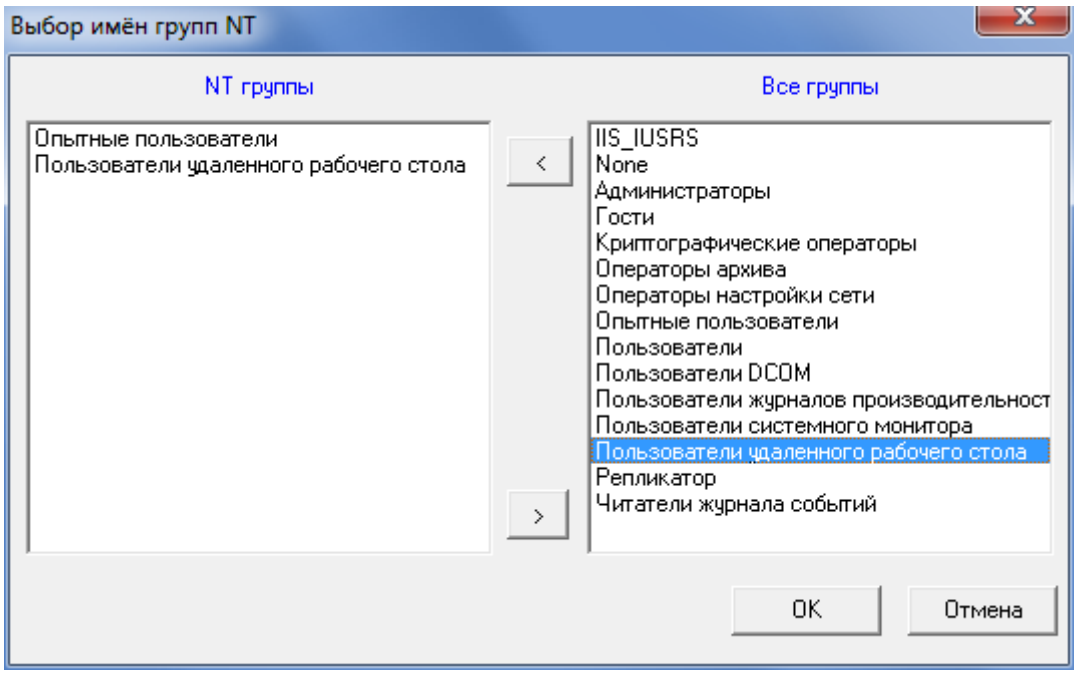

Рисунок 118 - Синхронизация пользователя СЗИ «Аккорд» с несколькими группами ОС

Для завершения процедуры с сохранением нажмите <Ок>, выход без сохранения изменений - <Отмена>. При завершении программы ACED32.EXE с сохранением изменений пользователи «Аккорда» будут добавляться в базу данных ОС с членством в указанных группах.

Установка СПО «Аккорд» на контроллере домена Windows требует некоторых специфических настроек. Формат AD несколько отличается от обычной базы пользователей NT. Синхронизация с базой NT при выходе из редактора ПРД не происходит, поэтому данный флаг нужно выключить в программе настройки СПО «Аккорд». Пользователь должен вначале создаваться в AD средствами ОС, а потом включаться в список пользователей СЗИ Аккорд с назначением идентификатора. О синхронизации баз см. также п. 5.1 настоящего Руководства.

ВНИМАНИЕ! Правила разграничения доступа, установленные в системе «Аккорд», будут действовать только в том случае, когда пользователь проходит процедуру идентификации/аутентификации на компьютере, на котором установлен контроллер домена. При удаленном подключении пользователя к домену с другого компьютера действуют настройки политики безопасности домена.

8. Заключение

Программа ACED32.EXE является лишь редактором параметров доступа пользователя к объектам доступа СВТ. Разграничение доступа пользователей к ресурсам компьютера реализуется монитором безопасности ACRUN.SYS, который использует матрицу доступа, подготовленную с помощью редактора ACED32.EXE. Подробно процесс настройки и запуска монитора безопасности описан в «Руководстве по установке» (37222406.26.20.40.140.091 98).

Приложение 1.
Файл ACCORD.INI – файл конфигурации СПО «Аккорд»

Описание параметров, задаваемых в файле accord.ini, которые могут быть изменены администратором СПО «Аккорд» или субъектом с правами администратора:

[COMMON]

TmPageNo=0 – страница идентификатора. В этой и следующей странице памяти идентификатора хранится ключ пользователя. Значение по умолчанию – 0, т.е. данные занимают 0-ю и 1-ю страницы.

ВНИМАНИЕ! Не рекомендуется изменять этот параметр без необходимости. При изменении параметра требуется перерегистрировать ВСЕ идентификаторы с генерацией нового ключа. Будьте внимательны при использовании программных средств других производителей, которые используют ТМ для хранения своих данных. Если эта информация будет повреждена, то пользователь не получит доступ к компьютеру с установленным СПО Аккорд, т.к. в базе данных хранится результирующая функция, в которой используется заводской номер идентификатора, пароль и ключ пользователя.

TmTimeout=20

PasswTimeout=20 – Временной интервал, который отводится для предъявления идентификатора и ввода пароля.

UseLogicalDisksNames=(«No» по умолчанию) – использование логических имен разделов жесткого диска в матрице описаний правил доступа. Параметр может быть изменен в случае использования дополнительных съемных дисков или аппаратных RAID массивов, которые меняют порядок физических дисков в системе. После изменения этого параметра обязательно запустить редактор ПРД для создания нового списка контролируемых логических разделов. Если используются логические имена, то невозможно будет разграничить доступ к съемным дискам (флоппи, USB и др.).

UsePPOCheck – Параметр зарезервирован для дальнейшего использования.

[ACRUN]

LockUSB - блокировка USB портов во время работы ScreenSaver. Значения: «Yes» – блокировать, «No» – не блокировать (установлено по умолчанию).

ClearSteps=1 – число повторов записи последовательности случайных чисел на диск (при удалении файлов с очисткой).

ClearPagefile – очищать файл подкачки при завершении сеанса пользователя

Значения: «Yes» – очищать. «No» – не очищать (установлено по умолчанию).

ClearLevel – очищать при удалении файлы, начиная с выбранного уровня конфиденциальности

ClearOnNet - отвечает за удаление с очисткой файлов на сетевых дисках. Эти файлы могут быть в общем доступе, или DFS, поэтому параметр по умолчанию выключен.

DisplayNSD – Выводить на экран сообщения об НСД от имени СЗИ. «No» – не выводить отдельного сообщения (установлено по умолчанию), а все отказы в доступе транслировать на уровень стандартного интерфейса ОС.

WriteNsdOnFind=Yes - (установлено по умолчанию) параметр определяет запись в журнал событий НСД при операциях Find1st/FindNxt, Traverse и CreateDir, т.е. при проверке существования пути. Если параметру присвоено значение «No», то не будет записи таких событий в журнал. Редактируется флаг только вручную.

WriteWarningToLog=No – Определяет запись в журнал кода результата «Warning». Данный результат фиксируется при применении атрибута O при очистке файла, а пишется в журнал при установке значения «Yes». Редактируется флаг только вручную.

CheckCompOffTime – контроль времени завершения сеанса пользователя

Значения: «Yes» – контроль времени используется. «No» – не используется.

WarningCompOffTime=5 – интервал времени до завершения сеанса, с того момента, когда выводится пользователю предупреждение о предстоящем окончании работы. Задается в минутах.

HardResetCompDeltaTime=2 – интервал времени, по истечении которого принудительно перегружается компьютер, если сеанс не удалось завершить корректно (с закрытием всех приложений). Задается в минутах.

DisableSessionLogOff – принудительная перезагрузка по завершении сеанса пользователя (по умолчанию – «No», в программе настройки флаг «завершать сессию полной перезагрузкой»).

LoginUseFullName (по умолчанию – «No») - использование полного имени пользователя при входе в систему.

FullProcessPath – контроль процессов по полному пути доступа. Значения: «Yes» – контроль по полному пути. «No» – контроль только по имени процесса.

WriteLogicalNames – тип записи в журнал регистрации событий имени тома. Значения: «Yes» – запись логического имени. «No» – запись в журнал полного пути, например: DEVICE\HardDiskVolum1\…

MarkCaption (по умолчанию «Yes») – выводить в заголовке окна текущее значение уровня доступа запущенного процесса.

CheckPrint (по умолчанию «No») - отвечает за перехват функций печати. Если значение параметра «No», то функции печати не перехватываются.

DelayStartSpecProcess=0

ExistsAsAttrib (по умолчанию «Yes»). Если установлен этот параметр, то проверка существования объекта проверяется через ZwQueryFullAttributesFile, т.е. более быстрым алгоритмом. Если вдруг начнут «отваливаться» службы ILO HP, или будет аварийно завершаться Device Lock, то установить значение «No».

CheckDevices (по умолчанию «No») - отвечает за контроль доступа к устройствам. Список контролируемых устройств появляется в редакторе ПРД после включения этого параметра.

ChkDsk – параметр определяет возможность старта программы проверки дисков при загрузке ОС. Значение по умолчанию – «No».

VirtualManager=Yes - параметр определяет режим работы специального ПО «ГиперАккорд».

LogonAtSecretKey – параметр определяет способ аутентификации пользователя: если параметр установлен в значение «No», то при выполнении процедур И/А выполняется проверка номера идентификатора пользователя, если параметр установлен в значение «Yes», то при выполнении процедур И/А помимо номера идентификатора пользователя выполняется проверка ключа пользователя, записанного в идентификатор.

NoCheckDateTime - если параметр установлен в значение «Yes», то при выполнении проверки файла для КЦ дата и время модификации файла не проверяются.

MdDelFile (по умолчанию «Yes») – параметр определяет режим работы мандатного механизма разграничения доступа. Если параметру присвоено значение «No», то пользователь может выполнить процедуру удаления файла, даже если уровень доступа пользователя ниже метки доступа файла, если же параметру присвоено значение «Yes», то пользователь сможет удалить файл, только если его уровень доступа будет больше или равен метке доступа файла.

DefaultStartType – обозначает версию СПО «Аккорд». Если параметру присвоено значение «3», значит, на СВТ установлено СПО «Аккорд-Win64 K».

AutoLogin=Yes – установлен флаг «Автоматический логин в ОС» в программе настройки СПО «Аккорд».

SafeMode=Yes - установлен флаг «Мягкий режим» в программе настройки СПО «Аккорд».

TrayExportLogs=Yes – параметр определяет отображение дополнительного меню экспорта журналов в иконке СПО «Аккорд» в трее.

UseVirtualDisk - параметр определяет режим работы СПО «Аккорд» (Accord-VirtualDisk), в рамках которого имеется возможность работы с виртуальными дисками.

[ACED]

Flag0100=Не контролировать UNC имена

Flag0200=Удаление файлов с очисткой

Flag0400=Маркировка печати

Flag0800=<не используется>

Flag1000=Может изменять дату/время

Flag2000=Запрет доступа к общим ресурсам

Flag4000=Полный доступ для АРМ АБИ

Flag8000=Проверять доступ к реестру

English – язык интерфейса программ СЗИ Аккорд (значение No определяет вывод всех заголовков и сообщений на русском языке).

PrdType=New

UseNTBase – синхронизация с БД пользователей операционной системы. Значения: Yes – при создании пользователя в БД СЗИ «Аккорд» он заносится в список пользователей операционной системы. «No» – синхронизация не выполняется.

DeleteNoAccordUsers – при синхронизации с базой пользователей ОС удалять существующих пользователей, которые не являются пользователями СЗИ «Аккорд». Значения: «Yes» – удалять. «No» – не удалять.

InactiveDays - устанавливает временной период неактивности (в днях), по истечении которого учетная запись пользователя блокируется (параметр «Блокировать учетную запись при неактивности» программы настройки комплекса «Аккорд»).

DiscreteAccess – использование дискреционного метода разграничения доступа Значения: «Yes» – используется. «No» – не используется.

MandatoryAccess – использование мандатного метода разграничения доступа. Значения: «Yes» – используется. «No» – не используется.

CheckProcess – использование контроля исполняемых файлов как дополнительной подсистемы дискреционного и/или мандатного метода. Значения: «Yes» – используется, при этом в сеансе конкретного пользователя допускается выполнение только процессов из «белого» списка. Процессу назначается уровень доступа. «No» – не используется.

NoConvertNetPath (по умолчанию «No»). Если значение Yes, то при выходе из редактора Aced32 в базу пишутся только длинные имена сетевых файлов (т.е. не производится их конвертация в короткие имена). Параметр необходим в тех случаях, когда в базу ПРД включено много сетевых ресурсов на серверах, недоступных в данный момент времени. Преобразование таких имен при выходе из Aced32 занимает очень много времени, т.к. ОС пытается несколько раз получить доступ к недоступному ресурсу, прежде чем возвращает код ошибки.

ServerName – имя сервера

IncludeDomainName – включать ли имя домена в полное имя пользователя

DomainName – имя домена в виде строковой переменной.

37222406.26.20.40.140.091 97

[MANDATORY]
Level0=Общедоступно
Level1=ОБЩИЙ_РЕСУРС
Level2=Конфиденциально
Level3=Секретно
Level4=Совершенно_секретно

[Terminal Server]

Check0Session=Yes – параметр позволяет отменить проверку ПРД для 0 сессии.

RdpProtocol – использование протокола RDP. Значения: Yes – используется. No – не используется.

IcaProtocol - использование протокола ICA. Значения: Yes – используется. No – не используется.

OneRemoteSessionPerUser=Yes – параметр определяет вариант работы, когда удаленный пользователь не может одновременно открыть несколько удаленных сессий.

AutoLoginSession=Yes – параметр определяет режим работы пользовательского терминала, при котором результаты идентификации/аутентификации пользователя передаются от контроллера «Аккорд-АМДЗ» программному обеспечению, которое обрабатывает начало сессии удаленного пользователя.

XAuthLoginSession=Yes - параметр определяет 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».

LockSession=Yes – параметр определяет режим работы сессии пользователя при извлечении идентификатора.

COHOnly - параметр определяет режим работы с ПАК «Секрет Особого Назначения». Если параметр установлен в значение «Yes», то в режиме терминальной сессии разрешена работа только с ПАК «Секрет Особого Назначения», доступ к остальным съемным устройствам запрещен. Если параметр установлен в значение «No», то разрешена работа со всеми съемными устройствами, подключенными к рабочей станции.

FastUserSwitch=Yes – параметр определяет режим работы пользовательского терминала, при котором возможно переключение между пользователями СВТ с сохранением активных сессий ранее работавших на СВТ пользователей (аналогично функции «Сменить пользователя» в ОС Windows).

Параметры, задаваемые в файле accord.ini, изменяются программой настройки СПО «Аккорд». Не рекомендуется менять их значение вручную без четкого понимания последствий вносимых изменений. Исключение – параметры UseLogicalDisksNames, WriteNsdOnFind, WriteWarningToLog, и NoConvertNetPath, они корректируются только в файле accord.ini любым текстовым редактором.

ВНИМАНИЕ! После изменения значения параметра WriteNsdOnFind в файле Accord.ini требуется перезагрузка СВТ!

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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