ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.4012-037 97-ЛУ

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-Win64» (версия 5.0)

Установка правил разграничения доступа Программа ACED32

11443195.4012-037 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 комплекса СЗИ НСД «Аккорд-Win64» v.5.0 (ТУ 4012-037-11443195-2010) при настройке подсистемы разграничения доступа комплекса в соответствии с принятыми ПРД и входит в состав специального ПО комплекса.

Настоящее руководство предназначено для конкретизации действий администратора БИ (либо субъектов доступа, наделенными правами администратора) и содержит описание программы ACED32.EXE и порядок ее применения при установке и сопровождении комплекса.

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

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

СОДЕРЖАНИЕ

1. Назначение программы 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 13
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. Поиск пользователя по идентификатору 25
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 33
7.4. Задание пароля пользователя 34
7.5. Установка детальности протокола работы пользователей 36
7.6. Установка режима блокировки экрана 40
7.7. Установка временных ограничений для сеанса работы и учетной записи пользователя 45
7.8. Блокировка пользователя 46
7.9. Установка стартовой задачи пользователя 46
7.10. Контроль целостности файлов 52
7.10.1. «Статический» контроль целостности файлов 52
7.10.2. «Динамический» контроль целостности файлов 56
7.11. Установка правил разграничения доступа (ПРД) к объектам доступа 59
7.11.1. Установка доступа к объектам с использованием дискреционного метода ПРД 60
7.11.2. Установка доступа к объектам с использованием мандатного метода контроля ПРД 71
7.12. Контроль процессов с использованием мандатного и/или дискреционного механизмов разграничения доступа 74
7.12.1. Общие сведения 74

7.12.2. Особенности настройки контроля процессов с использованием мандатного механизма разграничения доступа 76

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 87

7.13. Установка опций настройки 103

7.14. Установка фиксированных сетевых имен ресурсов общего пользования 104

7.15. Экспорт/импорт базы данных пользователей и правил разграничения доступа 106

7.15.1. Сохранение/загрузка базы данных пользователей 106

7.15.2. Экспорт/импорт правил разграничения доступа 108

7.16. Формирование списка разрешенных USB устройств и SD карт 111

7.17. Формирование правил доступа для отдельных программ (процессов) 115

7.18. Групповая политика и особенности установки ПРД на контроллере домена Windows 118

8. Заключение 122

Приложение 1. Настройка Startup-пользователя 123

Приложение 2. Файл ACCORD.INI – файл конфигурации СЗИ НСД «Аккорд» 133

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 ЭНП контроллера «Аккорд»
СВТ	– средство вычислительной техники
Синхронизация параметров пользователя	– сопоставление БД пользователей в ЭНП контроллера «Аккорд» с параметрами БД пользователей подсистемы разграничения доступа и 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
ЭНП	– энергонезависимая память контроллера «Аккорд»™

1. Назначение программы

Программа ACED32.EXE – редактор параметров (атрибутов) доступа пользователей, используемых в комплексе СЗИ НСД «Аккорд-Win64» v.5.0 (далее ПАК СЗИ НСД «Аккорд», комплекс «Аккорд» или комплекс) дискреционного и мандатного механизмов доступа субъектов (пользователей) к объектам СВТ или АС – предназначена для администрирования подсистемы разграничения доступом комплекса.

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

Программа ACED32.EXE входит в состав специального ПО комплекса, инсталлируется на жесткий диск СВТ (РС) при установке комплекса.

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 комплекса необходимо запустить программу C:\ACCORD.X64\ACED32.EXE (Выбрать мышкой Пуск>Все программы>Аккорд-Win64>Редактор прав доступа). При запуске программы выполняется синхронизация базы данных редактора прав доступа с базой данных пользователей, находящейся в ЭНП контроллера «Аккорд-АМДЗ», если в настройках комплекса установлен соответствующий флаг. На экран выводится окно идентификации пользователей, показанное на рисунке 1.

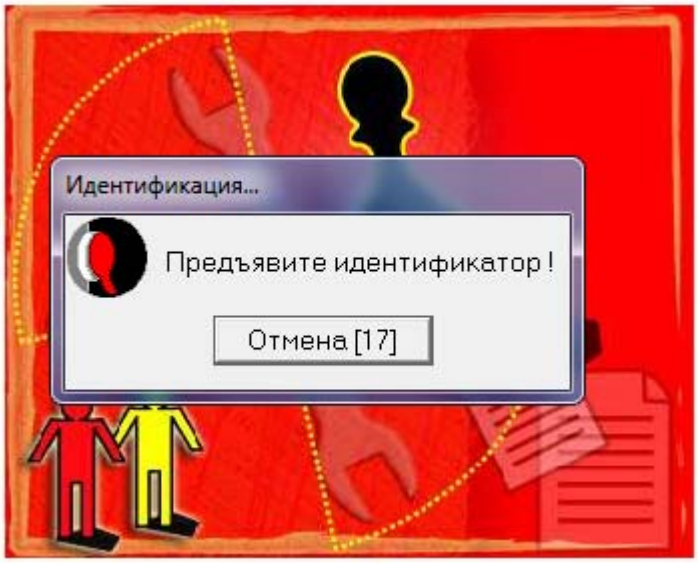

Рисунок 1 - Запрос идентификатора пользователя

Далее программа запрашивает пароль пользователя (если пароль определен при установке комплекса «Аккорд-АМДЗ» и хранится в ЭНП контроллера).

Если процедура идентификации/аутентификации прошла успешно, т.е. пользователь, который предъявил идентификатор и ввел правильный пароль, входит в группу «Администраторы», то на экран выводится 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).

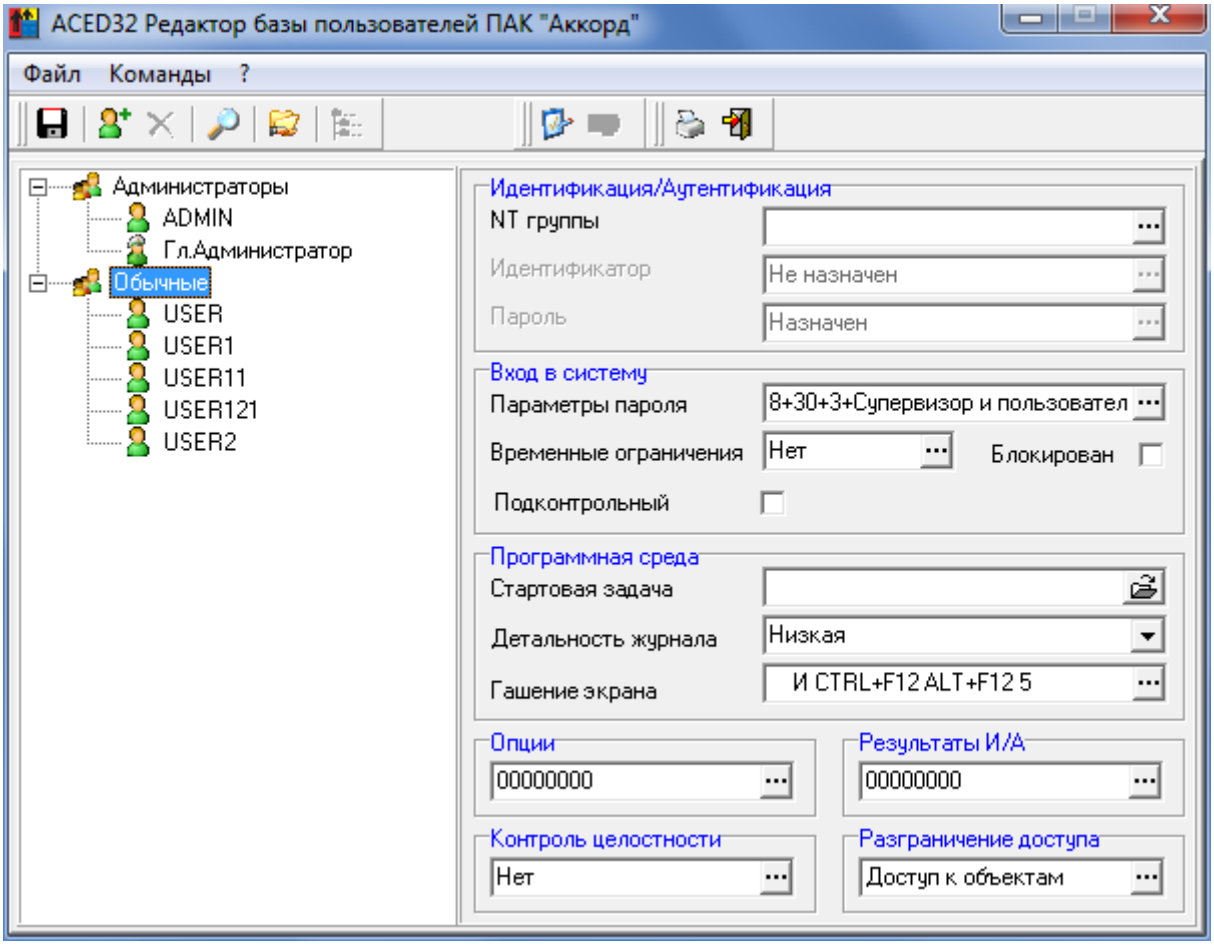

Рисунок 2 - Главное окно программы

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

Сообщение	Причина	Порядок действий
«Неверный или старый файл списка пользователей»	БД пользователей ACED32 не соответствует БД пользователей контроллера «Аккорд»	Нажмите кнопку <OK>. Удалите файл C:\ACCORD.x64\Accord.amz. Запустите программу ACED32.EXE.
«Редактор могут использовать только администраторы»	Введен пароль не соответствующий данному идентификатору.	Введите правильный пароль
«Редактор может использовать только Администратор»	Попытка запуска редактора лицом, не являющимся администратором.	Предъявите зарегистрированный идентификатор администратора, или введите правильный пароль
Выход из ACED32 без предупреждения	Истекло время для предъявления идентификатора	Перезапустите программу ACED32. Предъявите идентификатор 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:

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

если в программе настройки комплекса «Аккорд» установлены флаги «Синхронизация с базой пользователей NT» и флаг «Мандатный +процессы», то при запуске редактора прав доступа на экране появляется сообщение (рисунок 3):

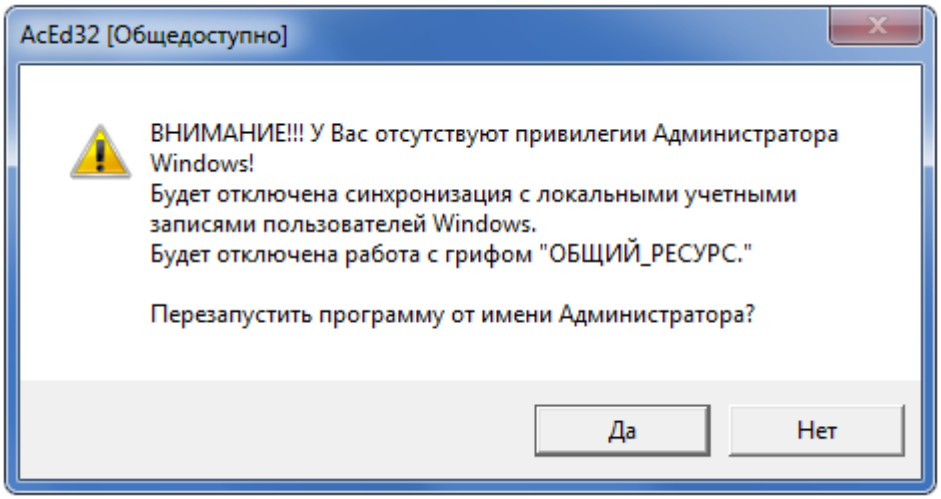

Рисунок 3 – Сообщение, возникающее при запуске редактора прав доступа, в случае если в настройке комплекса установлены флаги «синхронизация с NT», «+процессы»

если в программе настройки комплекса «Аккорд» установлен флаг «Синхронизация с базой пользователей NT», но не установлен флаг «Мандатный +процессы», то при запуске редактора прав доступа на экране появляется сообщение (рисунок 4):

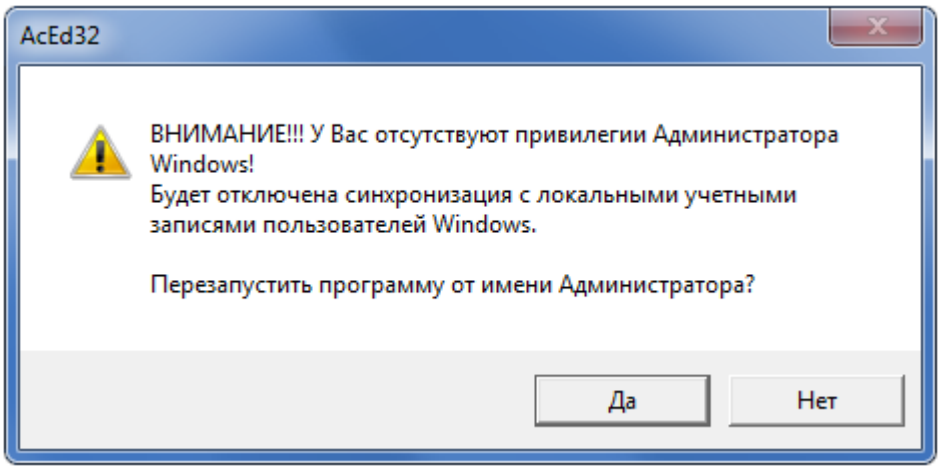

Рисунок 4 - Сообщение, возникающее при запуске редактора прав доступа, в случае если в настройке комплекса установлен флаг «синхронизация с NT» и не установлен флаг «+процессы»

если в программе настройки комплекса «Аккорд» не установлен флаг «Синхронизация с базой пользователей NT», но установлен флаг «Мандатный +процессы», то при запуске редактора прав доступа на экране появляется сообщение (рисунок 5):

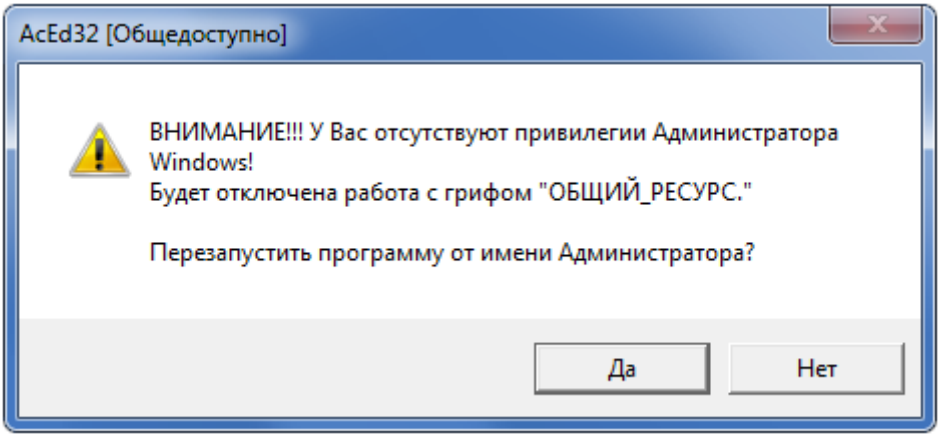

Рисунок 5 - Сообщение, возникающее при запуске редактора прав доступа, в случае если в настройке комплекса не установлен флаг «синхронизация с NT», но установлен флаг «+процессы»

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

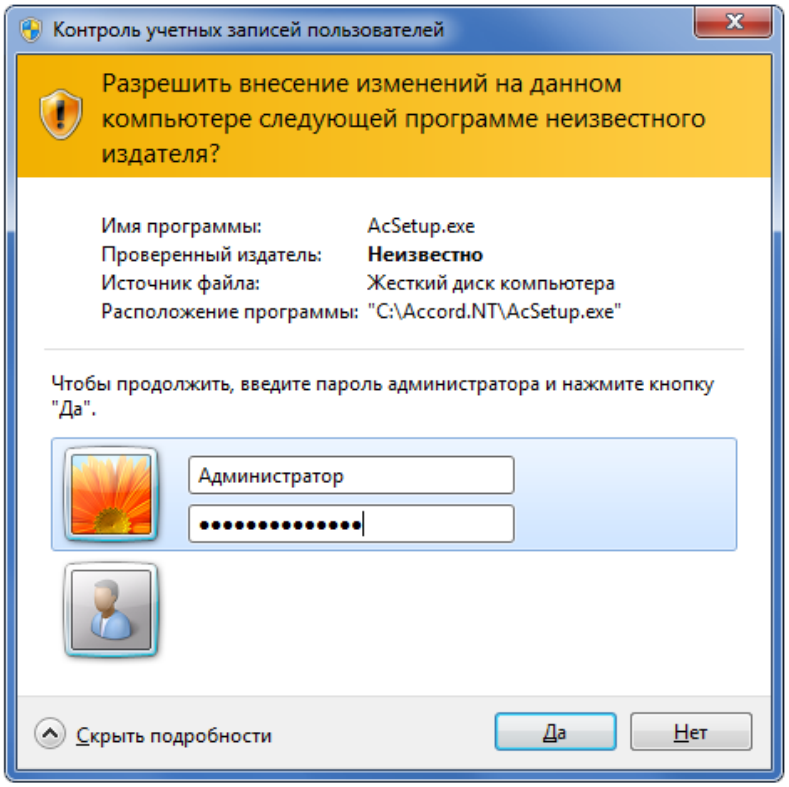

Рисунок 6 – Окно ввода пароля Администратора ОС Windows

После этого на экране появляется главное окно программы ACED32 (рисунок 2), все функции которой доступны (также, как и для Администратора ОС, см. подраздел 2.1).

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

окно программы ACED32, две (или одна из двух)[1] функции которой заблокированы: синхронизация с локальными учетными записями ОС Windows, работа с грифом «ОБЩИЙ_РЕСУРС» (рисунок 7):

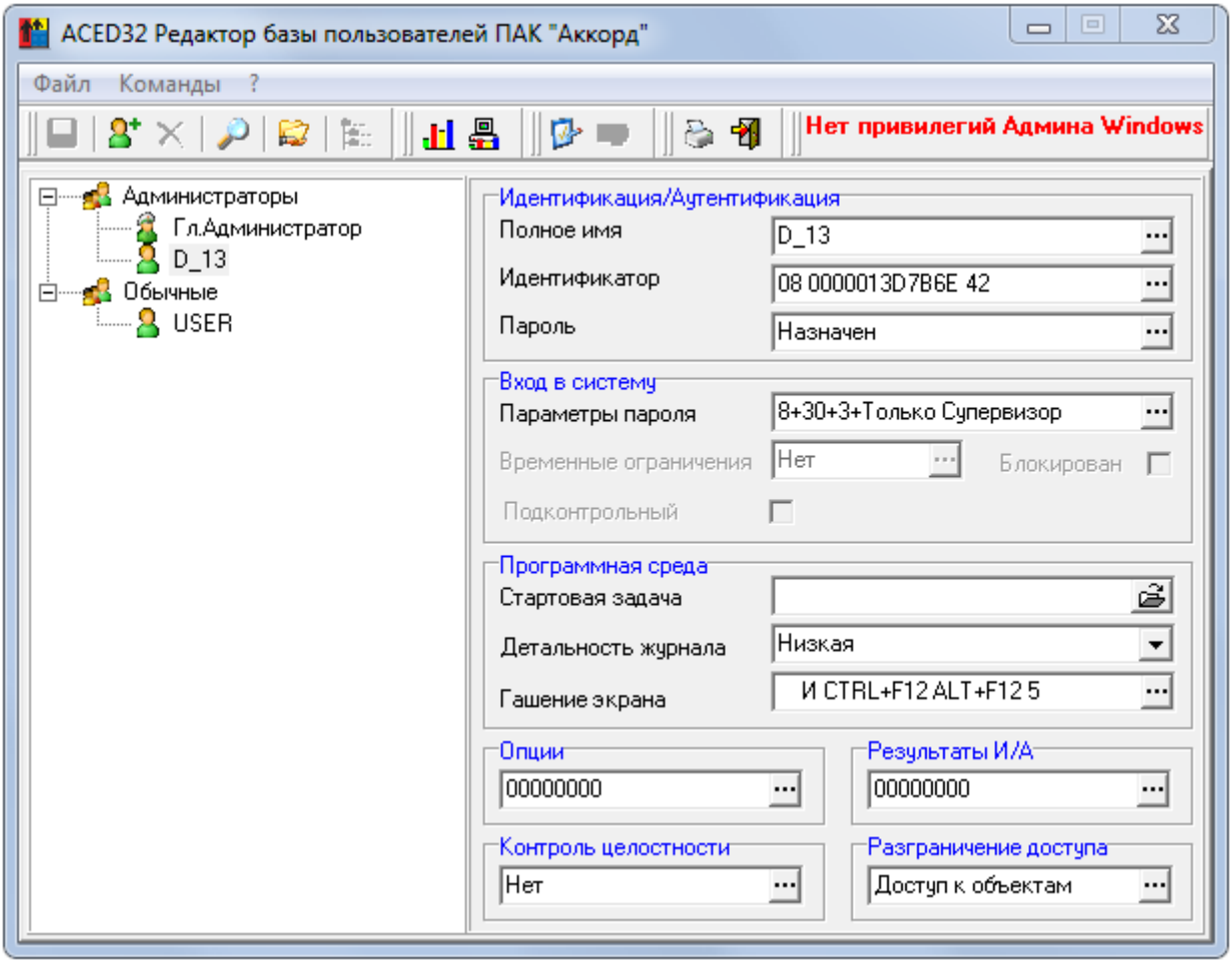

Рисунок 7 - Главное окно программы ACED32 с заблокированными функциями

В случае если Администратор БИ не является Главным Администратором ПАК «Аккорд», и не является Администратором ОС Windows, то он может запустить редактор прав доступа. При этом на экране 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 на экране появляется главное окно программы ACED32, две (или одна из двух)[1]

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

функции 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).

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).

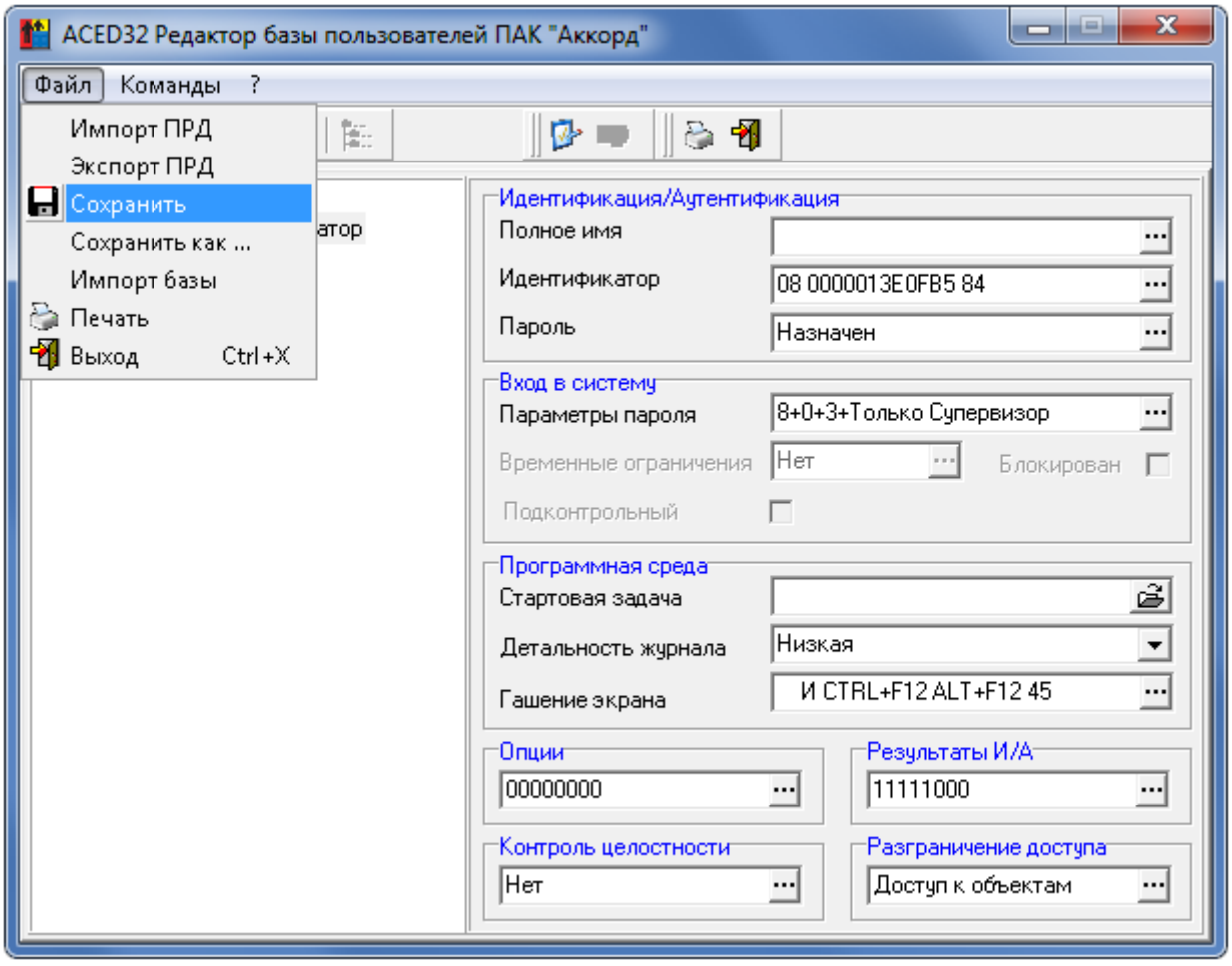

Рисунок 8 – Сохранение настроек

---

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

2.3. Выход из программы

В подменю «Файл» (рисунок 2) выберите команду «Выход»[1] или на панели инструментов нажмите кнопку <Выход из программы>.

Если были внесены изменения в ПРД любого пользователя, то на экран выводится запрос на подтверждение сохранения изменений. При выборе кнопки <ДА> все изменения базы пользователей будут сохранены.

Если в программе настройки комплекса 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 комплекса установлен флаг «Синхронизация с базой пользователей NT», то при выходе из программы ACED32 на экране появляется предупреждение (рисунок 9).

[1)] команде <Выход> в подменю <Файл> соответствуют клавиши <Cttl+X>.

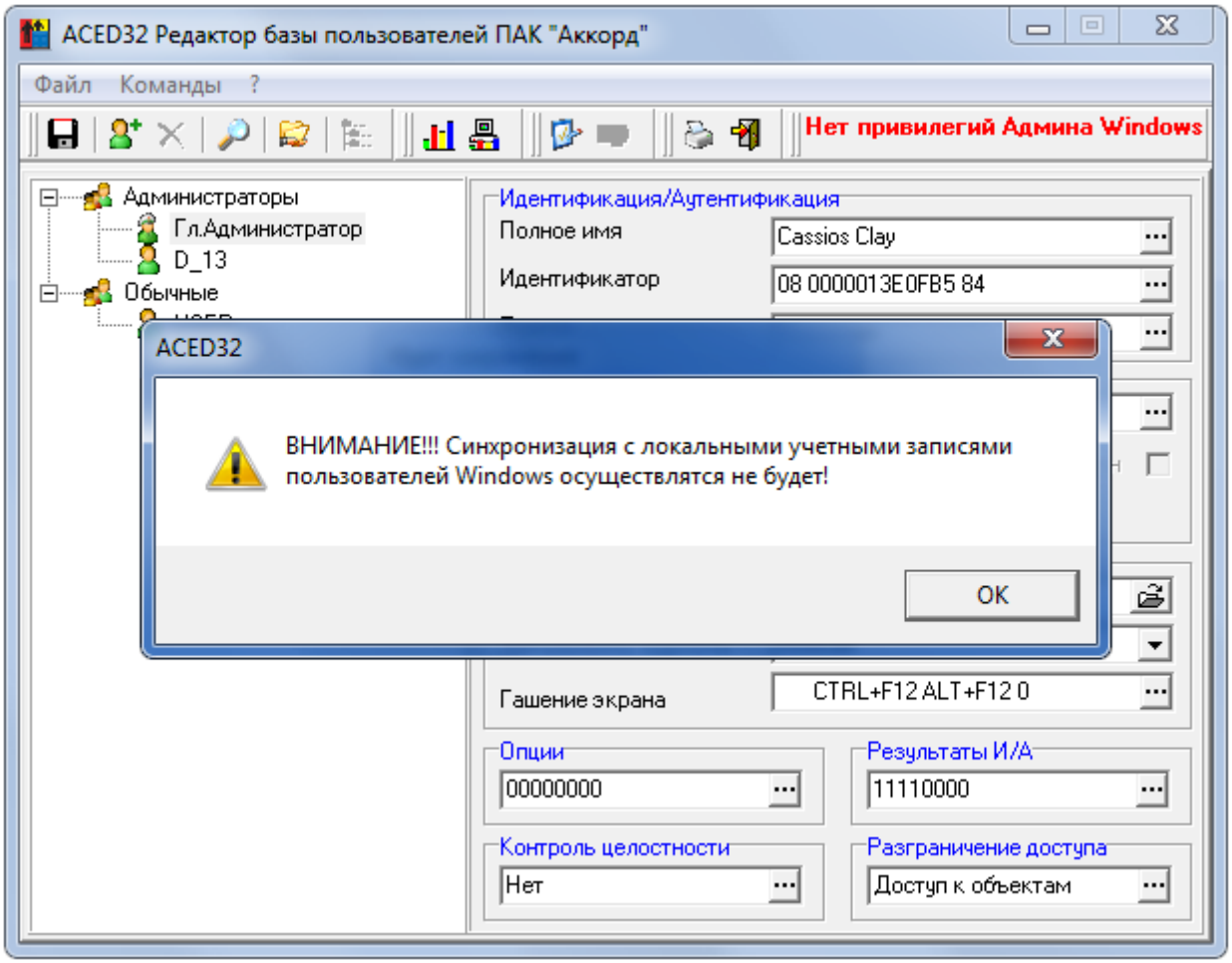

Рисунок 9 - Предупреждение, возникающее при выходе из программы

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

Сообщение	Причина	Порядок действий
«Назначьте пользователю (*имя_пользователя)* пароль!»	Пользователю зарегистрирован идентификатор, но не назначен пароль	Назначить пользователю (*имя_пользователя)* пароль, или отменить использование пароля: в поле «Параметры пароля» (установить инимальную длину пароля - 0)

3. Информация о программе

Выберите команду <?> в меню главного окна программы (рисунок 2). В подменю <?> выберите команду <О программе>. На экран выводится окно, показанное на рисунке 10.

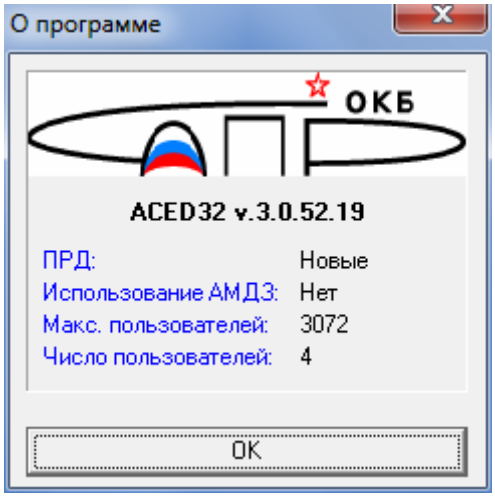

Рисунок 10 - Информация о программе

Информация о программе содержит сведения о версии программы, типе ПРД (см. приложение accord.ini), использовании базы данных контроллера «Аккорд-АМДЗ»; максимальном количестве пользователей, которые могут быть зарегистрированы; типе БД контроллера, разработчике программы. Для продолжения работы нажмите кнопку <ОК> или клавишу <Enter>.

4. Регистрация новой группы пользователей

В подменю «Команды» выберите команду «Создать» (рисунок 11) или нажмите кнопку <Создать> в главном окне программы. На экран выводится окно, предлагающее выбрать тип создаваемого объекта. Установите отметку на строке «Группа» и введите имя новой группы пользователей. После этого следует выбрать кнопку <ОК>. В главном окне программы появится новая группа.

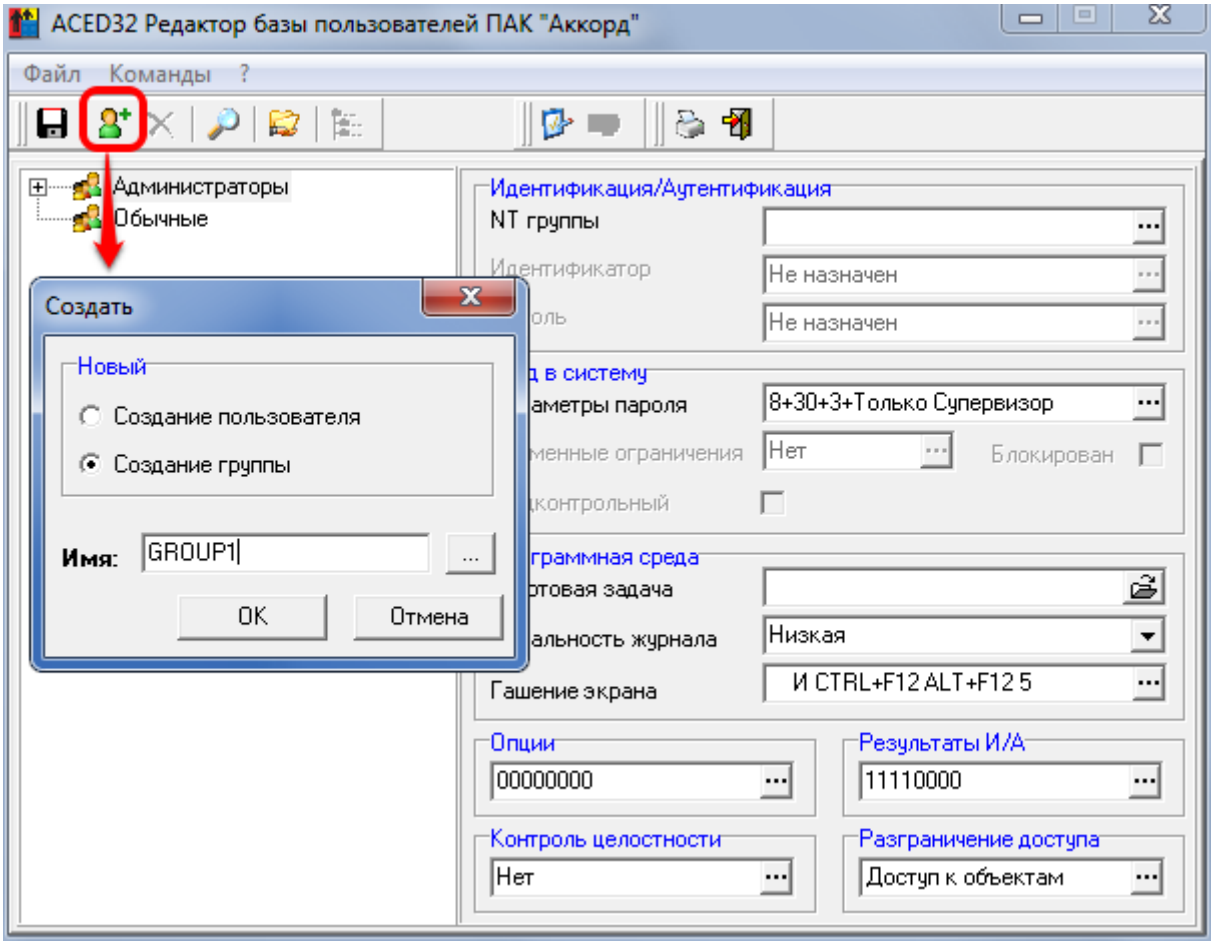

Рисунок 11 – Создание группы пользователей

Для группы можно задать параметры доступа к ресурсам СВТ.

В строке «NT Группа» можно выбрать группу в составе ОС, в которую будут включаться пользователи группы СЗИ «Аккорд» при синхронизации с базой данных пользователей операционной системы.

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 блокировал свой компьютер, то USER2 может разблокировать компьютер пользователя USER1[1]. При этом в ПАК

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

«Аккорд» будет начата новая сессия для USER2. Однако в ОС Windows сессия останется прежней.

ВНИМАНИЕ! Начиная с версии «Аккорд» X.0.9.42 для корректной работы опции «Коллективная работа» необходимо, чтобы в параметрах «Гашения экрана» был установлен флаг «Защита паролем» (рисунок 33).

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 12). После этого следует выбрать кнопку <OK>. В главном окне программы появится новый пользователь.

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

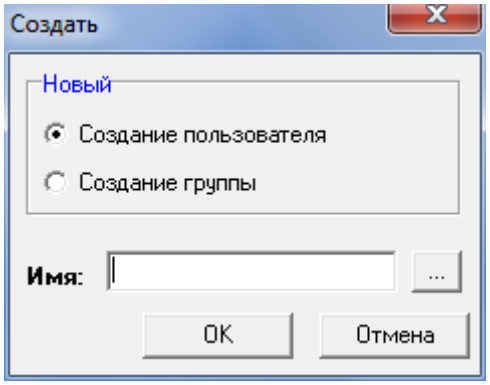

Рисунок 12 - Окно регистрации нового пользователя

Имя пользователя можно ввести с клавиатуры или выбрать из состава пользователей, уже зарегистрированных в ОС. Для этого достаточно нажать кнопку, расположенную справа от поля ввода имени пользователя. Открывается окно списка существующих пользователей (рисунок 13).

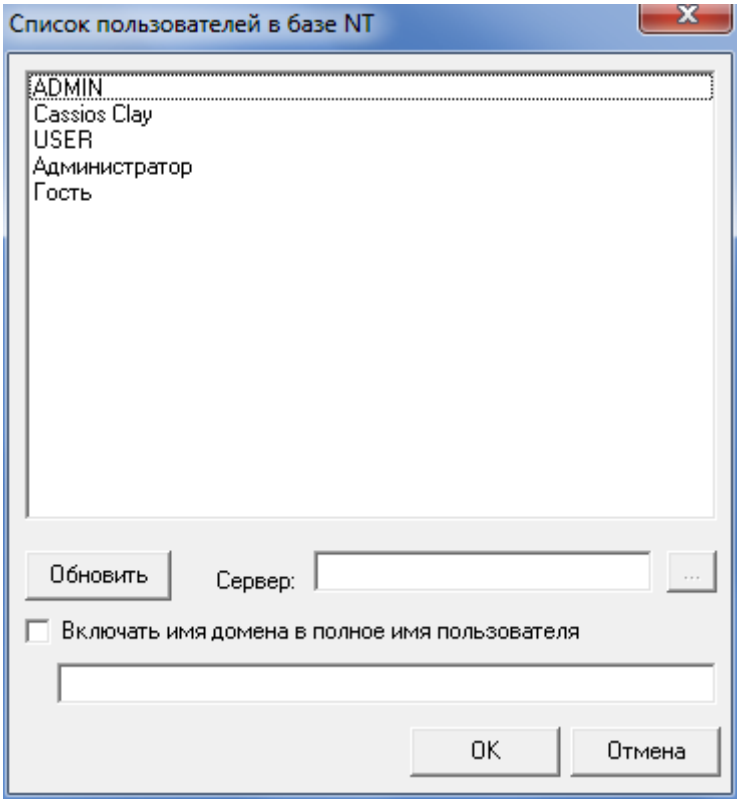

Рисунок 13 - Окно выбора нового пользователя

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.

После нажатия кнопки <OK> запрашивается имя и пароль администратора контроллера домена и, если информация введена правильно, то можно выбрать пользователя из списка. Данная функция недоступна в Windows 7 и Windows 2008 Server.

Если в настройке комплекса установлен флаг «Использовать полное имя в учетных записях Windows NT», то в нижней части окна становится доступным 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>). При этом максимальное количество символов, которое можно установить в поле «Полное имя», ограничивается 34 символами.

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 описываются в пункте 6.17 данного руководства.

ВНИМАНИЕ! В качестве основного имени пользователя можно использовать заглавные латинские буквы, цифры и _ (символ подчеркивания). Это связано с ограничениями, которые существуют в аппаратной части комплекса, с которой синхронизируется список пользователей.

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 (порядковые номера идентификаторов пользователей, хэш-функцию от ключа пользователя, служебные данные) в файл *.atf посредством утилиты AcTmReg.EXE (см. п.п. 2.5.2 документа «Инструкция по установке» 11443195.4012-036 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 необходимо добавить в базу пользователей ПАК «Аккорд» (файл *.amz). Для этого нужно 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 14);

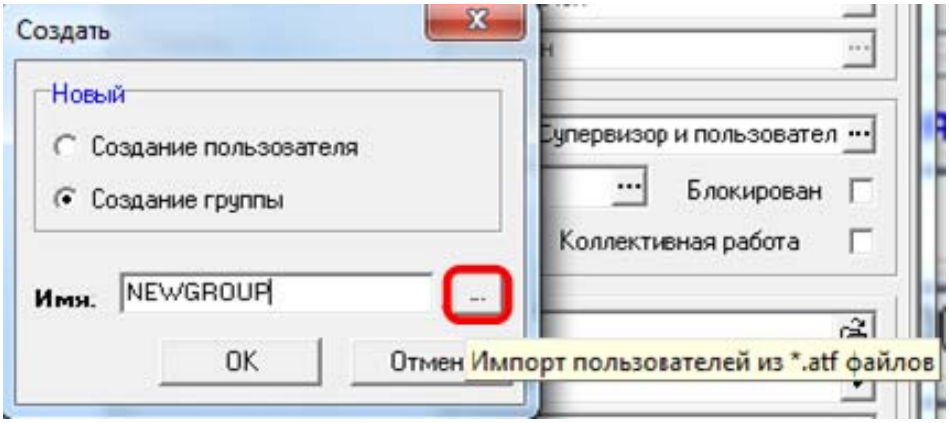

Рисунок 14 – Импортирование пользователей из файла .atf

4. При нажатии кнопки <Импорт пользователей из *.atf файлов> (рисунок 14) на экране появляется окно, в котором нужно выбрать один или несколько файлов формата *.atf и нажать кнопку <Открыть> (рисунок 15);

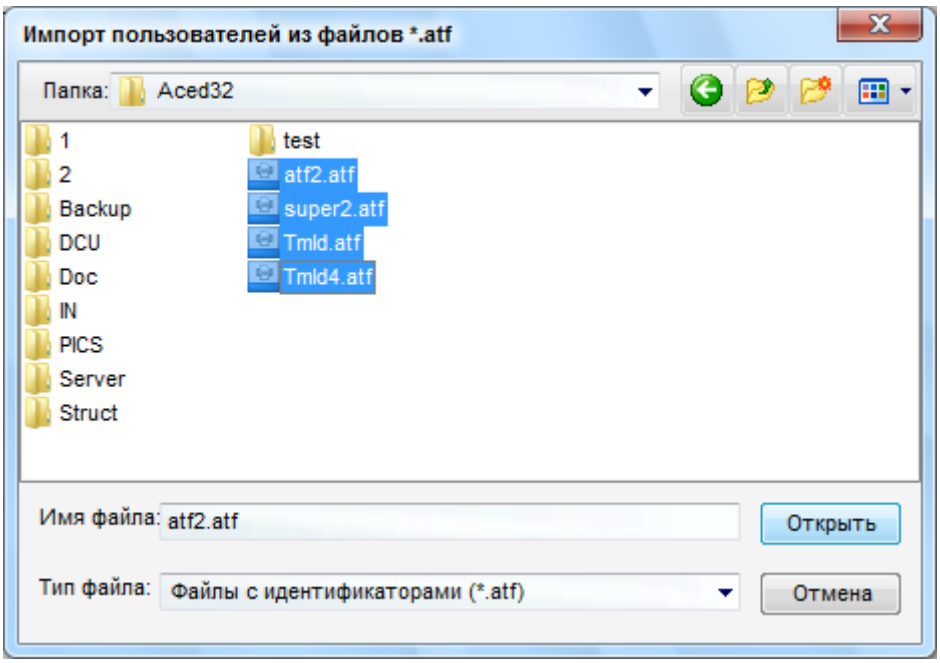

Рисунок 15 – Выбор файлов формата .atf

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». Далее заполнение поля «Полное имя» осуществляется следующим образом:
   - Если в поле «Описание» указано доменное имя учетной записи пользователя (определяется по наличию символов «@» или «\»), то значение этого поля переносится в поле «Полное имя»;
   - Если доменное имя в поле «Описание» не указано, а параметр IncludeDomainName файла конфигурации ACCORD.INI имеет значение «Yes», то доменное имя берется из параметра

«DomainName» файла конфигурации ACCORD.INI, добавляется к «Описанию», и результат записывается в поле «Полное имя» пользователя. Если при этом поле «DomainName» не заполнено, выводится диалоговое окно с предложением добавить текст (рисунок 16);

- Если доменное имя в поле «Описание» не указано, а параметр IncludeDomainName файла конфигурации ACCORD.INI имеет значение «No», то будет выведено диалоговое окно с предложением добавить текст к полному имени (рисунок 16).

При редактировании следует помнить, что количество символов в поле «Полное имя» ограничено 34 символами.

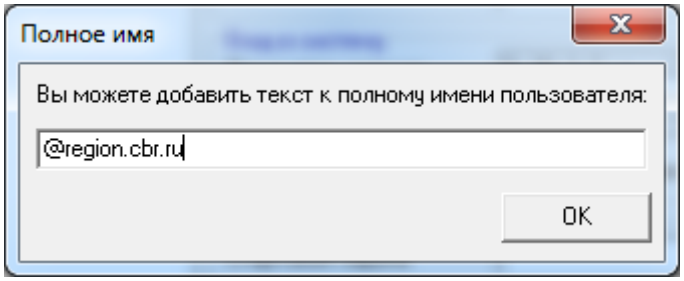

Рисунок 16 – Редактирование полного имени пользователя

6. Для сохранения изменений нужно нажать кнопку <OK> (рисунок 16). 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 ПАК «Аккорд». Если процедура импорта выполняется успешно, то на экране появляется сообщение:

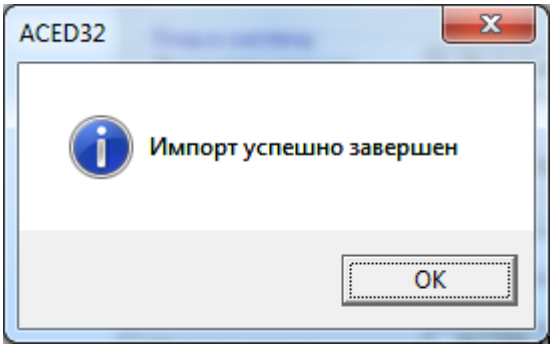

Рисунок 17 – Сообщение об успешном выполнении процедуры импорта пользователей из файлов *.atf в файл *.amz

После успешного выполнения процедуры импорта в базу ПАК «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 на экране появляется сообщение:

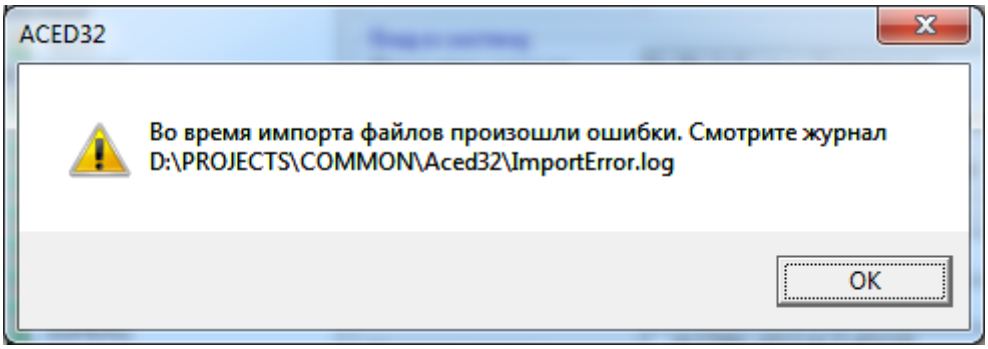

Рисунок 18 – Сообщение об ошибках во время выполнения процедуры импорта пользователей из файлов *.atf в файл *.amz

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

Базу пользователей «Аккорд», содержащуюся в файле *.amz, можно экспортировать в файл *.lst посредством команд, выполняемых в командной строке, со следующими ключами (порядок и регистр ключей не важен):

/convert:filename
/base:basename

Переход на работу с командной строкой осуществляется, если есть хотя бы один ключ.

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.

При запуске программы с ключами командной строки информация выводится на консоль. Все сообщения пропадают через 5 секунд.

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

База из каталога c:\accord.x64 экспортируется в файл c:\users.txt.

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).

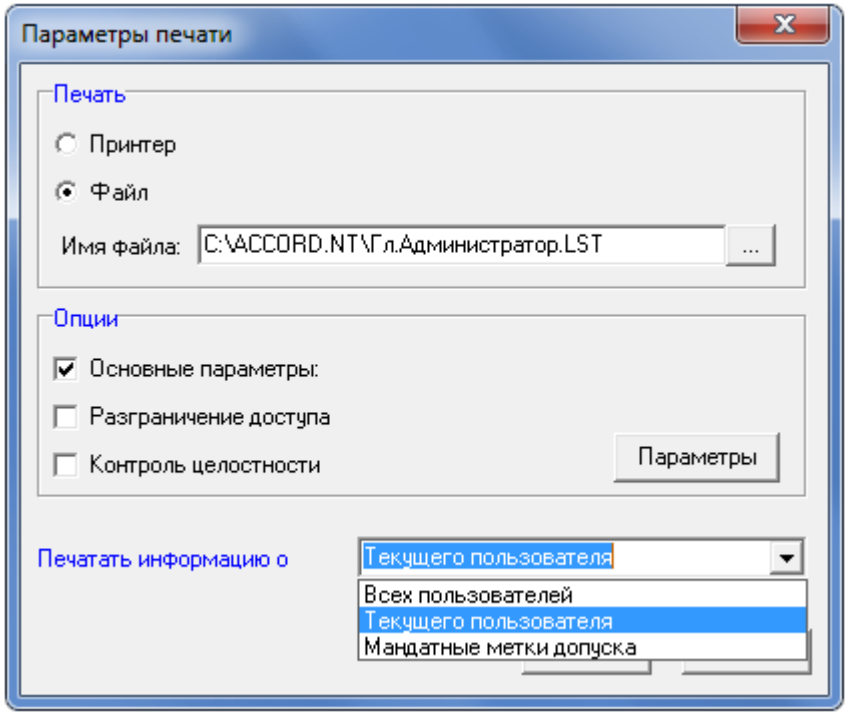

Рисунок 19 - Окно для выбора параметров пользователя и устройства печати

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 рисунок 19.

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

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 <Переименовать>.

На экран выводится окно (рисунок 20), предлагающее ввести новое имя пользователя.

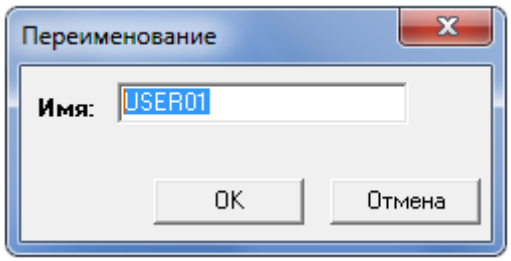

Рисунок 20 - Переименование пользователя

<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. 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 21) с запросом идентификатора.

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

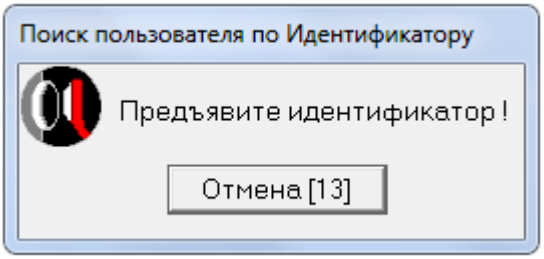

Рисунок 21 - Запрос идентификатора для поиска

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.

На экран выводится окно «Выбор параметров синхронизации», показанное на рисунке 22. Установите те параметры пользователя, которые будут синхронизированы. Для выполнения синхронизации нажмите кнопку <Синхронизация> или клавишу <F2>, для отмены - <Отмена> или <Esc>.

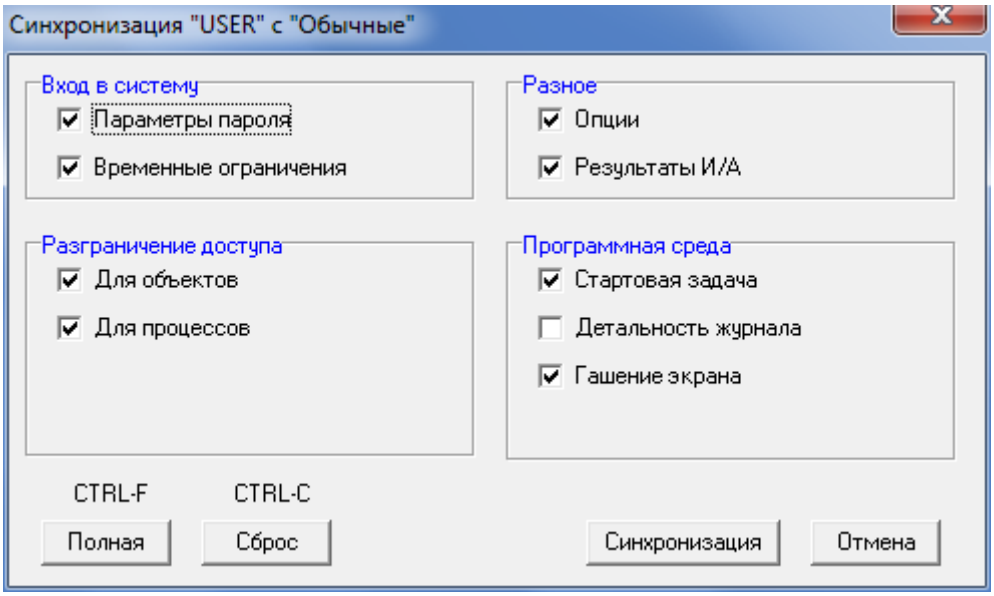

Рисунок 22 - Параметры синхронизации

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

На экран выводится окно «Выбор параметров синхронизации», показанное на рисунке 22. 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 комплекса «Аккорд». 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 контроллера «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 (см. рисунок 23), изменять которые может только главный Администратор:

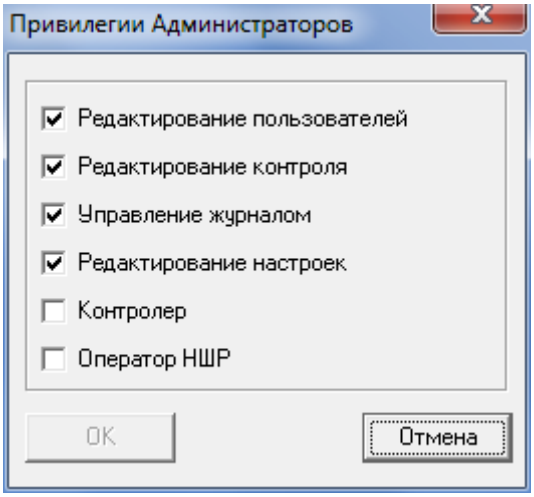

Рисунок 23 – Привилегии Администраторов

Привилегии Администраторов включают в себя 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(см. рисунок 2);
- «Управление журналом» – позволяет выполнять процедуры архивации и разархивации 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» 11443195.4012-055 98, подраздел 2.1);

• «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».

ВНИМАНИЕ! При включении опции «Подконтрольный» для запроса идентификатора контролера при включении компьютера «с нуля», в «Аккорд-АМДЗ» необходимо для выбранного пользователя:

1. включить дополнительно любую опцию из реакций на отключение идентификатора;

2. не включать опцию «Не запрещать автологин....».

В этом случае после выполнения функционала «Аккорд-АМДЗ» будет повторно запрошен идентификатор самого пользователя, а затем идентификатор Контролера.

• «Оператор НШР» - может выполнять выход из Хранителя экрана других пользователей.

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[1].

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/ (при выбранных настройках пользователь может

[1)] В более ранних версиях ПАК «Аккорд-Win64» если у пользователей группы «Администраторы» в разделе «Привилегии Администраторов» снят один из флагов: «Редактирование пользователей», «Управление журналом», «Редактирование журнала», то для такого пользователя действовали правила разграничения доступа СЗИ от НСД «Аккорд», а, значит, ему нужно прописать полный доступ к дискам и к сети. Теперь, в новых версиях ПО «Аккорд-Win64» этого делать не нужно

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 комплекса установлен параметр «Использовать полное имя в учетных записях NT» (подробнее в 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>. На экране появится окно «Работа с ключом пользователя» (рисунок 24).

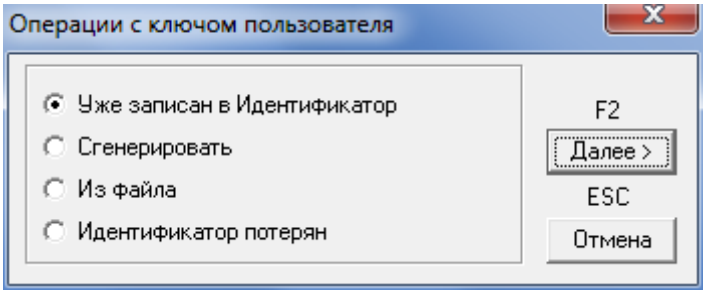

Рисунок 24 - Работа с ключом пользователя

Ключ пользователя генерируется с использованием датчика случайных чисел (ДСЧ), установленного на плате контроллера «Аккорд-АМДЗ», и записывается в энергонезависимую память идентификатора.

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 может быть уже записан в идентификаторе, например, при перерегистрации пользователя, который был уже зарегистрирован в составе комплекса «Аккорд» на другой ПЭВМ (РС), или ключ уже был сгенерирован при регистрации пользователя в контроллере «Аккорд-АМДЗ» из состава комплекса.

После выбора кнопки <Далее> или нажатия клавиши <F2> выдается запрос на считывание серийного номера идентификатора - выводится окно, показанное на рисунке 1. 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 новый ключ и выдается запрос на считывание идентификатора (рисунок 1). 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, 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» 11443195.4012-037 98, подраздел 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.

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

Сообщение	Причина	Порядок действий
«Идентификатор принадлежит пользователю *имя_пользователя*»	Данный идентификатор уже зарегистрирован для пользователя *(указывается имя)*	Нажмите кнопку <ОК>. Предъявите другой идентификатор
«Ошибка чтения ключа!»	Ошибка чтения данных из идентификатора	Нажмите кнопку <ОК>, повторите операцию. Если ошибка повторится, сгенерируйте новый ключ
«Неверный тип идентификатора»	Идентификаторы данного типа не поддерживаются комплексом «Аккорд»	Нажмите кнопку <ОК>. Предъявите другой идентификатор
«Ошибка создания ключа!»	Ошибка записи в идентификатор	Нажмите кнопку <ОК>. Повторите операцию

Если в качестве идентификатора используется устройство RuToken-S, необходимо сначала выполнить процедуру его инициализации в соответствии с «Инструкцией по инициализации RuToken-S», в процессе которой можно изменить пин-код устройства (по умолчанию 12345678).

Если пин-код был изменен, то для идентификации с помощью RuToken-S потребуется ввести актуальный пин-код (рисунок **25**).

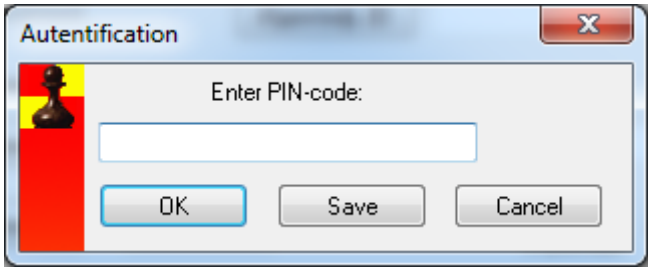

Рисунок 25 - Окно ввода пин-кода RuToken-S

При нажатии кнопки <OK> введенный код будет применен однократно. При нажатии кнопки <Save> пин-код будет применен и сохранен для следующего использования данного RuToken-S.

При использовании стандартного (12345678) или сохраненного пин-кода диалоговое окно (рисунок **25**) выводиться не будет.

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>. На экран выводится окно «Параметры пароля» (рисунок 26).

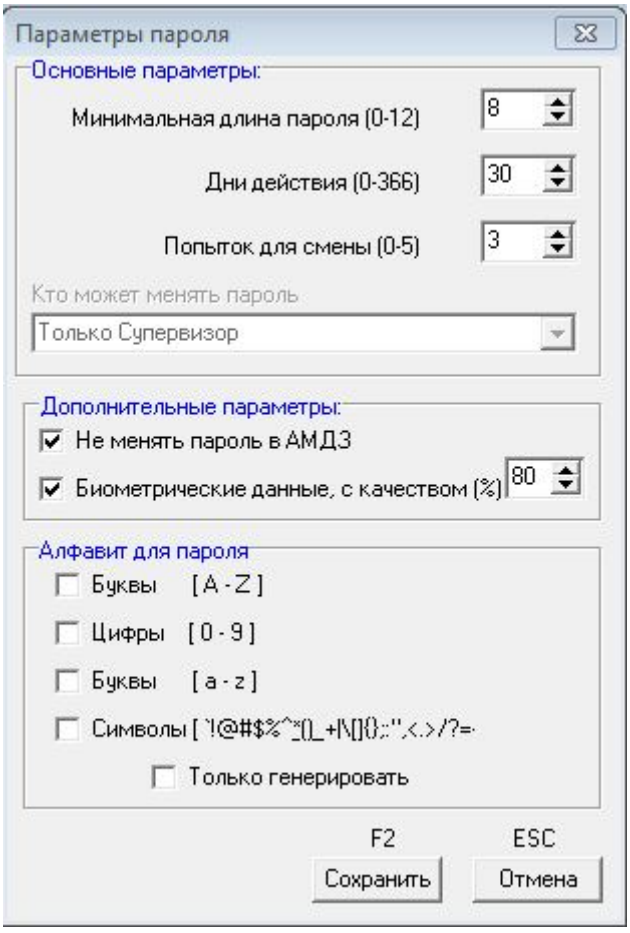

Рисунок 26 - Параметры пароля пользователя

Параметры пароля включают в себя следующие поля:

- «Длина пароля» - минимальная длина пароля – 0 (пароль задавать не обязательно), максимальная - 12 символов.
- «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).
- «Дополнительные параметры»:
  - «Не менять пароль в АМДЗ» - этот флаг необходим для того, чтобы при включенной опции «Синхронизация с базой АМДЗ» (см. документ «ПАК СЗИ от НСД "Аккорд-Win32". Руководство по установке» 11443195.4012-036 98, подраздел 2.2.1) в процессе смены пароля для входа в ОС пароль в АМДЗ не менялся.
  - «Биометрические данные, с качеством (%)» - этот флаг устанавливается в случае применения биометрической идентификации по отпечатку пальца или сосудистому руслу руки (см. п. «Особенности работы утилиты «Настройка идентификаторов СЗИ Аккорд» «Руководства по установке») и определяет процент совпадения предъявляемых биометрических данных с установленным эталонным значением.

ВНИМАНИЕ! При использовании биометрии в ОС Windows XP для параметра «Биометрические данные, с качеством (%)» необходимо указывать следующие значения:

1. для сосудистого русла – не ниже 80;
2. для отпечатка пальца – не ниже 60.

- «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, расположенную справа в поле «Пароль» или клавишу <Enter>. На экране появится окно «Ввод пароля» (рисунок 27).

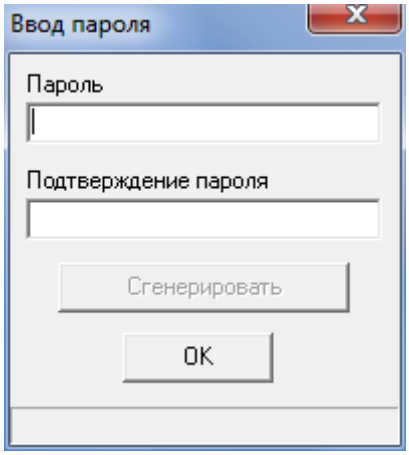

Рисунок 27 - Задание пароля пользователя

Введите пароль и повторите ввод пароля для подтверждения (следует помнить, что максимальная длина пароля ограничена 12 символами). 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 28).

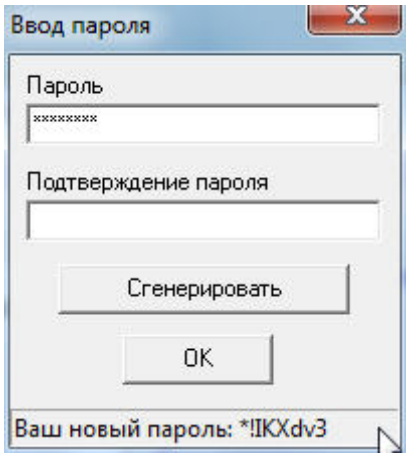

Рисунок 28 - Ввод пароля с использованием процедуры генерации

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

Сообщение	Причина	Порядок действий
«Такую комбинацию символов недопустимо использовать в качестве пароля»	При вводе пароля контролируется нажатие последовательно расположенных клавиш	Используйте другой пароль
«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	Количество введенных символов меньше	Введите пароль из большего количества символов, или

(указывается число) символов»	установленной минимальной длины пароля	уменьшите минимальную длину в параметрах пароля
«Вы ошиблись - начинаем все сначала»	Ошибка при повторном вводе пароля	Повторите процедуру ввода пароля заново

При смене пароля в ОС Windows (посредством команды Ctrl-Alt-Del -> «Сменить пароль») или при попытке войти в ОС Windows может возникнуть ситуация, при которой старый пароль в ОС и в АМДЗ не совпадают. Например, если пользователь сменил пароль в AD на одном компьютере, а затем пытался сменить пароль на другом компьютере. Или в настройках учетной записи пользователя в ОС Windows стоит флаг «Потребовать смену пароля при следующем входе в систему». Чтобы избежать подобных ситуаций в СПО «Аккорд-Win64» реализован следующий механизм: в процессе смены пароля в ОС в поле «Старый пароль» необходимо указать старый пароль для ОС Windows. Если процедура смены пароля в ОС успешно выполнена, то начинается процедура смены пароля в контроллере АМДЗ. Если старый пароль для АМДЗ введен некорректно, то на экране появляется предупреждение: «Введите старый пароль для АМДЗ». Процедура смены пароля в контроллере также осуществляется по этому паролю. При этом если старый пароль ввести некорректно более 5 раз, то контроллер блокируется. Чтобы избежать подобной ситуации в окне смены пароля контроллера отображается счетчик попыток ввода старого пароля, количество которых должно быть не больше 5.

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 29). Значение поля «Детальность журнала» выбирается из списка, который раскрывается при щелчке мышью по кнопке, расположенной справа.

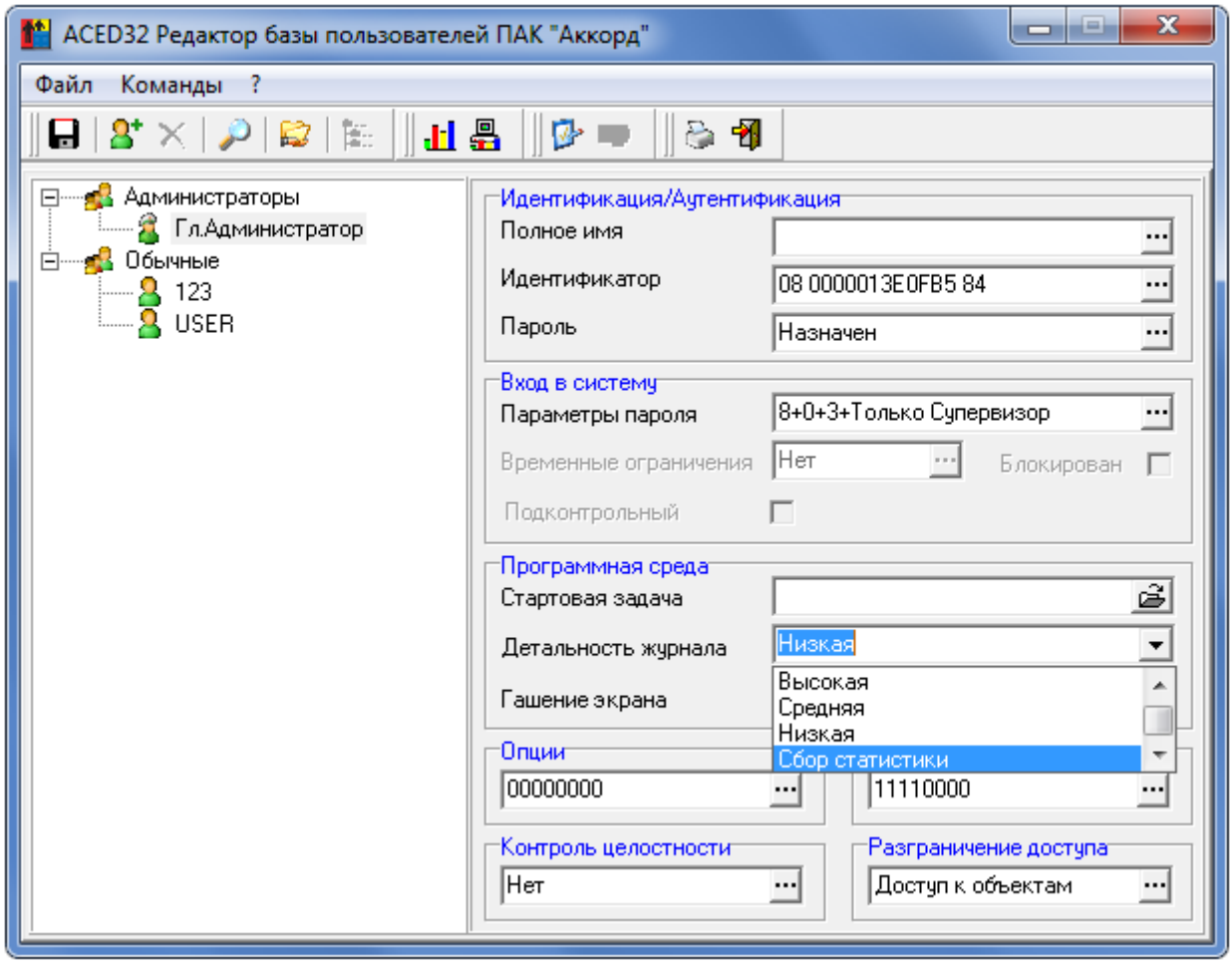

Рисунок 29 – Выбор детальности журнала

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 30).

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 30 – Журнал событий с низкой детальностью

- «Средняя» - то же, что при низкой детальности, плюс операции доступа к файлам и каталогам (рисунок 31).

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 31 - Журнал событий со средней детальностью

- «Высокая» - то же, что и при средней детальности плюс все файловые операции, включая параметры команд (рисунок 32).

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 32 - 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[1]. 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 экране 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 по нажатии кнопки <ОК>, однако кнопка становится доступной по истечении 20 секунд с момента появления сообщения[2]. 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

---

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

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

«неактивности» пользователя, либо по нажатию комбинации горячих клавиш «Гашение» (по умолчанию установлена комбинация <Ctrl+F12>). Вернуться в рабочий режим можно только при помощи того идентификатора пользователя, который начал 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 33).

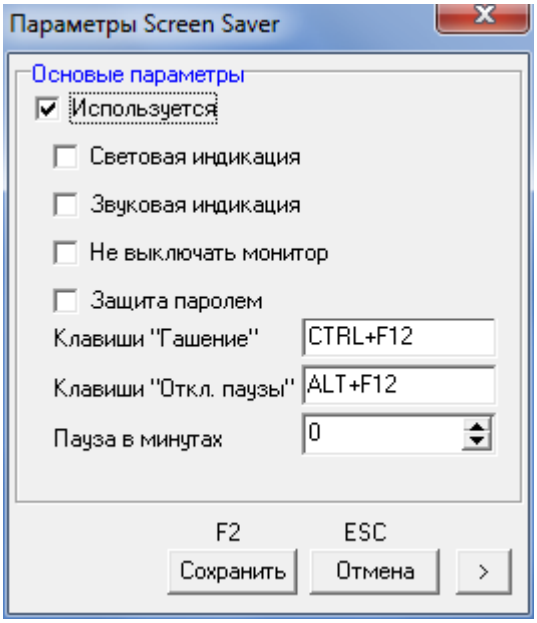

Рисунок 33 - Параметры гашения экрана

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[1].

«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 через указанное время. Такой режим может быть полезен на рабочих станциях, которые осуществляют мониторинг сети, почты и т.д.

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

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

Можно установить комбинацию клавиш принудительного включения Screen Saver – в поле Клавиши «Гашение» (по умолчанию <Ctrl+F12>). Предусмотрена установка комбинации клавиш «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 по нажатии кнопки <Гашение экрана> появляется предупреждение о том, что в версии TSE возможна только блокировка компьютера (рисунок 34):

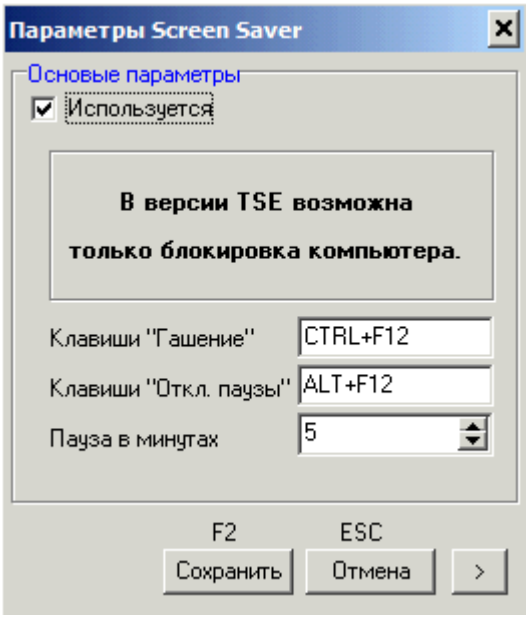

Рисунок 34 – Параметры гашения экрана в режиме терминальной сессии

В нижнем правом углу окна настроек Screen Saver находится кнопка со стрелкой. При нажатии на эту кнопку открывается поле дополнительных параметров блокировки (рисунок 35). 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.

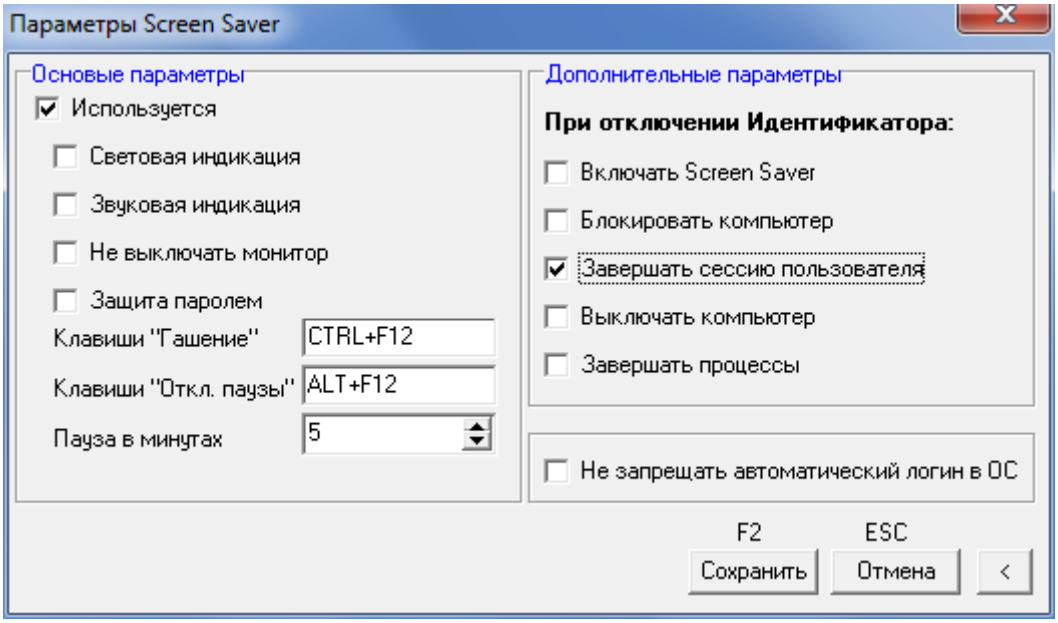

Рисунок 35 - Дополнительные параметры блокировки компьютера[1]

Примечание: В режиме терминальной сессии по нажатии кнопки со стрелкой в нижнем правом углу окна «Параметры Screen Saver» на экране появляется окно с предупреждением о том, что в версии TSE возможна только блокировка компьютера (рисунок 36):

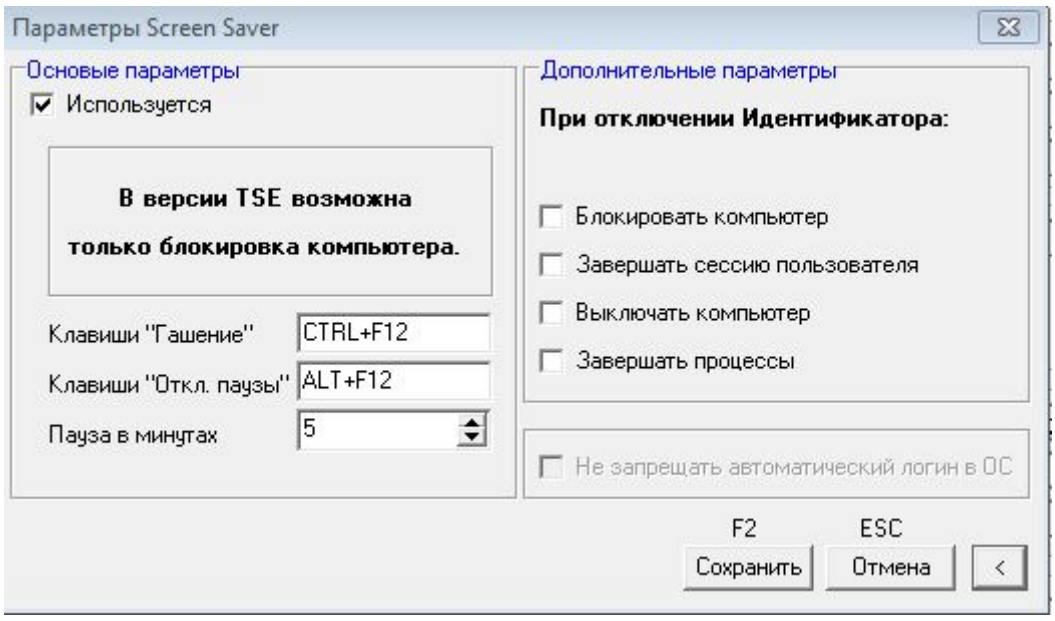

Рисунок 36 - Дополнительные параметры блокировки компьютера в режиме терминальной сессии

В окне, показанном на рисунке 36, можно выбрать дополнительные параметры блокировки. Настройка дополнительных параметров позволяет

[1)] В случае необходимости одновременного использования параметра Screen Saver «Блокировать компьютер» и флага «Автоматический логин» (см. документ «Руководство по установке» 11443195.4012-037 98) рекомендуется установить флаг «Не запрещать автоматический логин в ОС» (см. рисунок 35)

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 35). В терминальной сессии хранитель экрана не включается по 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[1]: 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 по нажатии 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.

[1)] Реакция на извлечение идентификатора отсутствует при использовании в качестве идентификатора устройства ШИПКА-1.68

7.7. Установка временных ограничений для сеанса работы и учетной записи 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. Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «Временные ограничения», или клавишу <Enter>. На экран выводится окно «Временные ограничения для (*указывается имя_пользователя)*» (рисунок 37).

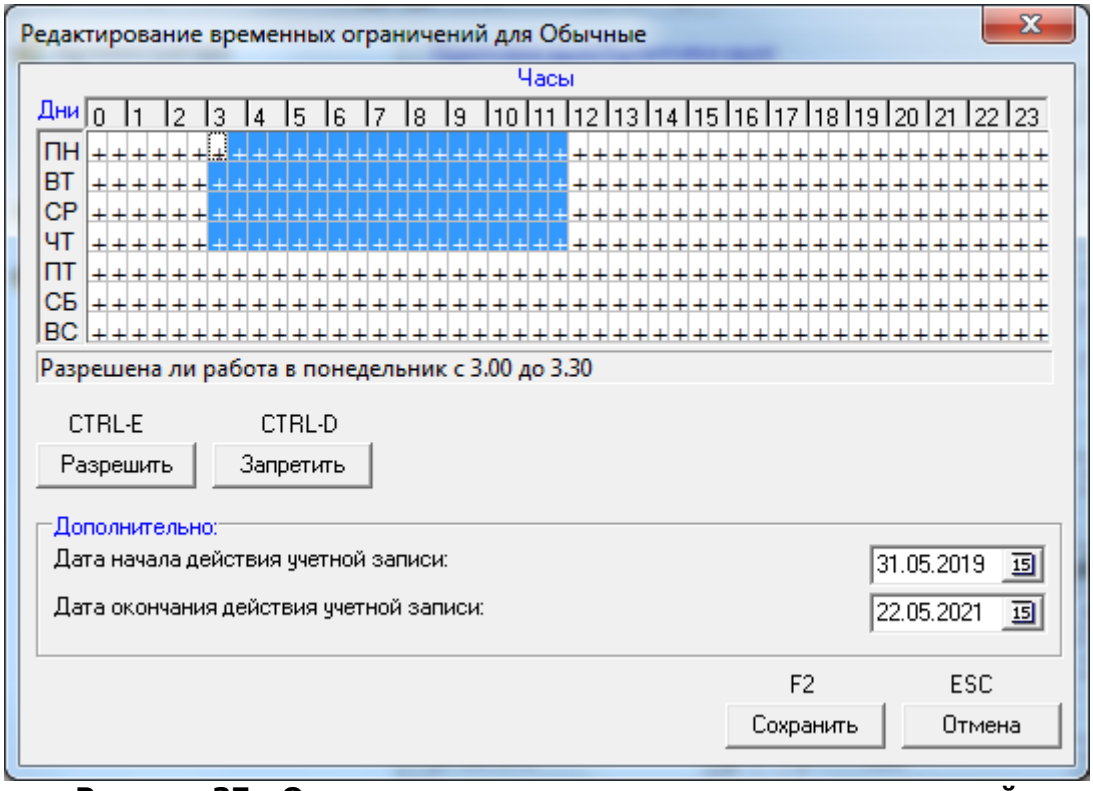

Рисунок 37 - Окно редактирования временных ограничений

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> или клавиши <Ctrl+E>. Для запрета работы в выделенной области необходимо нажать кнопку <Запретить> или клавишу <Ctrl+D>. Двойное нажатие мыши (или клавиши <Пробел>) на ячейку меняет ее значение на противоположное. Перемещение по таблице возможно как при помощи мыши, так и при помощи клавиатуры.

В поле «Дополнительно» 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 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.

ВНИМАНИЕ! Данный флаг поддерживается внутренним ПО «Аккорд АМДЗ» версии 02.01.007 и выше!

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 выводится 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 комплекса СЗИ «Аккорд» (рисунок 38).

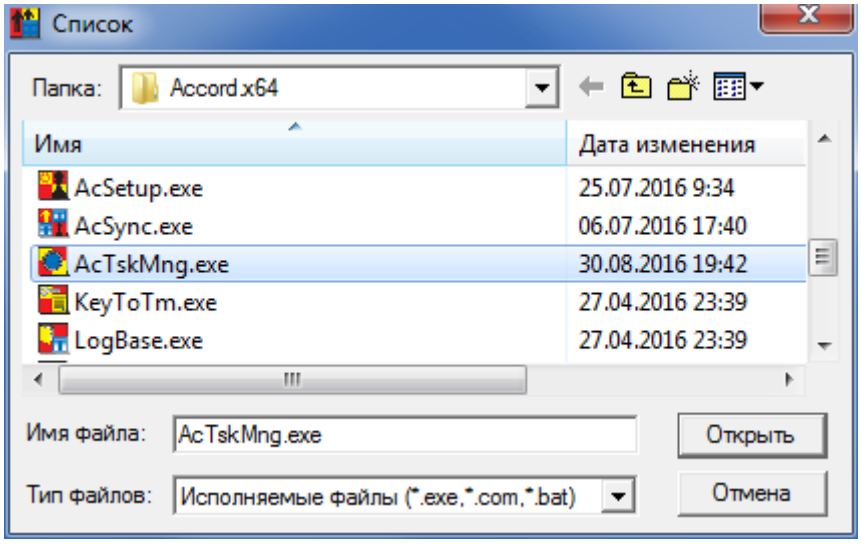

Рисунок 38 - Выбор стартовой задачи – менеджера приложений СЗИ «Аккорд»

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 качестве задачи для запуска 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.

Задачи пользователя можно объединять в группы по функциональному признаку. Если в файле используются русские наименования группы, или задачи, то они должны вводится в «windows» кодировке. Файл .ACT должен выглядеть следующим образом:

```
[Group1]
GroupName=File managers
[Task1.1]
DisplayName=FAR Manager
ImagePath=C:\Program Files\Far\far.exe
[Task1.2]
DisplayName=Norton Commander
ImagePath=c:\NC\nc.exe
Parameters=/V
[Group2]
GroupName=Офисные приложения
[Task2.1]
```

```
DisplayName= Excel
ImagePath=C:\Program Files\Microsoft Office\Office\Excel.exe
[Task2.2]
DisplayName= Winword
ImagePath=C:\Program Files\Microsoft Office\Office\winword.exe
[RUN_BEFORE]
GroupName=Предварительный запуск
[RunTask1]
DisplayName=IntelExtrimGraphics
ImagePath=c:\Program Files\Intel\IEG.exe
[RunTask2]
DisplayName=SoundMax
ImagePath=c:\Program Files\SM\smax3cp.exe
```

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

Если нет необходимости разбивать задачи на группы, то администратор может задать простой список в файле .ACT. В этом случае формат файла следующий:

```
[Task1.1]
#Комментарий
DisplayName=FAR Manager
ImagePath=C:\Program Files\Far\far.exe
[Task1.2]
DisplayName=Norton Commander
ImagePath=c:\NC\nc.exe
Parameters=/V
[Task1.3]
DisplayName= Excel
ImagePath=C:\Program Files\Microsoft Office\Office\Excel.exe
[Task1.4]
DisplayName= Winword
ImagePath=C:\Program Files\Microsoft Office\Office\winword.exe
```

В файле .ACT имеется возможность изменения значения параметра WorkDir. В этом случае для программы, заданной в параметре ImagePath, указывается рабочий каталог, аналогичный определенному (каталогу) в параметре WorkDir:

```
[Task2.1]
DisplayName=Acdsee
ImagePath=C:\Program Files\ACDSee32\Shortcuts\ACDSee32.lnk
WorkDir=C:\Program Files
```

```
Parameters=c:\test.jpg
WaitEndTask=No
[RUN_BEFORE]
GroupName=Предварительный запуск
```

В результате при старте монитора разграничения доступа запустится оболочка AcTskMng со списком программ, доступных для выполнения данным пользователем (рисунок 39).

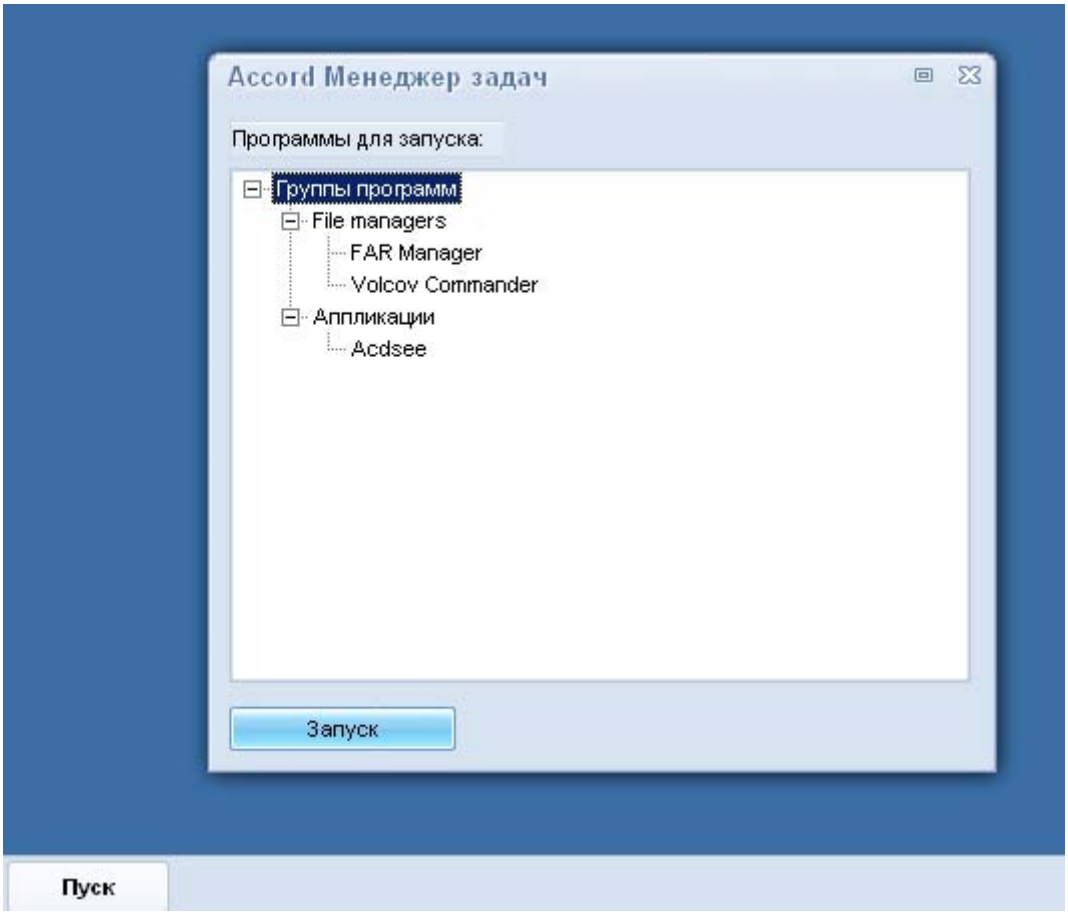

Рисунок 39 - Менеджер задач СЗИ «Аккорд»

По нажатии кнопки <Пуск> на экране появляется меню (рисунок 40).

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

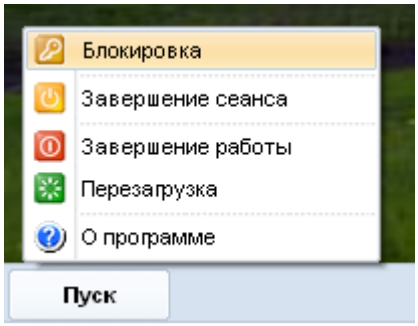

Рисунок 40 – Меню менеджера задач СЗИ от НСД «Аккорд»

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 40) на экране появляется информация о программе, а также информация о сессии пользователя (версия драйвера разграничении доступа, дата и время начала сессии пользователя, именя пользователя, дата и время завершения сессии пользователя[1]).

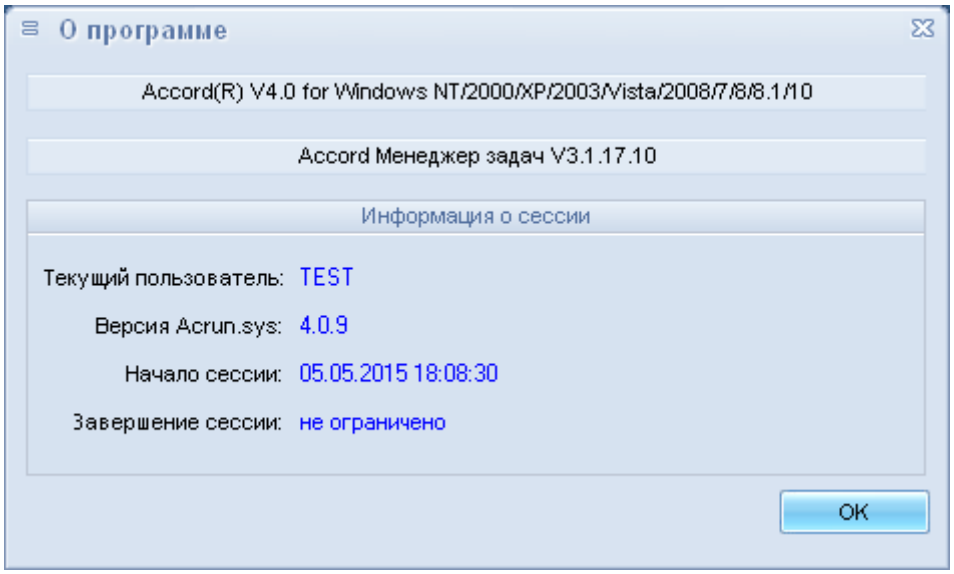

Рисунок 41 – Информация о программе

В качестве исполняемых задач можно задавать файлы типа .lnk. Кроме этого, можно управлять режимом запуска программы AcTskMng.exe. В папке Accord.x64 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).

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

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.

ВНИМАНИЕ! Если при установке стартовой задачи в опциях пользователя (см. подраздел 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 ShowTrayIcons=Yes позволяет выводить на панель задач в правом нижнем углу окна AcTskMng.exe иконки из системного трэя (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);

для корректного отображения иконок в системном трэе 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 СЗИ НСД «Аккорд» можно реализовать с помощью мандатного 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

Комплекс СЗИ НСД «Аккорд-Win64» v.5.0 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 и обновление контрольных сумм при завершении сеанса работы 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 файлов для *(указывается имя_пользователя)*», показанный на рисунке 42.

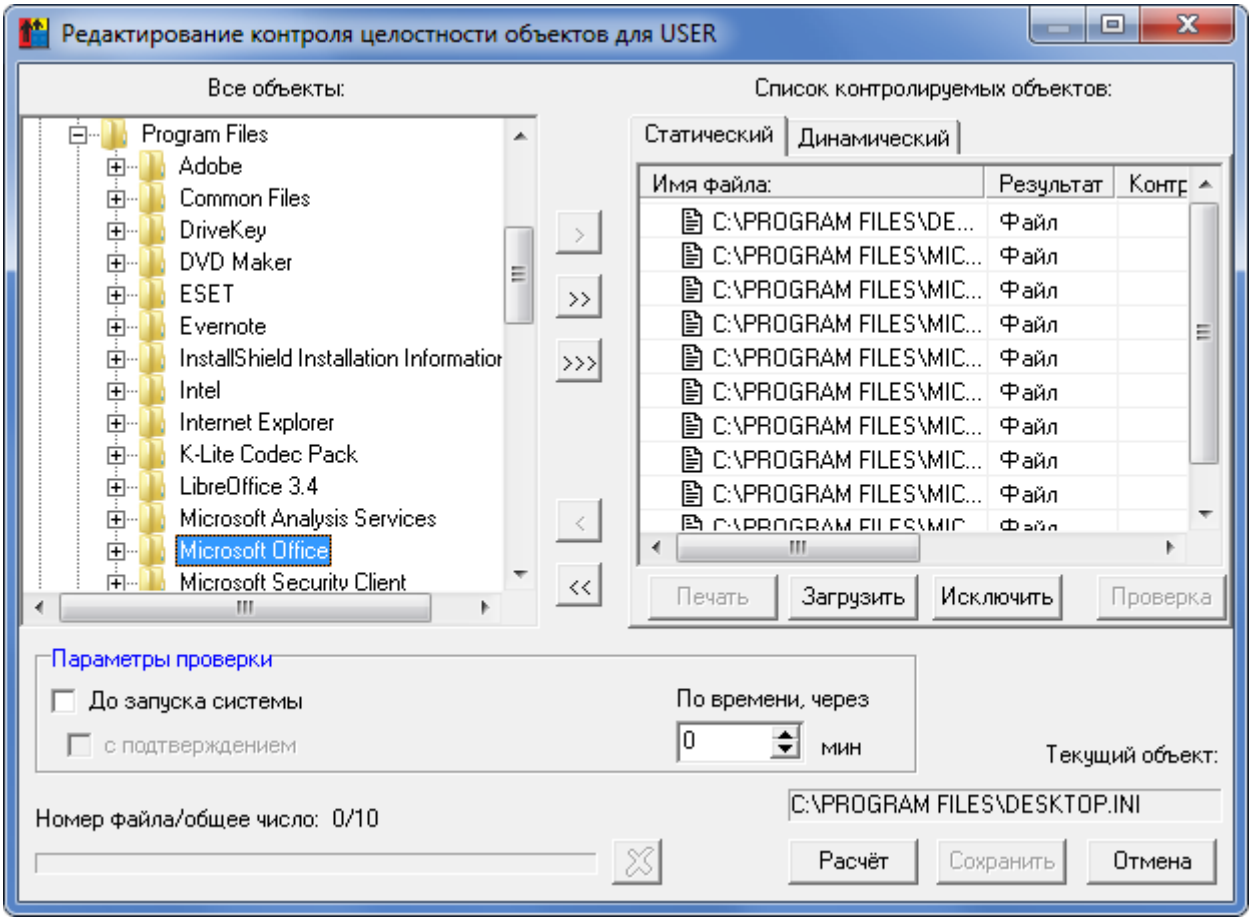

Рисунок 42 - Окно контроля целостности файлов

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

В разделе «Все папки» выберите нужный каталог с помощью мыши (левая кнопка). При нажатии на кнопку «>>», все файлы данного каталога переместятся в «Список контролируемых файлов». Щелчок правой кнопкой мыши на имени выделенного каталога вызывает всплывающее меню с пунктом «Добавить по фильтру». При выборе данного пункта выводится окно (рисунок 43), 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 файлов». Клавиша <Esc> отменяет операцию «Добавить по фильтру».

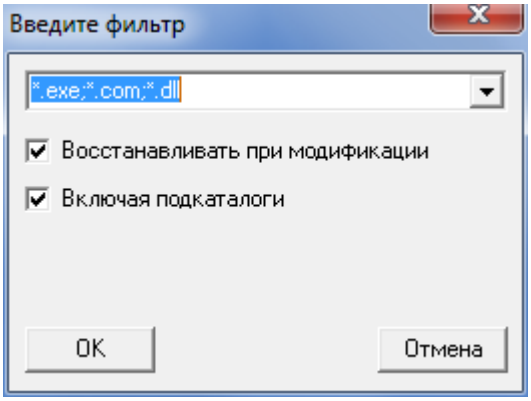

Рисунок 43 - Задание фильтра для выбора контролируемых файлов

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 44).

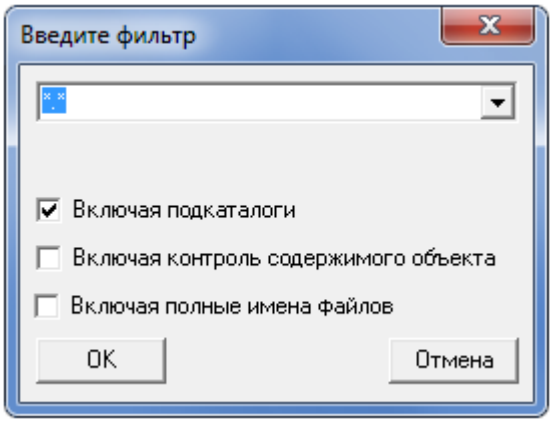

Рисунок 44 - Задание фильтра для контейнера объектов

Флаг «Включая подкаталоги» действует стандартно. Флаг «Включая полные имена файлов», добавляет контроль полного пути. Контрольная сумма содержимого самих файлов не вычисляется. В списке контролируемых объектов сохраняется одна запись с результирующей хэш-функцией. Нарушение целостности выявится при изменении состава контролируемых объектов, т.е. при удалении существующих, или добавлении новых файлов, или папок. Такая процедура контроля может успешно использоваться, если установлен режим автоматического обновления компонентов ПО из доверенного источника, а состав файлов не меняется.

Флаг «Включая контроль содержимого объектов» добавляет следующий уровень контроля, т.е. рассчитывается хэш-функция содержимого каталога и содержимого файлов. В контейнере хранится полный список файлов с контрольной суммой для каждого объекта. При обнаружении нарушений в журнал записывается имя контейнера и имя файла, у которого не совпадает контрольная сумма с эталонным значением.

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 файлов» можно нажав на кнопку «<<». Удалить файл из «Списка контролируемых файлов» 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[1]:

- *«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.
- *«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.

[1)] В ОС Windows Vista и выше флаг «При выходе из системы» отсутствует

При установке флагов «До запуска системы» и «С подтверждением» запрос подтверждения КЦ до запуска ОС не производится, контроль целостности выполняется автоматически.

Примечание: если на компьютере с ОС Vista и выше установлена опция автоматической блокировки (по нажатии комбинации клавиш C-A-D), то при установке флага «При выходе из системы» контроль целостности выполняется по завершении сессии пользователя.

Если на компьютере с ОС Vista и выше установлена опция автоматической блокировки, то при установке флага «При выходе из системы» контроль целостности выполняется по нажатии клавиш C-A-D.

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 45).

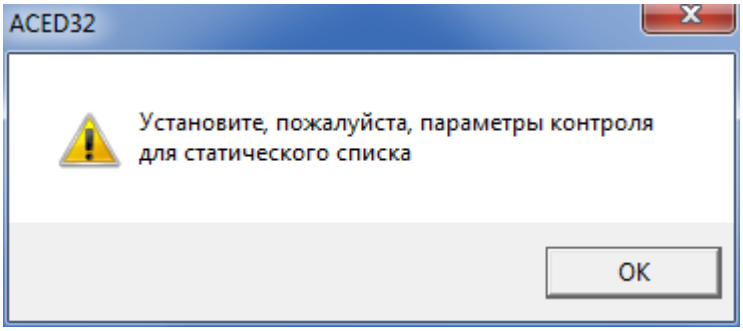

Рисунок 45 - Предупреждение о необходимости установки режимов контроля

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» и откроется список файлов для динамического контроля, показанный на рисунке 46.

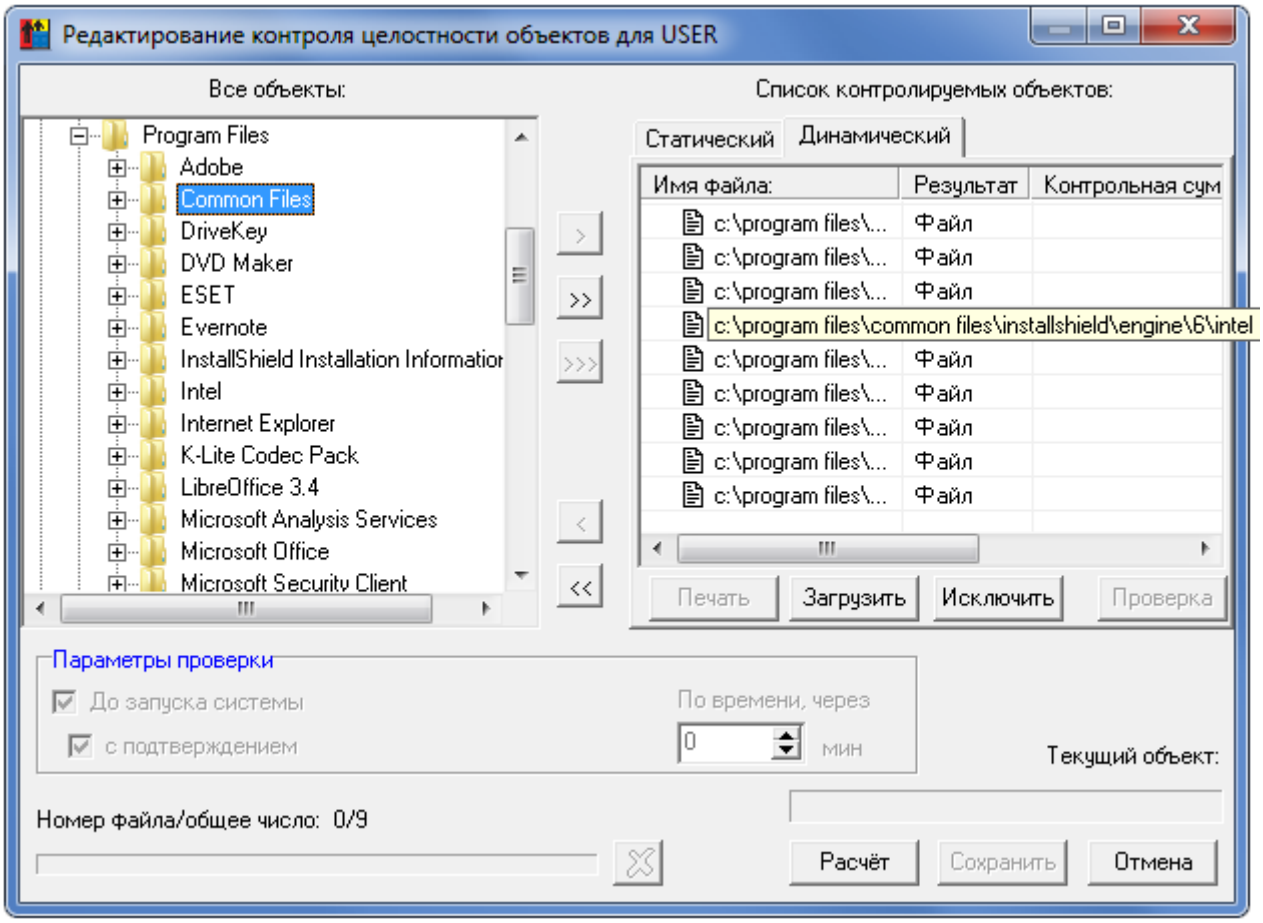

Рисунок 46 - Список файлов для динамического контроля

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. Программа работы с журналами регистрации 11443195.4012-037-2010 99»). Список файлов для контроля имеет расширение HSH. Для выполнения этой операции щелкните мышкой по кнопке <Загрузить>, откроется окно выбора файла (рисунок 47).

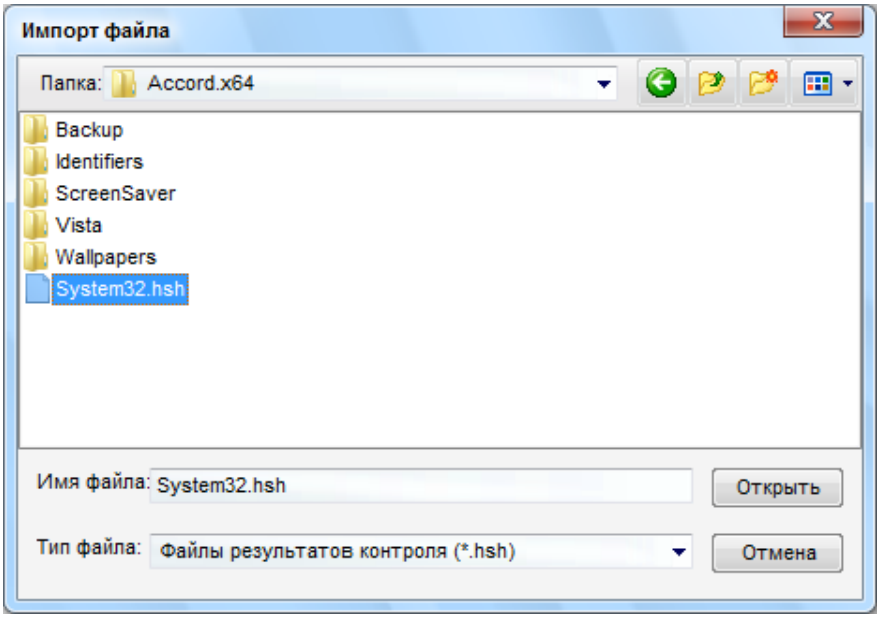

Рисунок 47 - Выбор файла со списком контролируемых объектов

Отметьте необходимый файл и нажмите кнопку <Открыть>. Файлы будут добавлены в соответствующий список контроля (рисунок 48).

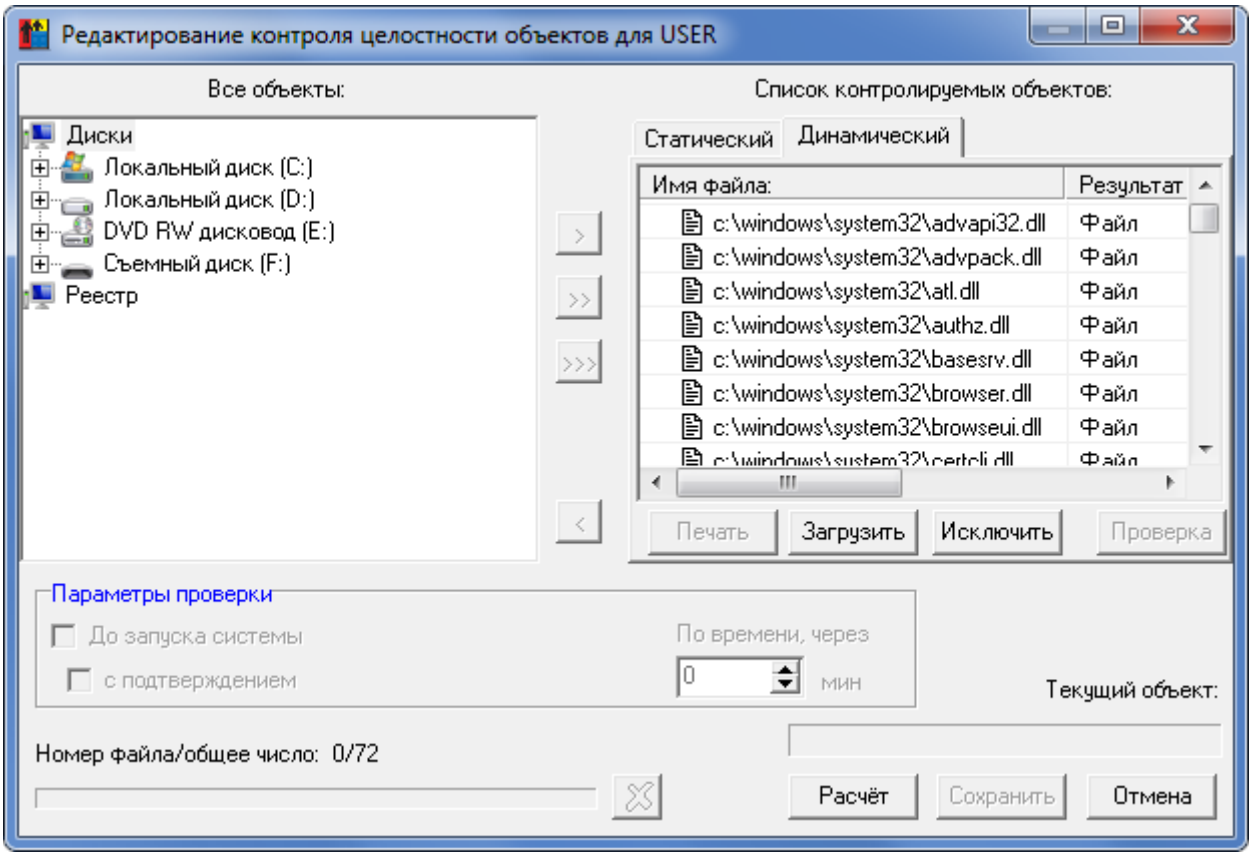

Рисунок 48 - Загрузка файлов в список контроля

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

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

СЗИ НСД «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» (11443195.4012-037 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 49), 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 49).

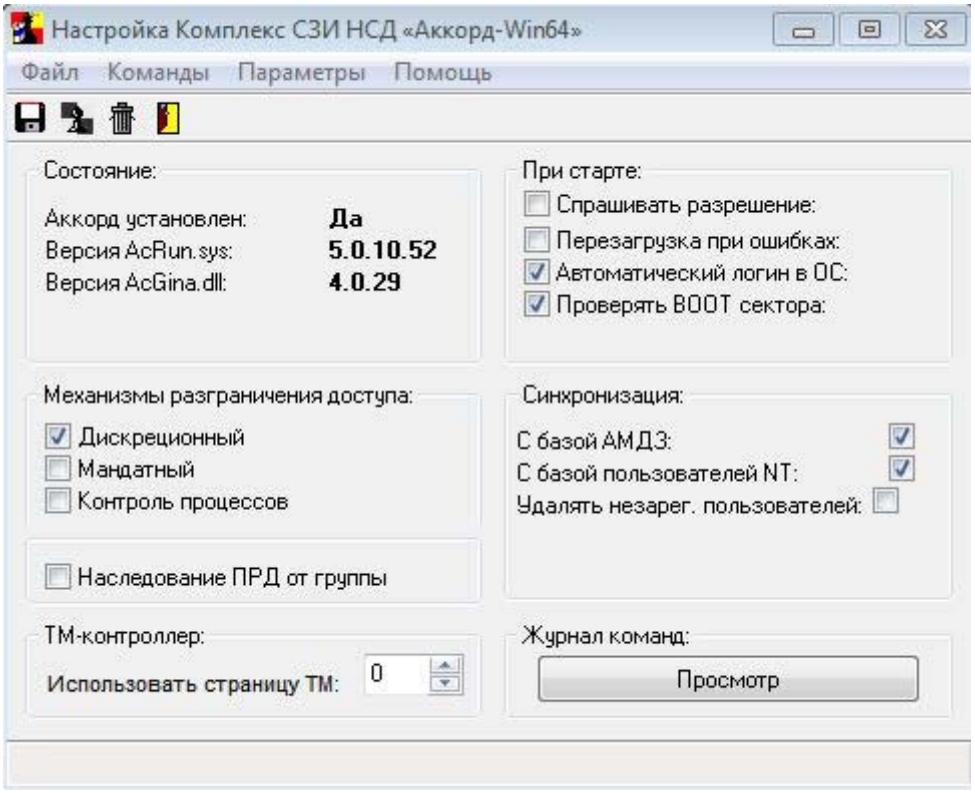

Рисунок 49 - – Главное окно утилиты «Настройка комплекса Аккорд»

Для редактирования правил разграничения доступа в главном окне программы ACED32.EXE (рисунок 2) нажмите мышкой правую кнопку в строке «Разграничение доступа» – на экран выводится окно с правами доступа пользователя к ресурсам СВТ, показанное на рисунке 50. 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.

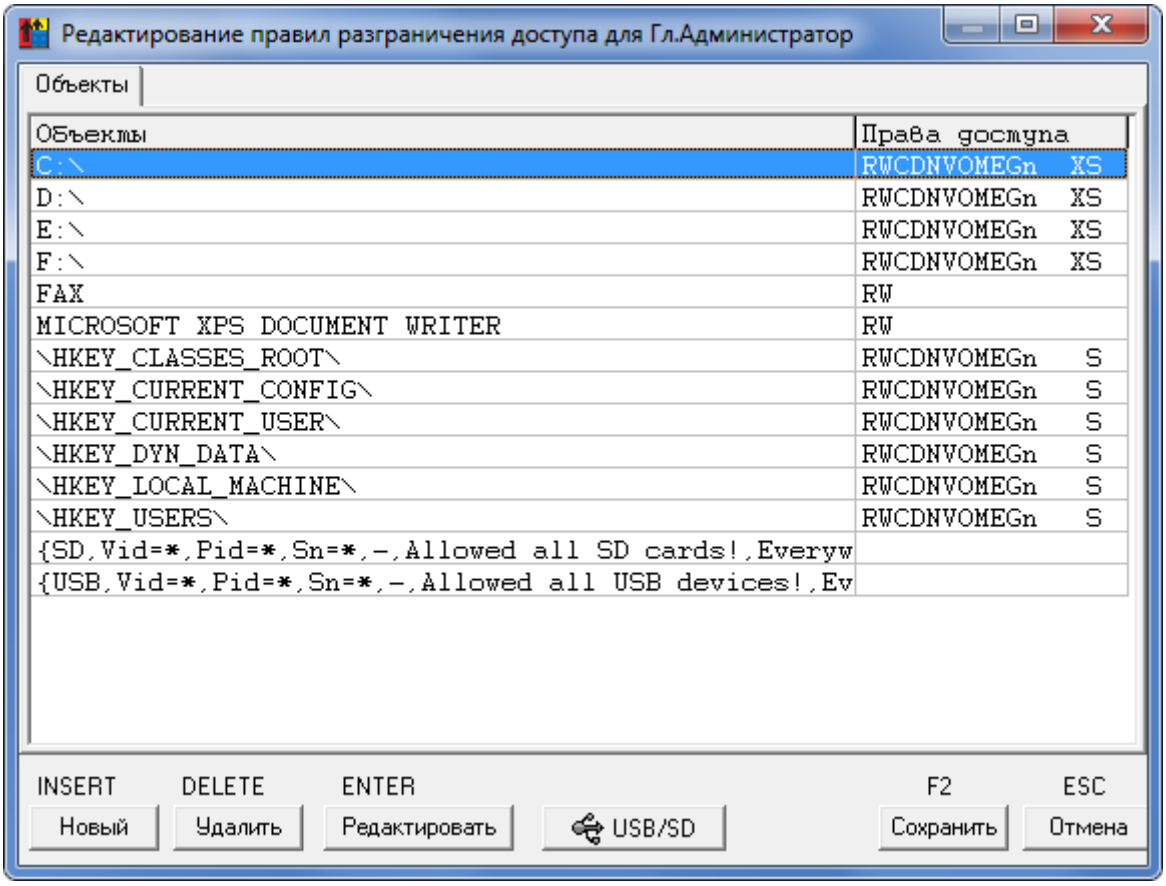

Рисунок 50 - Окно установки дискреционных ПРД к объектам

Более подробно действие атрибутов доступа описано в «Руководстве администратора» (11443195.4012-037 90).

В список объектов для обычных пользователей уже включены ограничения, которые защищают от модификации программные компоненты комплекса «Аккорд». В разделе «Объекты» (рисунок 50) выберите строку с нужным именем объекта и нажмите кнопку <Редактировать> или клавишу <Enter> - выводится окно для определения правил доступа к объекту, показанное на рисунке 51. Если Вы хотите удалить какой-либо объект и установленные для него ПРД, то 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.

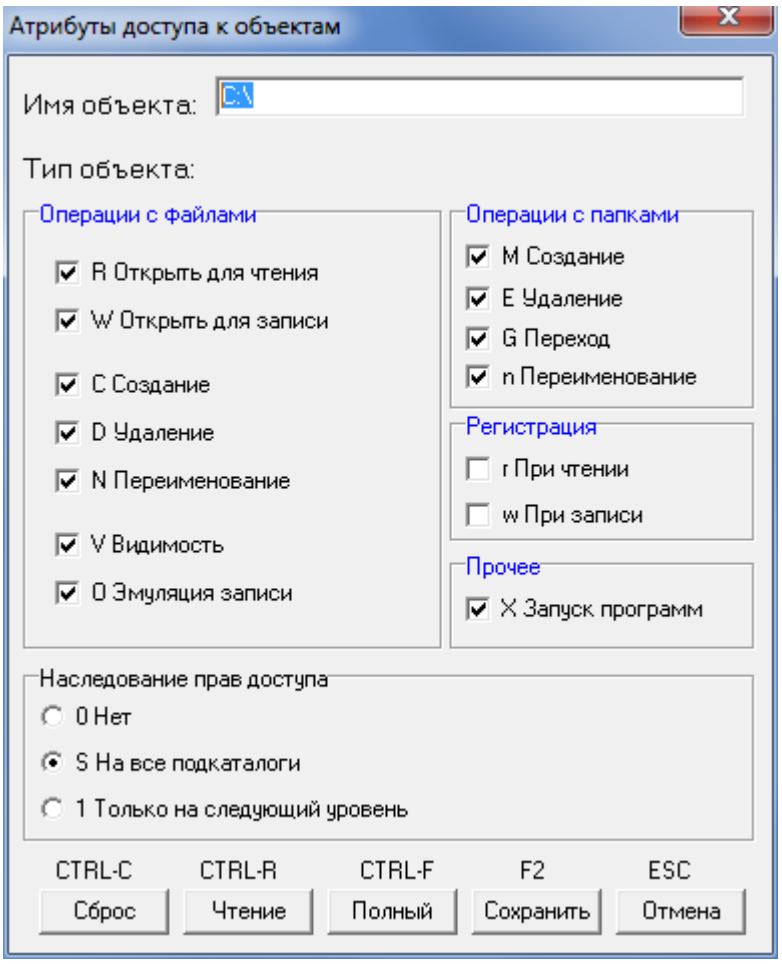

Рисунок 51 - Атрибуты доступа к объекту

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 38).

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 наследуется **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, сменный 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 50), нажмите кнопку <Новый> или клавишу <Insert> - на экран выводится расширенное окно «Атрибуты доступа к объектам» (рисунок 52). 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

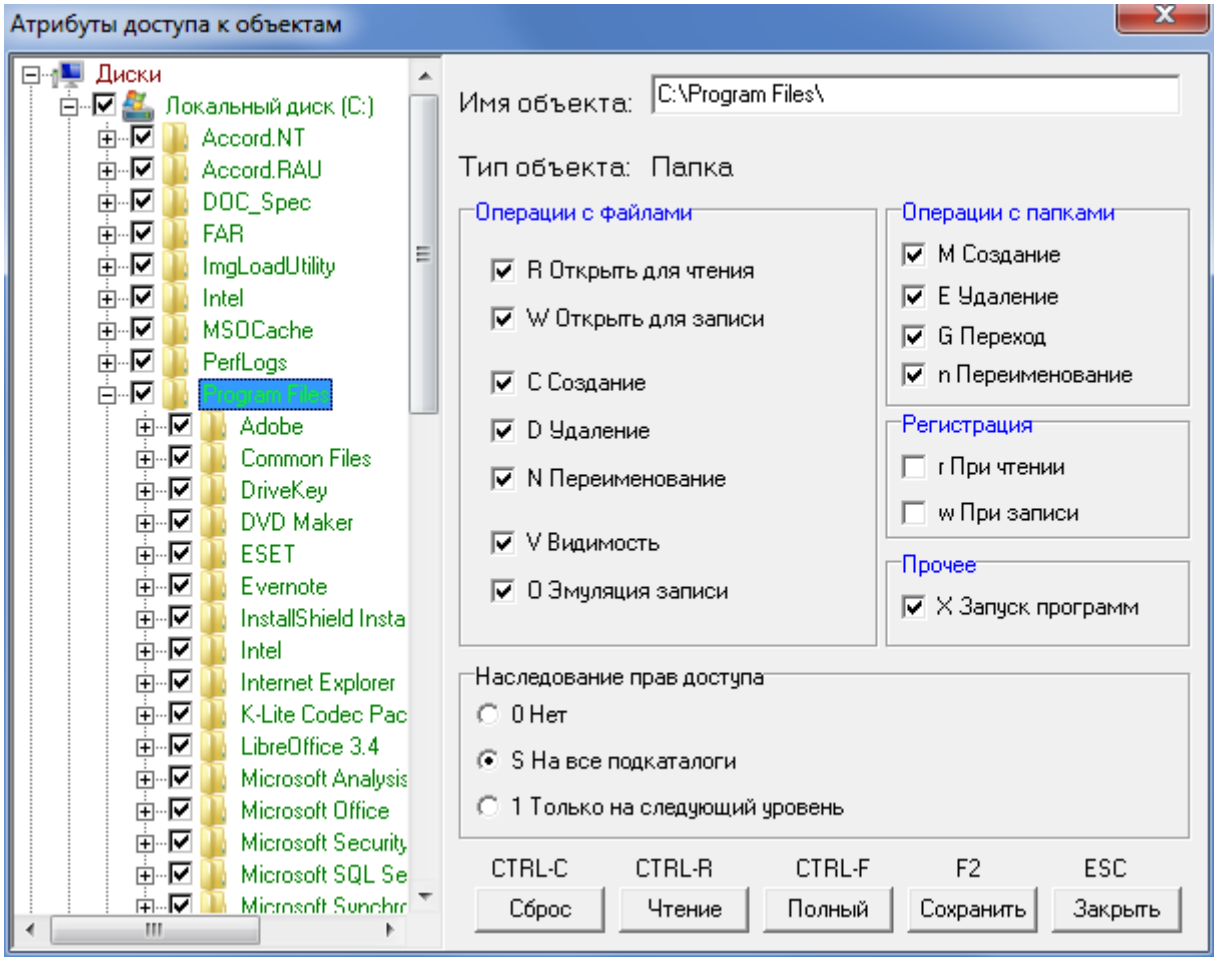

Рисунок 52 - Выбор нового объекта и установка ПРД

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 в поле «Тип объекта» - его тип (диск, каталог, файл, реестр, съемный диск, принтер, устройство). 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 ПАК «Аккорд» приводят к возникновению непрогнозируемых последствий, однако нарушения логики работы ПАК «Аккорд» при этом отсутствуют. Например, если установить запрет на удаление файлов в каталоге «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, или 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, сменные HDD) выполняется корректно только в том случае, когда сменное 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 данного руководства.

По умолчанию разрешено использование всех USB-устройств, т.е. в список объектов (рисунок 54) включена запись:

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

Разрешение на доступ для USB-устройства задаётся 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 53) следующим образом:

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

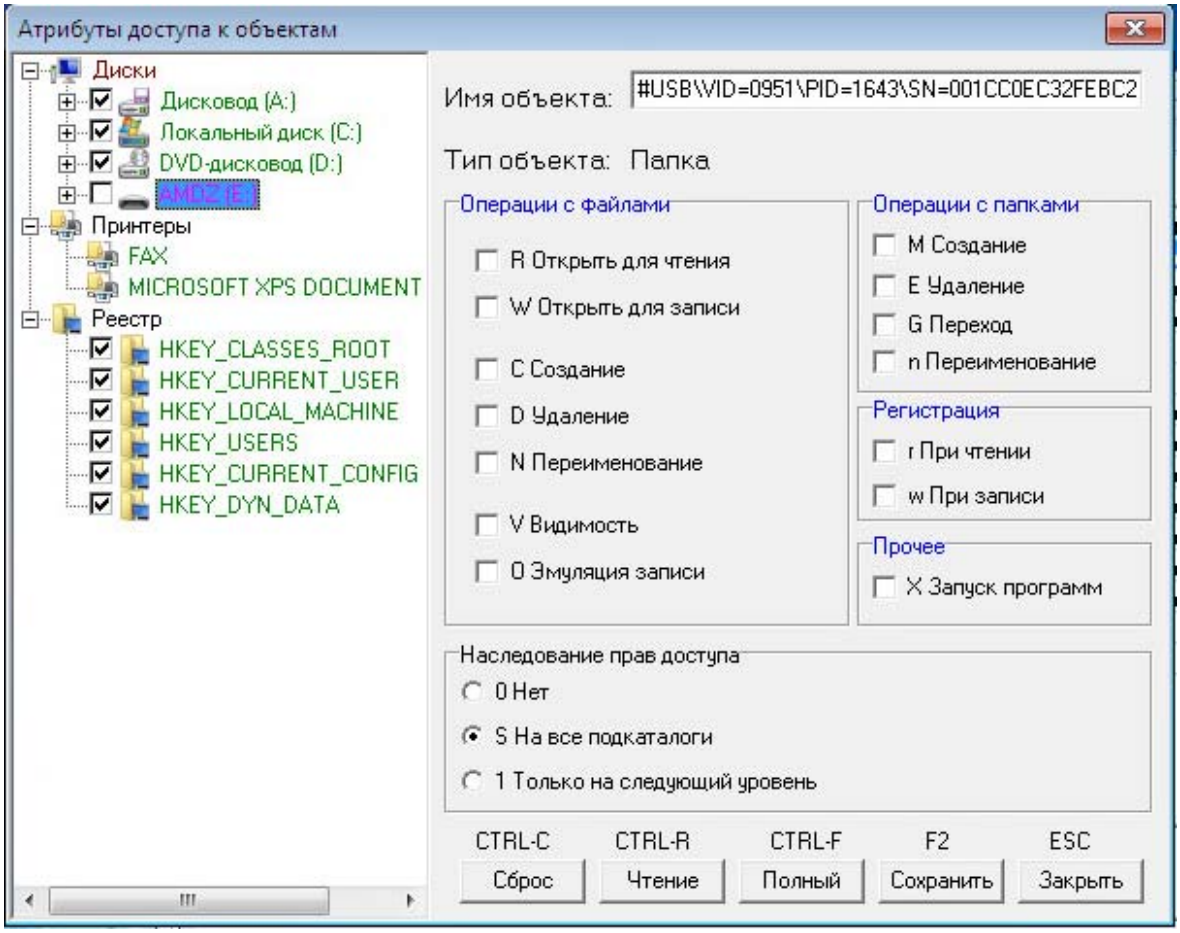

Рисунок 53 - Выбор USB-устройства и установка ПРД

После описания правил доступа для данного устройства в окне редактирования правил разграничения доступа (рисунок 54) будет добавлена запись вида

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

с описанными для данного устройства ПРД.

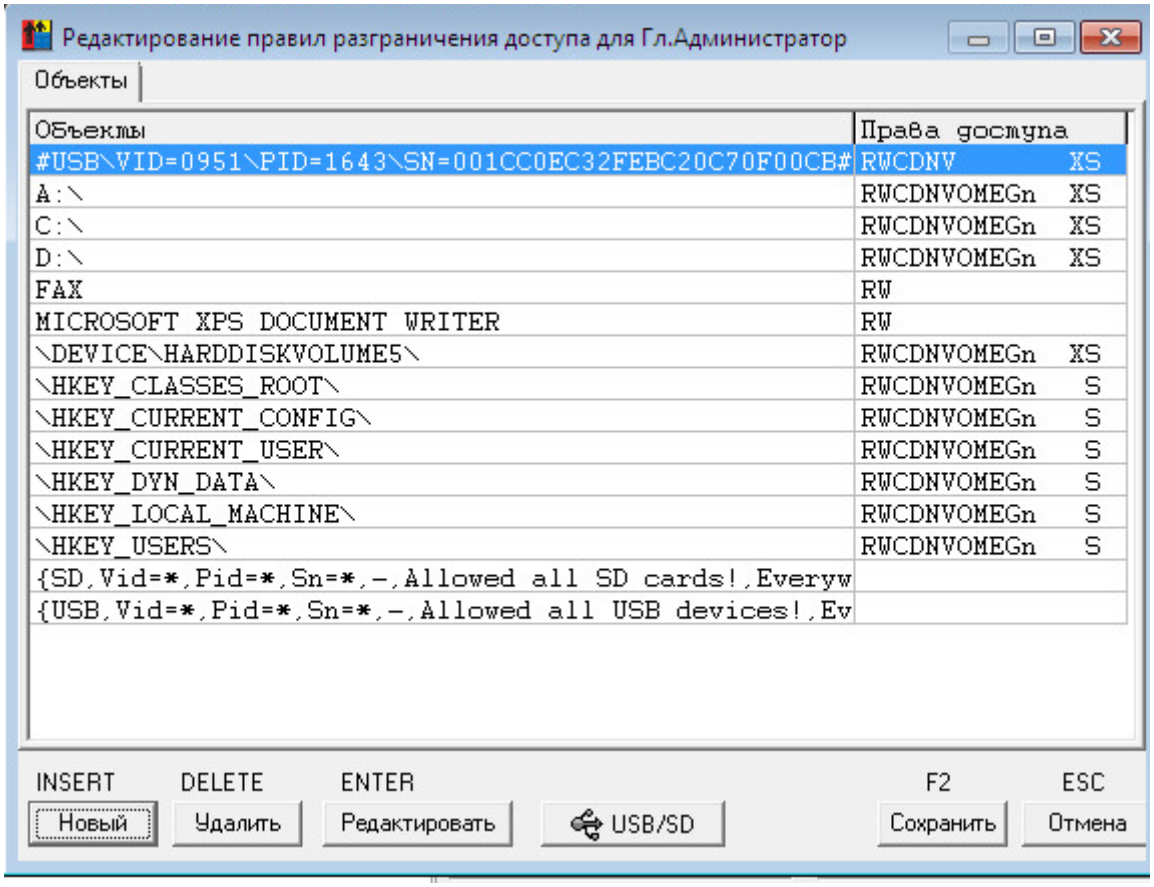

Рисунок 54 - Окно установки дискреционных ПРД к объектам

Для разрешения **доступа ко всем USB-накопителям** в окне задания атрибутов доступа к объектам (рисунок 53) следует добавить запись:

```
#USB\
```

Для разрешения **доступа к заданным USB-накопителям определенного производителя** в окне задания атрибутов доступа к объектам (рисунок 53) следует добавить запись:

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

где XXXX, YYYY – соответствующие значения vid и pid.

Имеется также дополнительная возможность **задания простых имён 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 55).

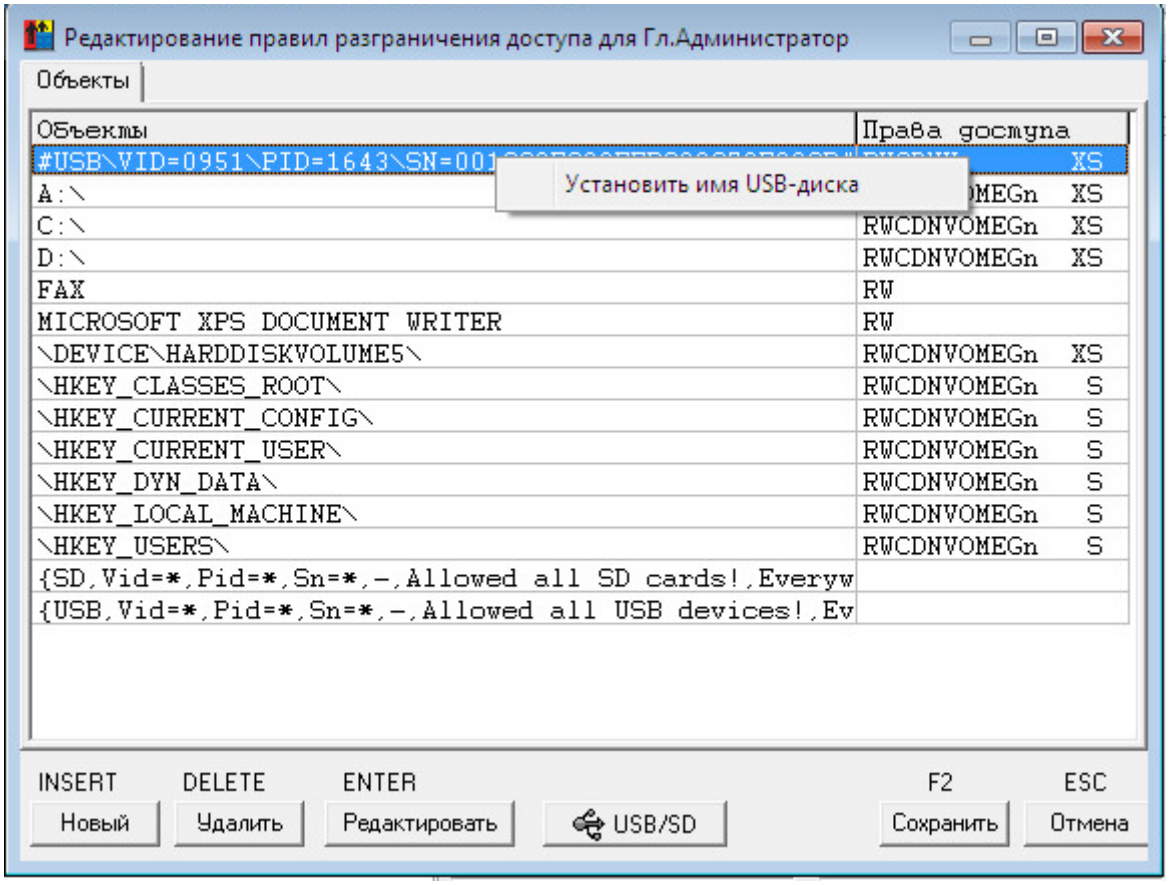

Рисунок 55 - Окно редактирования ПРД

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 56).

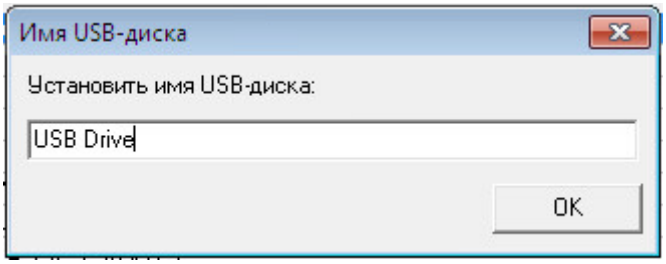

Рисунок 56 - Задание имени USB-диска

После этого заданное имя отобразится в списке объектов (рисунок 57) в следующем виде

`#USB\%название%#0\`

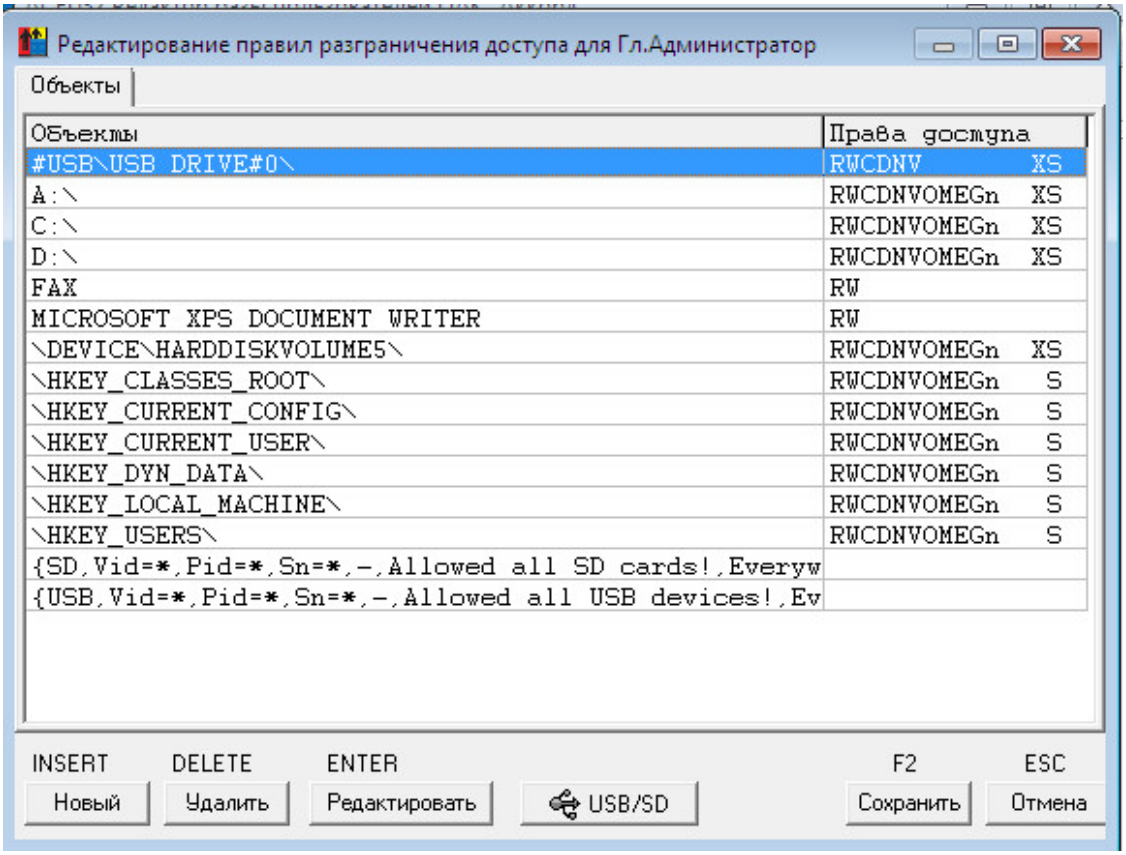

Рисунок 57 - Окно редактирования ПРД

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 58.

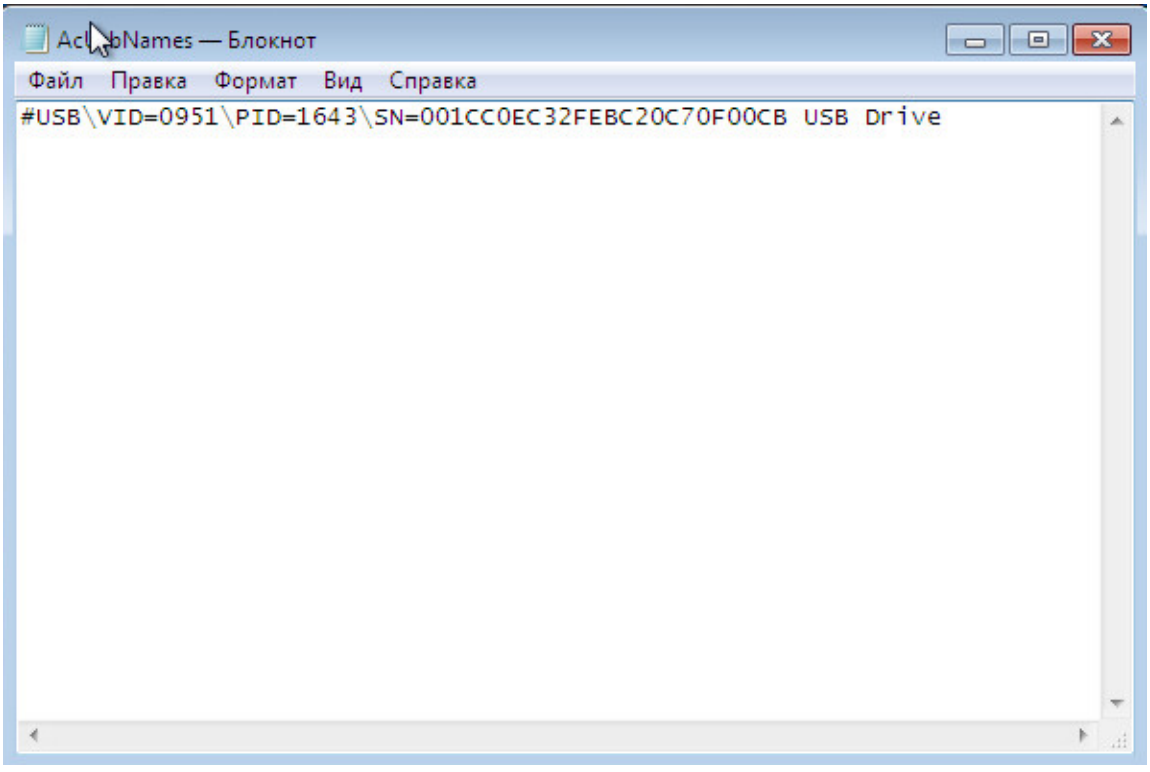

Рисунок 58 - Содержимое файла AcUsbNames

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.

Действует следующее правило, в отличие от дисковых ресурсов, - если устройство включено в список ПРД, то доступ к нему ЗАПРЕЩЕН, независимо от атрибутов доступа. Сделано это из необходимости поддерживать единый формат записи об объекте доступа, а реально установить режим «только чтение», или «только запись» для Com/Lpt порта весьма затруднительно.

Для того чтобы список устройств отображался в редакторе ПРД, нужно включить флаг «Контроль устройств» в дополнительных опциях программы настройки комплекса Аккорд.

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

Для выхода из режима редактирования нажмите кнопку <Закрыть> или клавишу <Esc>.

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 49, 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». С помощью этой команды можно установить, или изменить уровень доступа пользователя[1] (рисунок 59).

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

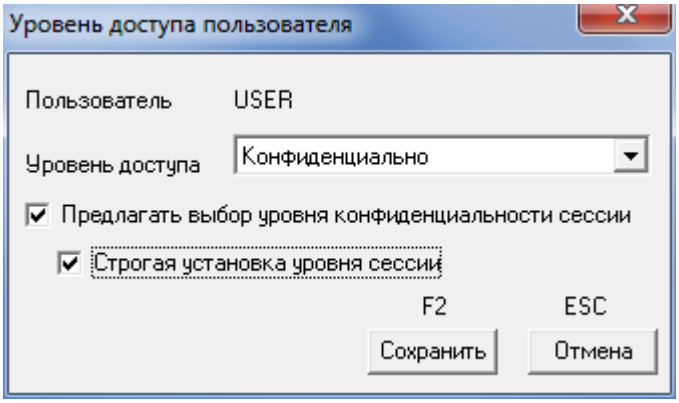

Рисунок 59 - Установка уровня доступа пользователя

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, ключи реестра), то доступ к объекту предоставляется данному субъекту. Если при этом установлены дискреционные ПРД, то операции, которые пользователь может выполнять с разрешенным объектом (чтение, запись, удаление и пр.), определяются атрибутами дискреционного доступа.

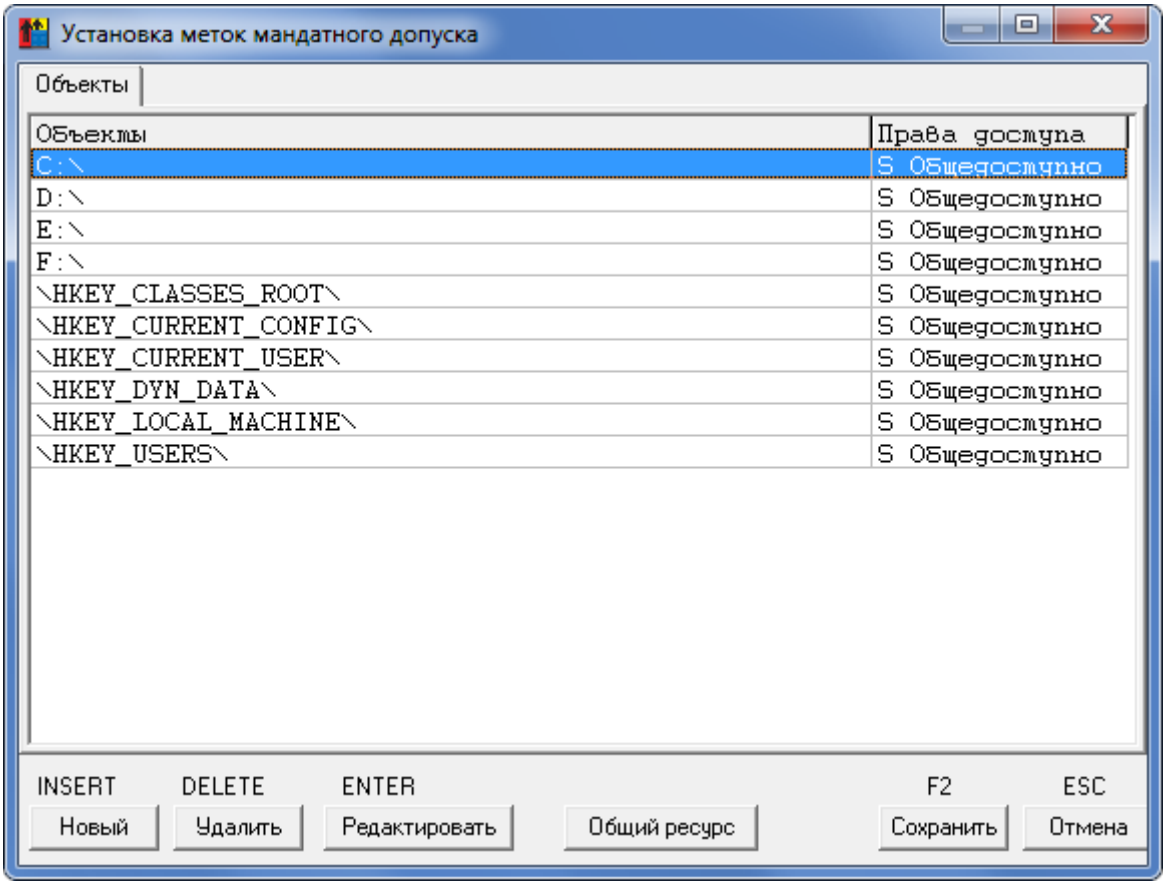

Рисунок 60 - Установка меток допуска объектов при использовании мандатных ПРД

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 60).

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 – уровень доступа и наследование прав доступа. Уровень доступа меняется нажатием мышью на кнопку в строке «Уровень доступа» и выбором значения из списка.

Если необходимый Вам объект отсутствует в списке (рисунок 60), нажмите кнопку <Новый> или клавишу <Insert>. На экран выводится расширенное окно «Атрибуты доступа к объектам» (рисунок 61).

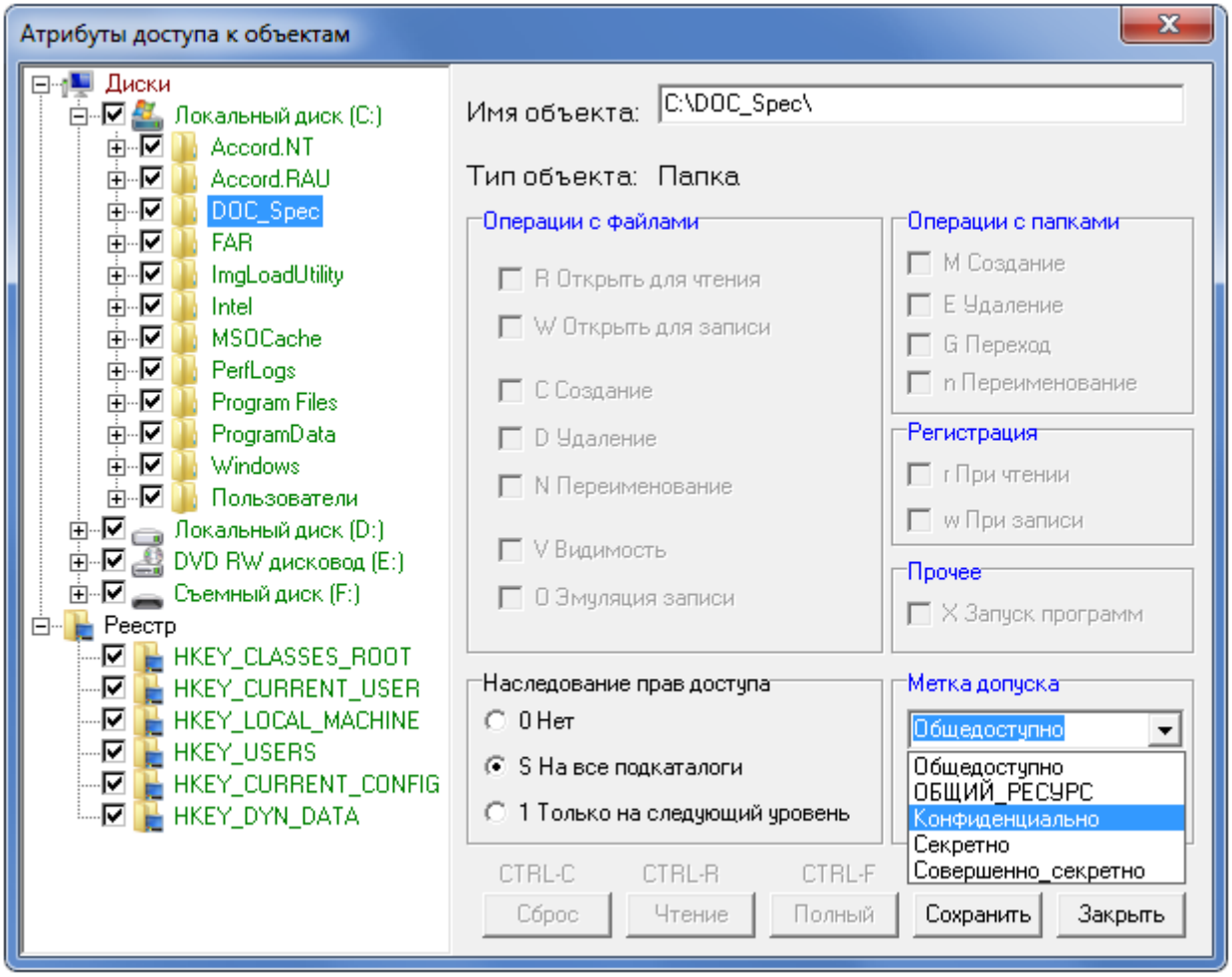

Рисунок 61 - Определение нового объекта и выбор его метки допуска

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».

Справа 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 установке меток допуска объекта. Установите указатель мыши на стрелку в правой части строки «Уровень доступа» 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 недоступным для всех пользователей, кроме администраторов.

В этом списке можно создавать записи, которые во время работы системы защиты будут определять переменную среды окружения для процессов с определенным уровнем доступа, например, _SET TEMP=C:\TEMP_1 [Конфиденциально]. В этом случае процесс будет создавать временные файлы именно в том каталоге, который указал администратор. Единственное ограничение – каталог с заданным именем должен существовать на жестком диске.

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

7.12.1. Общие сведения

В ПАК СЗИ НСД «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»[1] (рисунок 62);

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

[1)] в ПО «Аккорд» начиная с версии 5.0.10.51; в более ранних версиях – флаги «Мандатный» и «+процессы» (контроль процессов с использованием дискреционного механизма разграничения доступа раннее не был доступен).

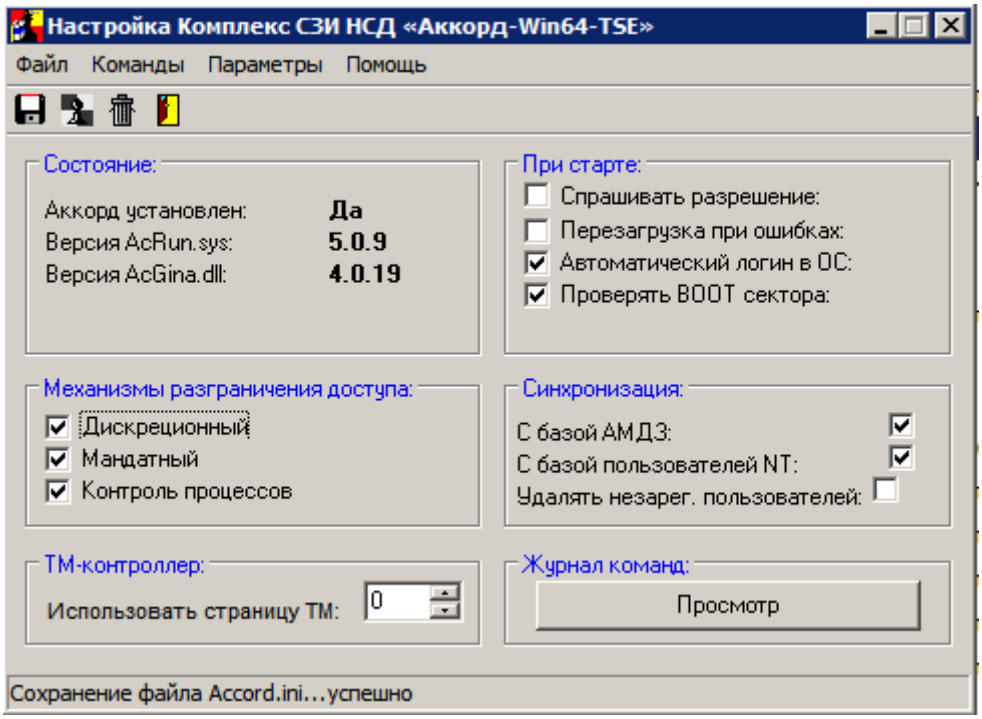

Рисунок 62 - Главное окно утилиты «Настройка комплекса Аккорд»

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 механизма 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.

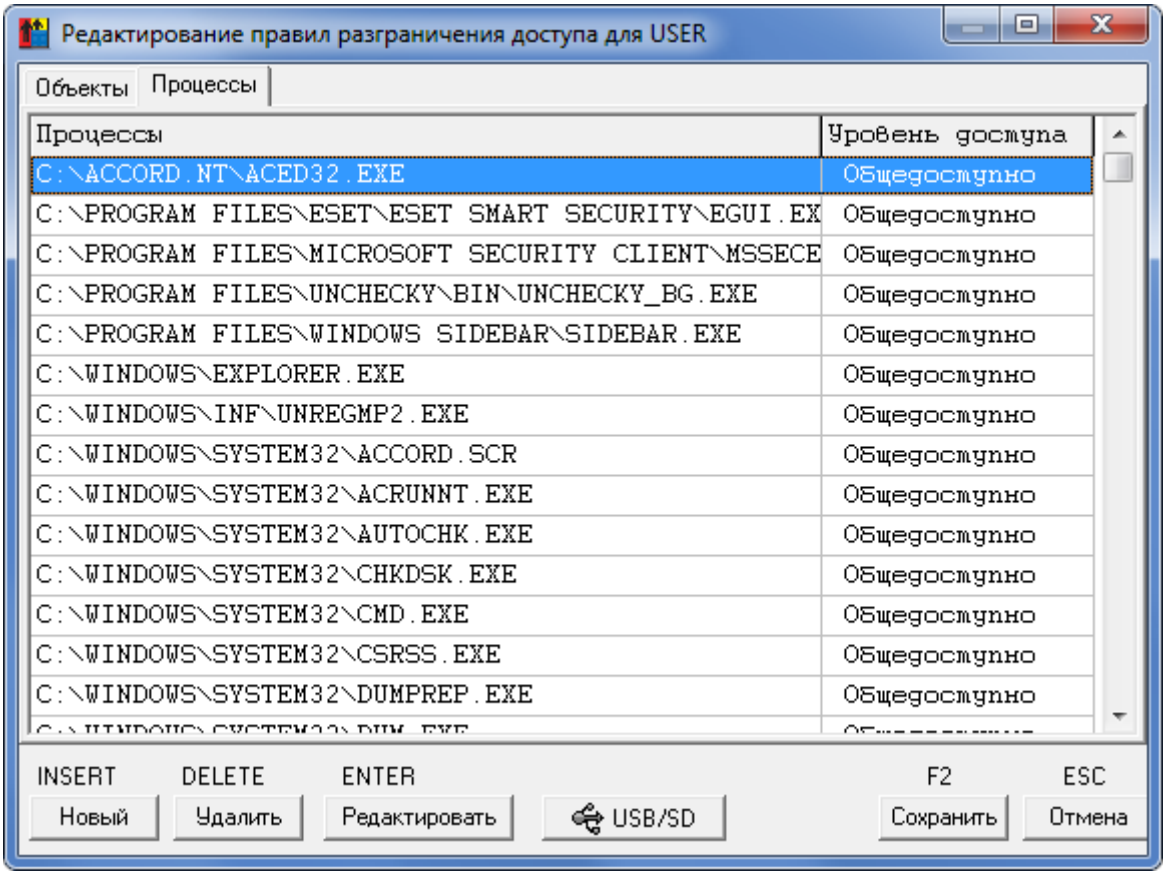

Рисунок 63 - Закладка «Процессы» при включенном механизме мандатного доступа для процессов

Если необходимый Вам процесс отсутствует в списке (рисунок 63), нажмите кнопку <Новый> или клавишу <Insert>.

На экран выводится окно установки уровня доступа (рисунок 64). Имя процесса вводится без указания пути, но с расширением. При установке в программе настройки комплекса 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>.

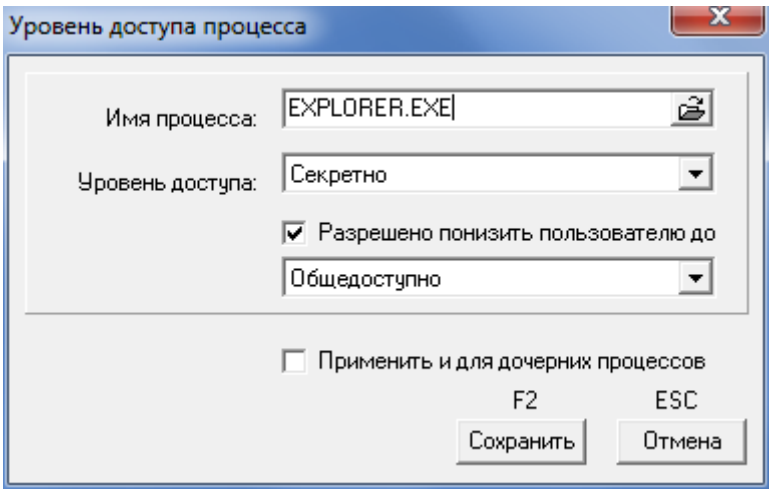

Рисунок 64 - Установка уровня доступа процесса

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[1].

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.

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

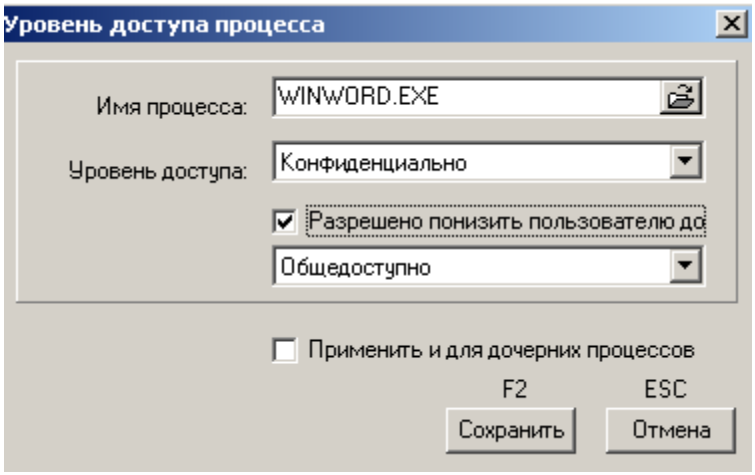

Рисунок 65 – Установка уровня доступа процесса

В случае запуска в рамках данного процесса двух объектов, имеющих разные уровни доступа, выводится предупреждающее сообщение (рисунок 66), которое остается на экране до тех пор пока документ другого уровня доступа не будет закрыт.

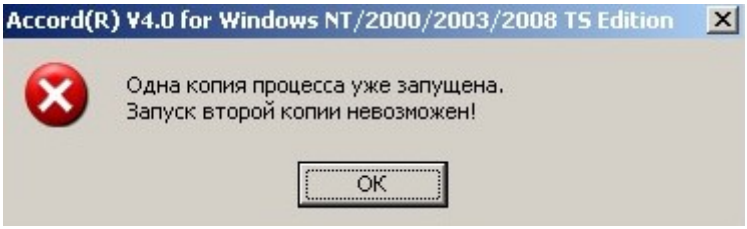

Рисунок 66 – Предупреждающее сообщение

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 СЗИ «Аккорд-Win64» 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 объёму 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 2007/2010 под Windows 7):

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

в редакторе ПРД установить уровень детальности журнала «Сбор статистики» для одного из пользователей, входящего в состав группы пользователей СЗИ от НСД «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.

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

завершить сеанс пользователя, запустить от имени Администратора СЗИ от НСД «Аккорд» программу AcProc.exe из каталога Accord.x64 (Пуск –> Программы –> Аккорд -> Создание списка процессов из журналов регистрации) (рисунок 67);

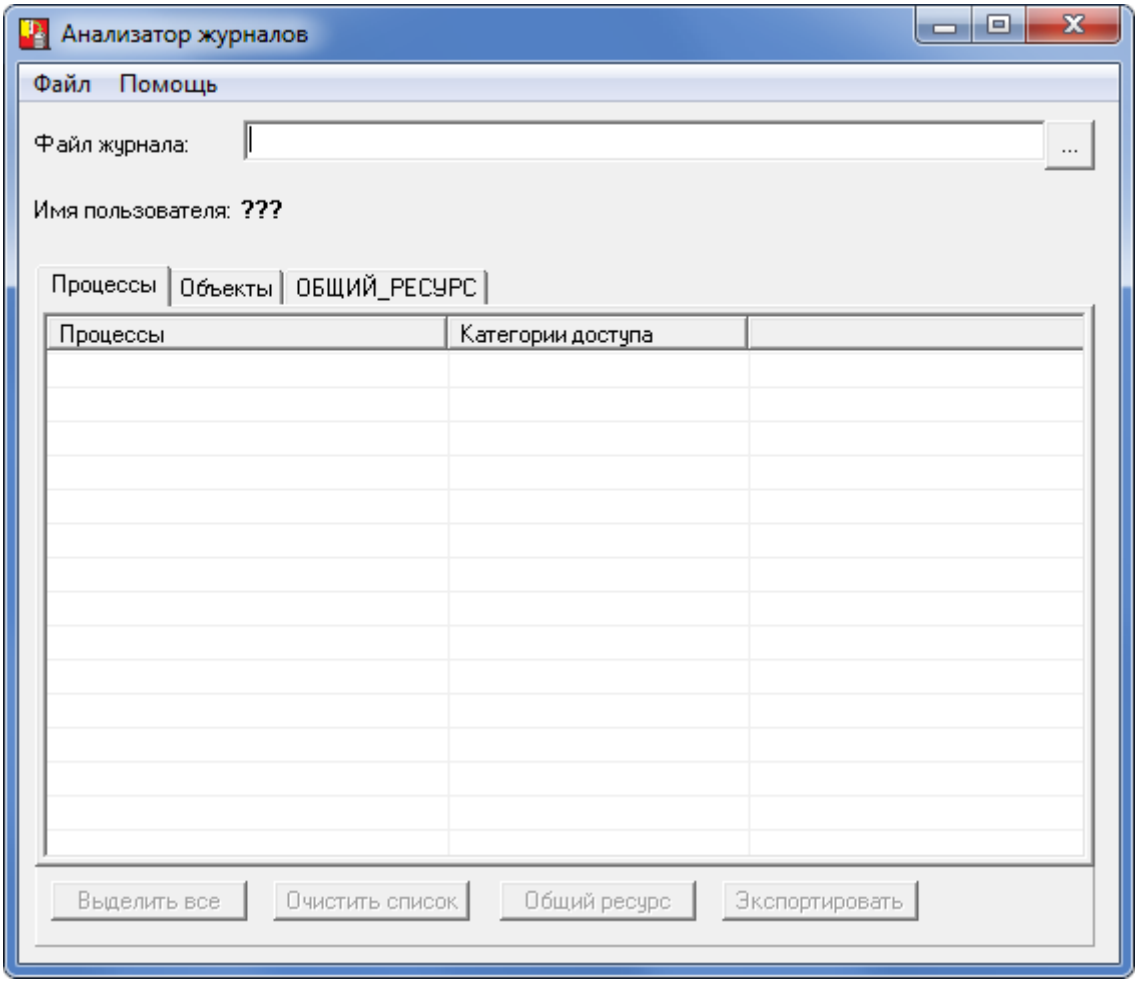

Рисунок 67 - Главное окно программы AcProc.exe

во вкладке «Процессы» загрузить журнал последнего сеанса работы пользователя: в окне программы AcProc.exe (рисунок 67) нажать на раскрывающийся список в поле «Файл журнала», далее в появившемся на экране окне (рисунок 68) выбрать файл журнала (или несколько файлов);

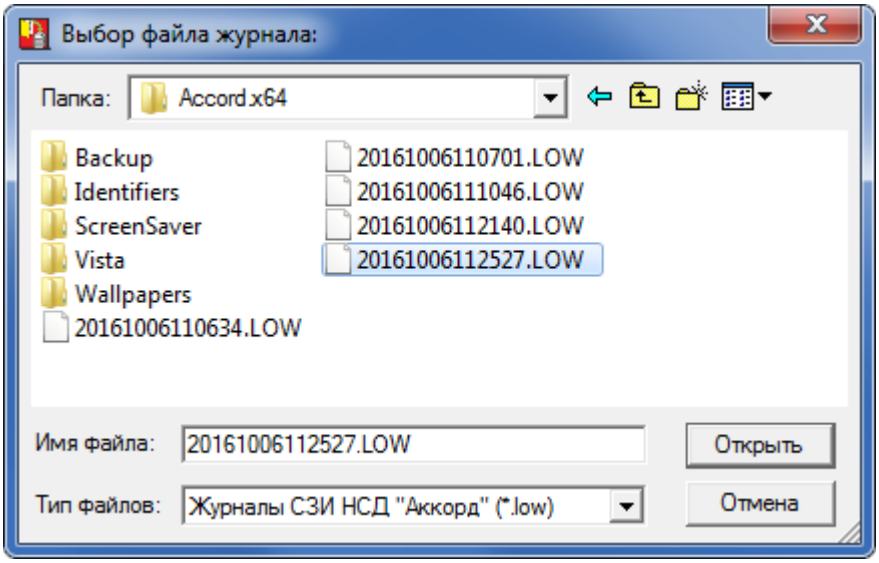

Рисунок 68 - Выбор файла журнала регистрации событий

в главном окне программы AcProc.exe выбрать процессы, которые необходимы для выполнения должностных обязанностей пользователя (рисунок 69);

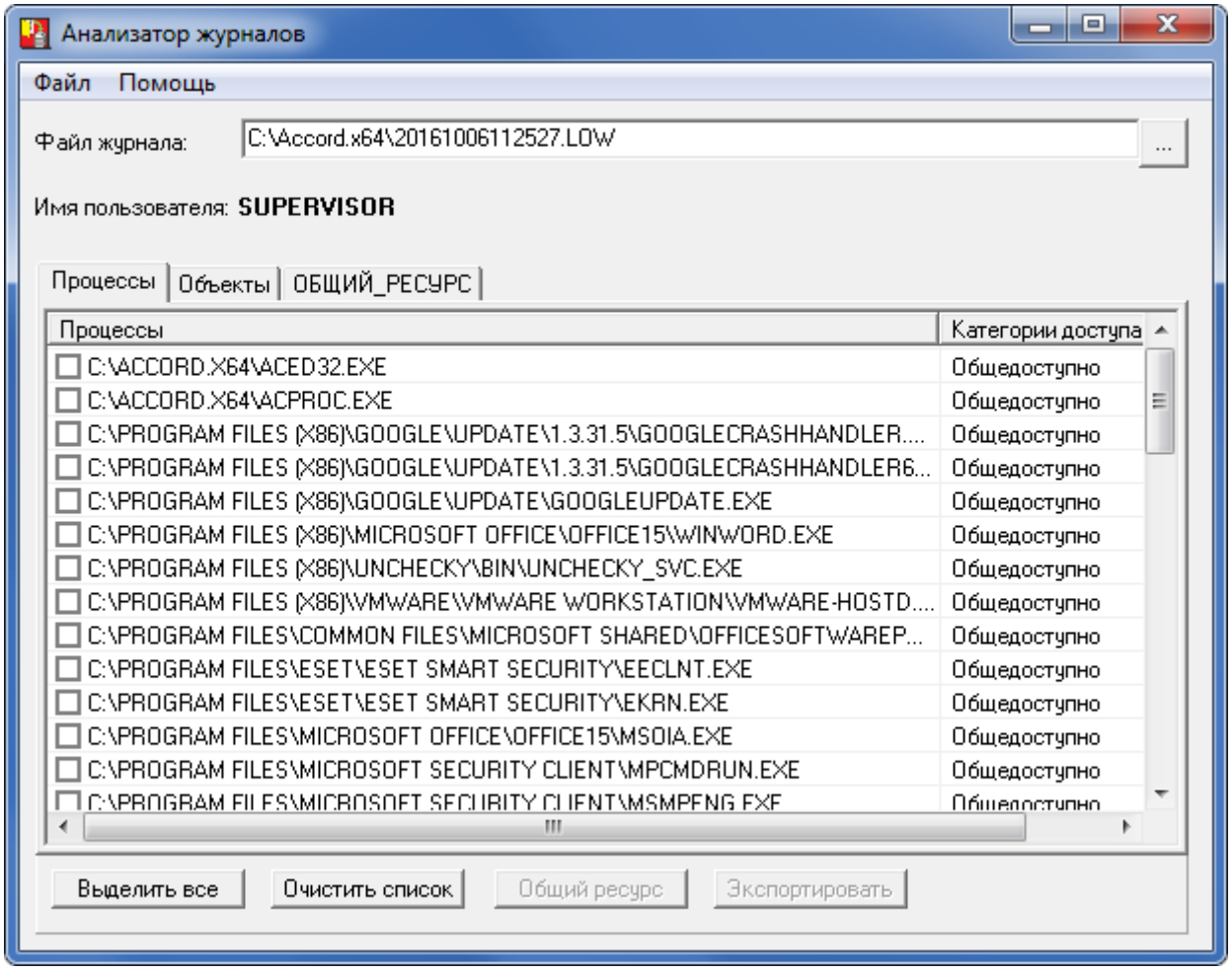

Рисунок 69 – Главное окно программы AcProc.exe. Выбор процесса

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 70);

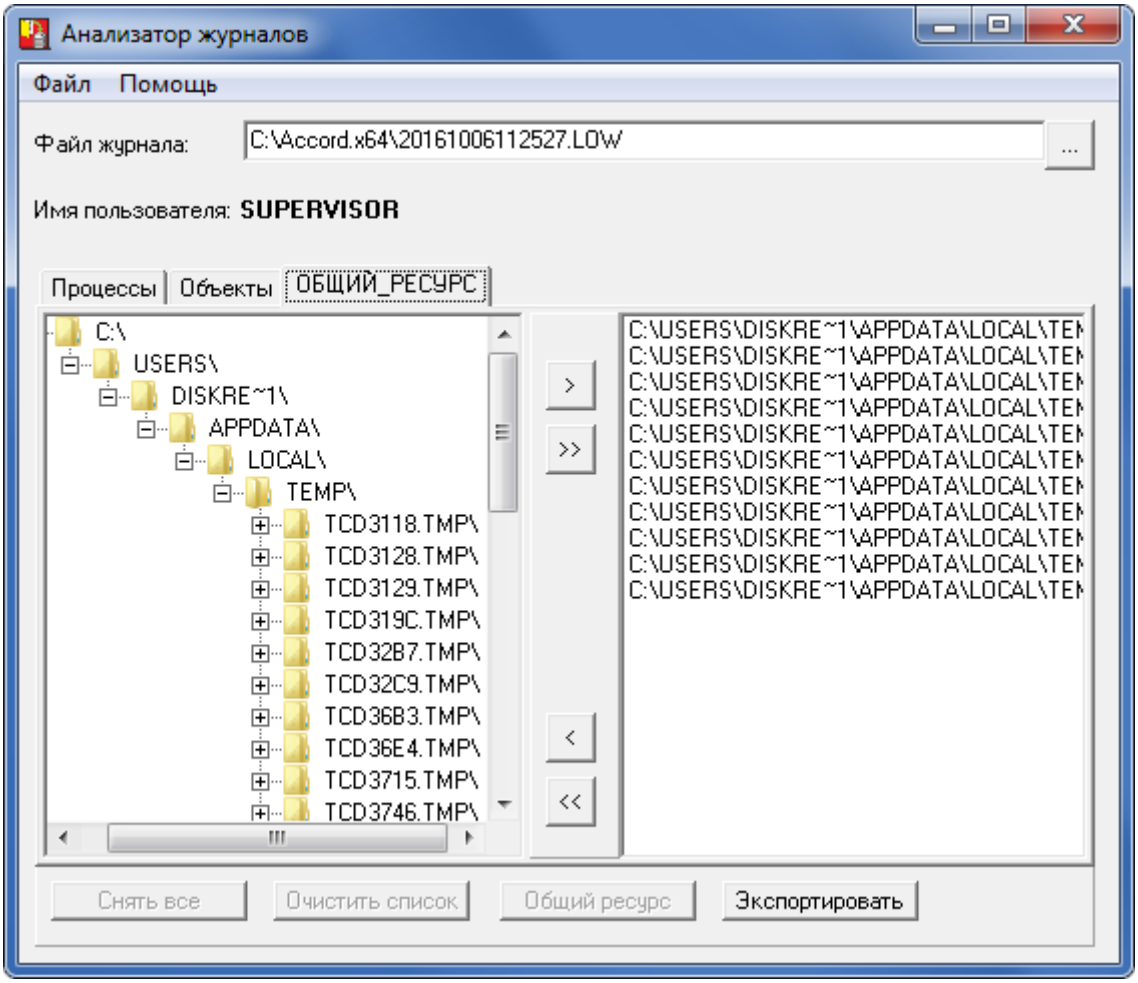

Рисунок 70 – Список объектов общего доступа

сохранить объекты, к которым обращались процессы. Для этого нужно нажать кнопку <Экспортировать> (рисунок 70). По нажатии кнопки на экране появляется окно, в котором нужно указать путь, имя файла (например, «SUPERVISOR.PRD») и нажать кнопку <Сохранить> (рисунок 71).

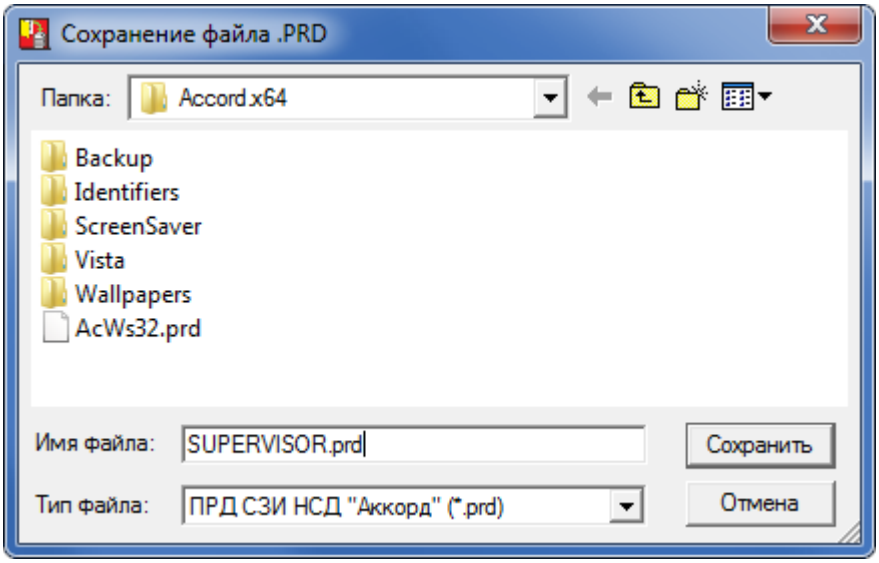

Рисунок 71 – Сохранение объектов, к которым обращались выбранные процессы

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

далее на экране появляется окно, в котором отображается список каталогов и файлов, к которым обращались выбранные процессы (рисунок 72);

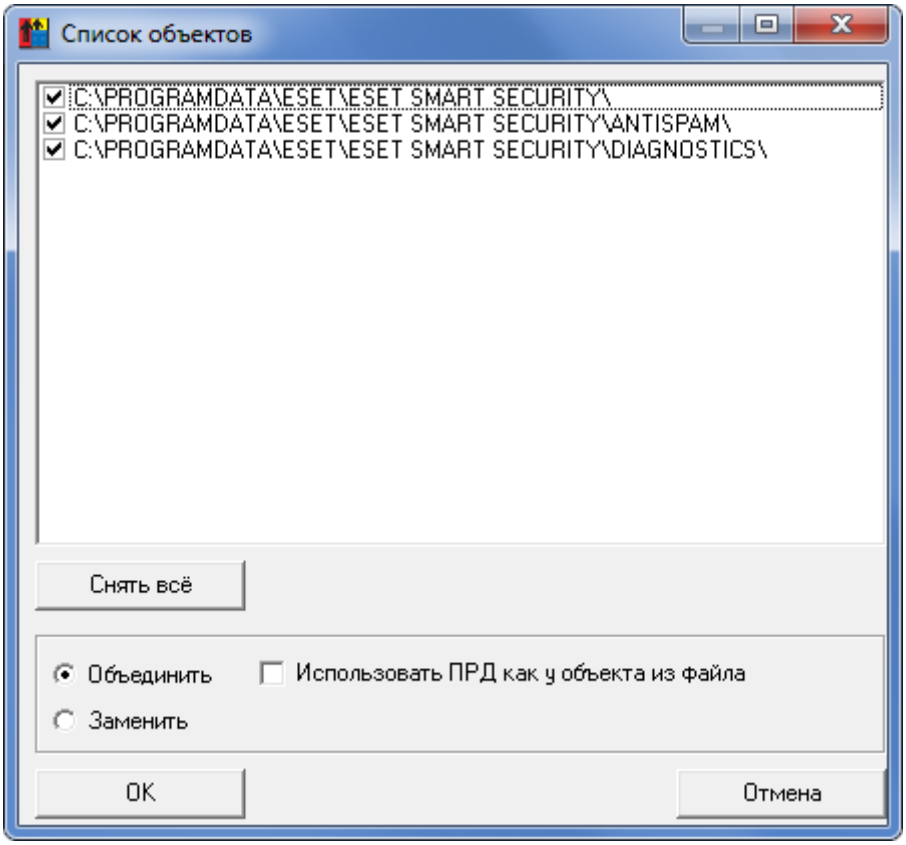

Рисунок 72 – Список объектов, к которым обращались анализируемые процессы

в окне 72 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\.

в редакторе ПРД для пользователя 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 процессов 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.

Ещё один вариант работы с разными уровнями процессов – это **выбор уровня доступа сессии пользователя.** При задании уровня доступа пользователя (рисунок 59) 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 ПО ПАК «Аккорд» для ОС Vista и выше 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»)[1] (рисунок 73);

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

[1)] в ПО «Аккорд» начиная с версии 5.0.10.51; в более ранних версиях – флаги «Мандатный» и «+процессы» (контроль процессов с использованием дискреционного механизма разграничения доступа раннее не был доступен).

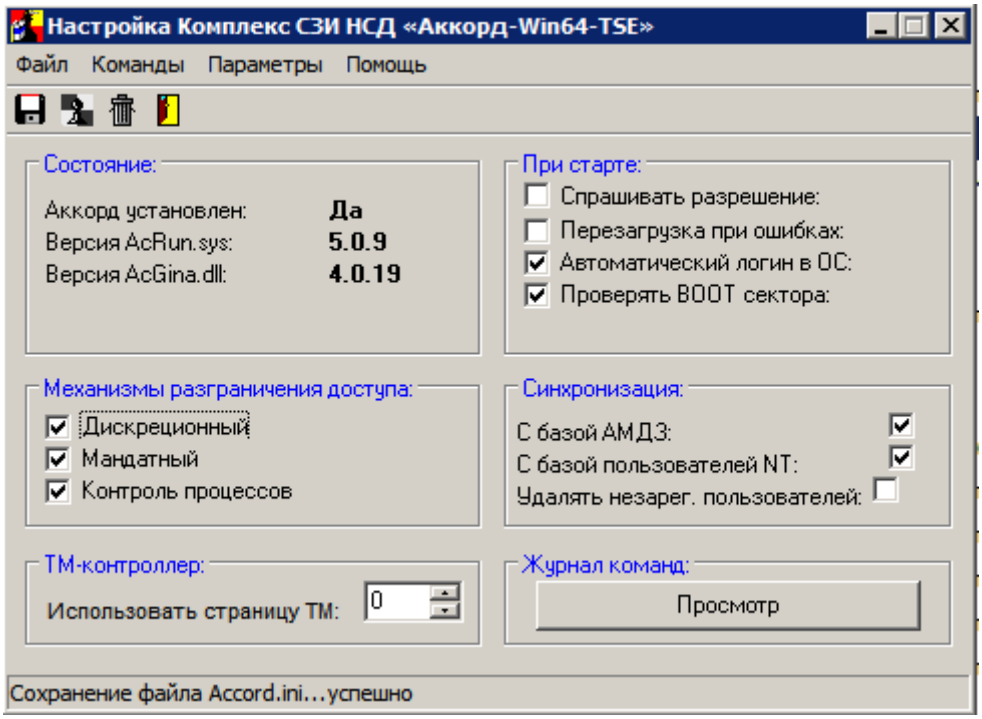

Рисунок 73 – Главное окно утилиты «Настройка комплекса Аккорд»

завершить работу приложения с сохранением изменений;

запустить утилиту «Редактор прав доступа» (Программы\Аккорд\Редактор прав доступа), в которой установить в уровень детальности журнала «Сбор статистики» для одного из пользователей, входящего в состав группы пользователей СЗИ от НСД «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;

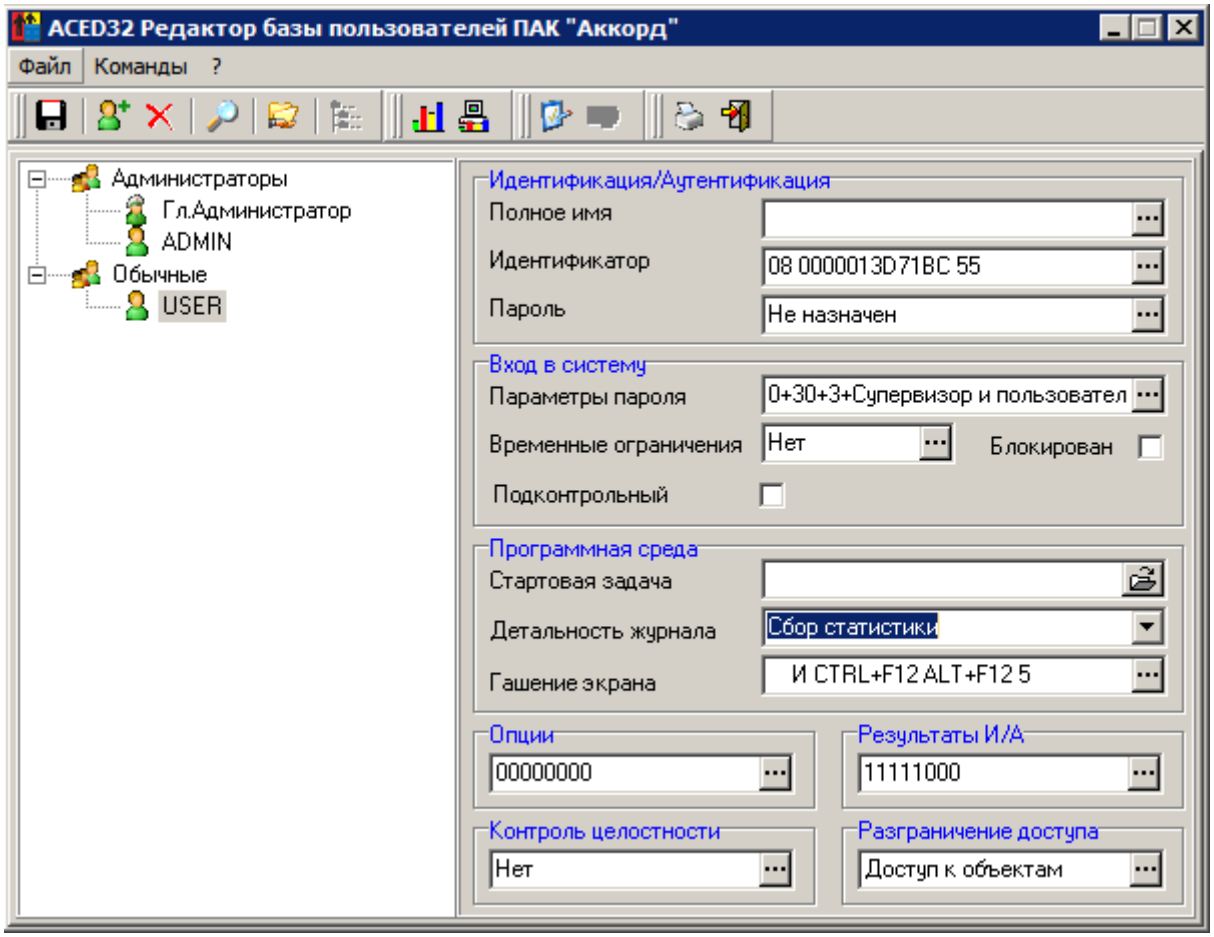

Рисунок 74 - Установка уровня детальности журнала «Сбор статистики»

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

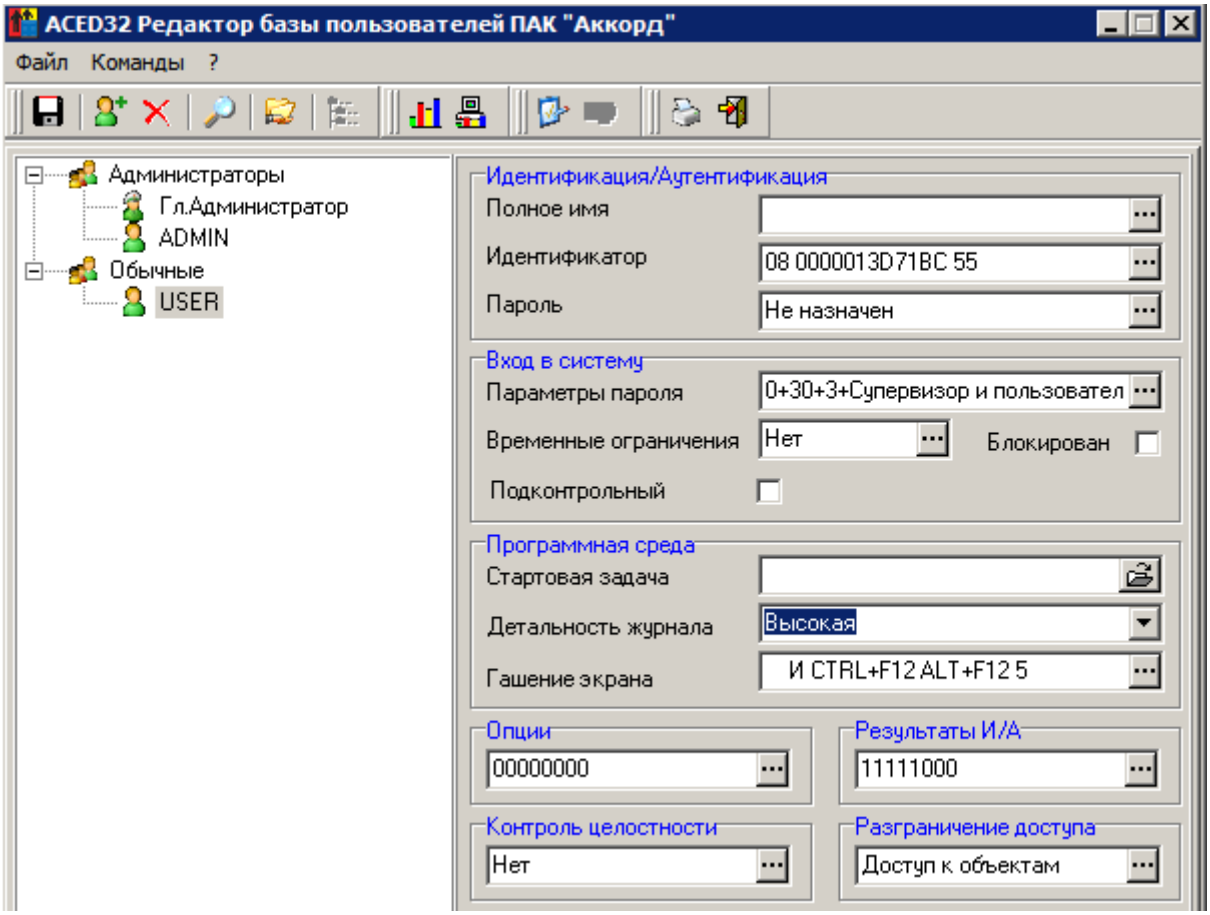

Рисунок 75 - Установка уровня детальности журнала «Высокая»

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

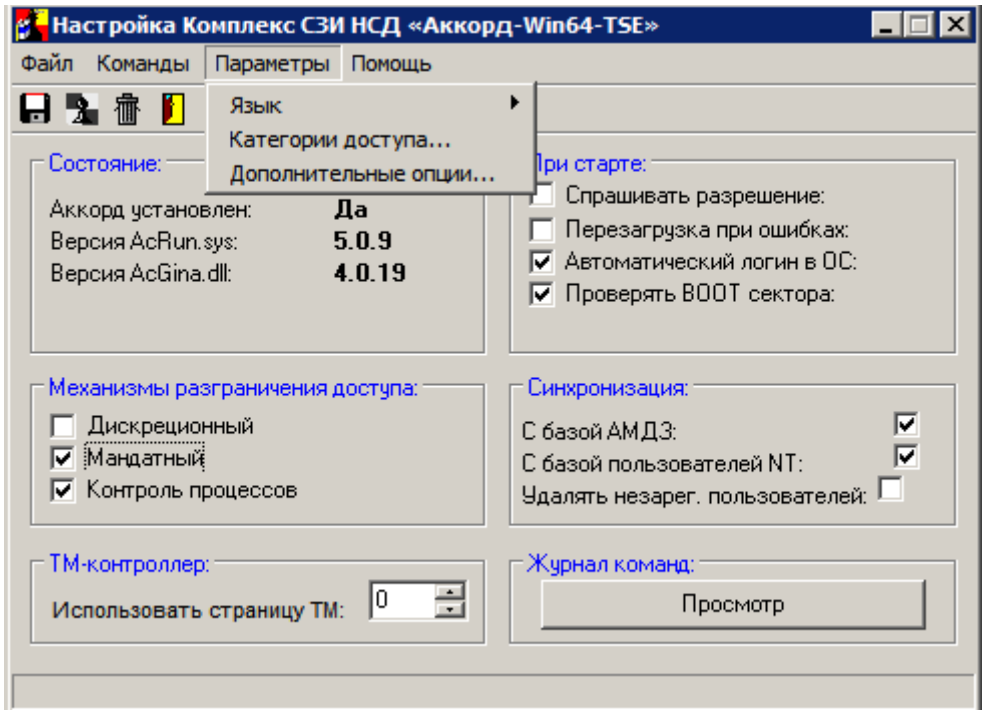

Рисунок 76 - Главное окно программы настройки комплекса «Аккорд»

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

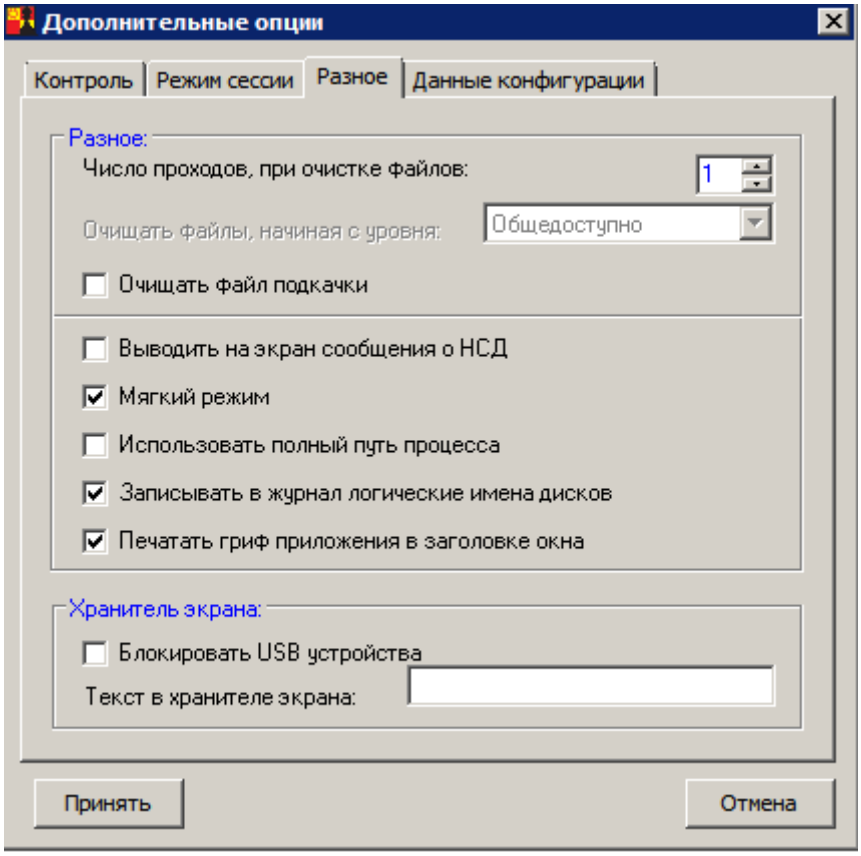

Рисунок 77 - Установка опции «Мягкий режим»

3. 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.

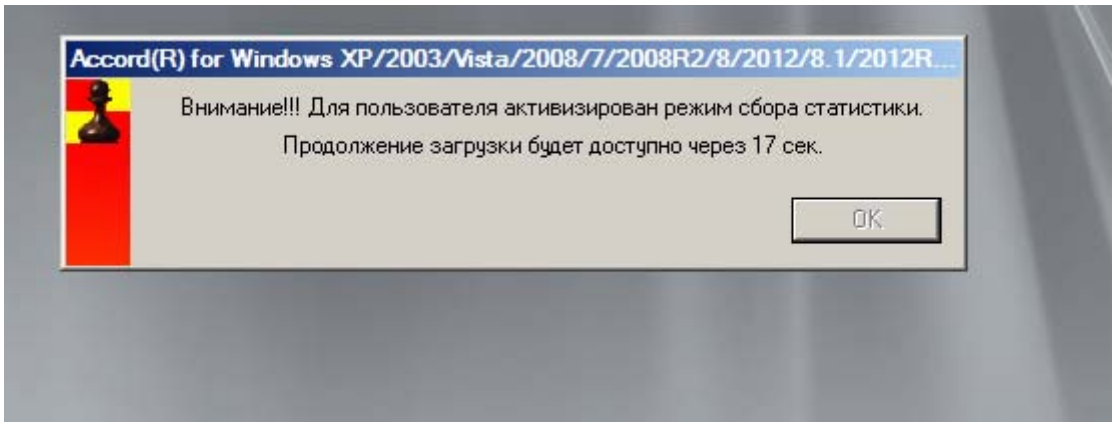

Рисунок 78 - Информационное сообщение

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

завершить сеанс пользователя[1], запустить от имени Администратора СЗИ от НСД «Аккорд» программу AcProc.exe (Программы\Аккорд\Создание списка процессов из журналов регистрации, рисунок 79);

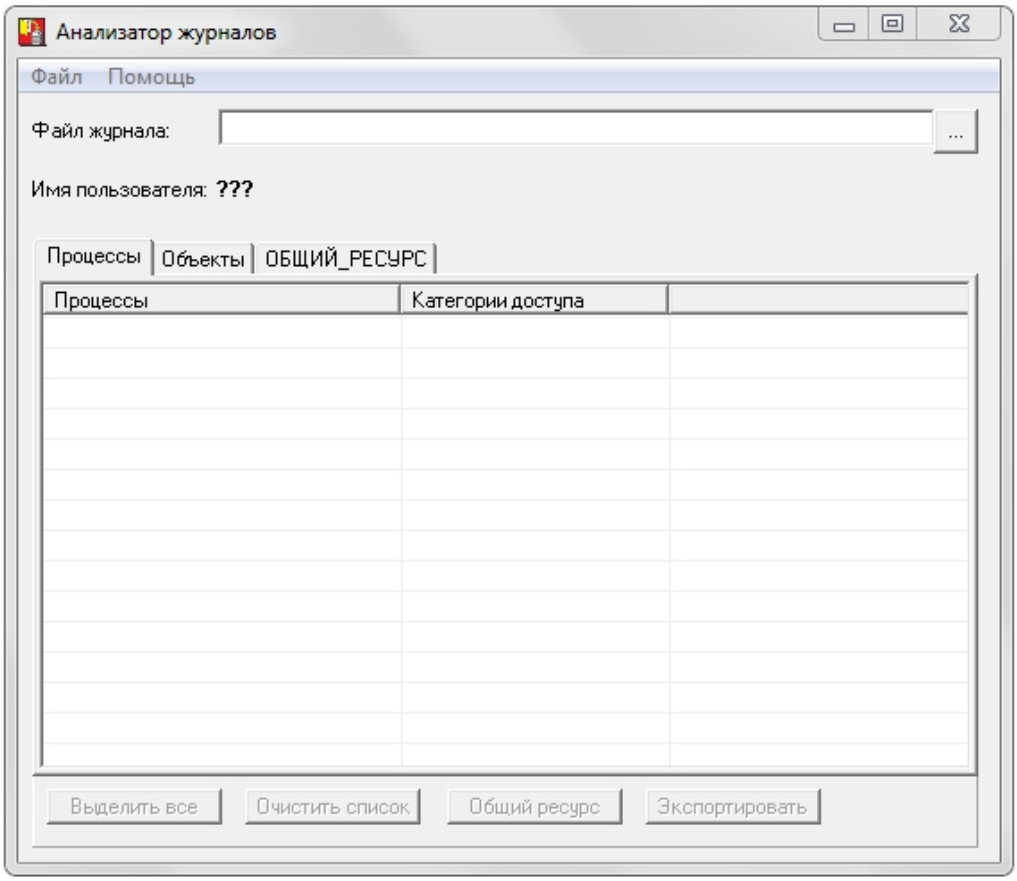

Рисунок 79 – Главное окно утилиты AcProc.exe

во вкладке «Процессы» загрузить журнал последнего сеанса работы пользователя: в окне программы AcProc.exe (рисунок 79) нажать на раскрывающийся список в поле «Файл журнала»), далее в появившемся на экране окне (рисунок 80) выбрать файл журнала (или несколько файлов);

[1)] 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»)

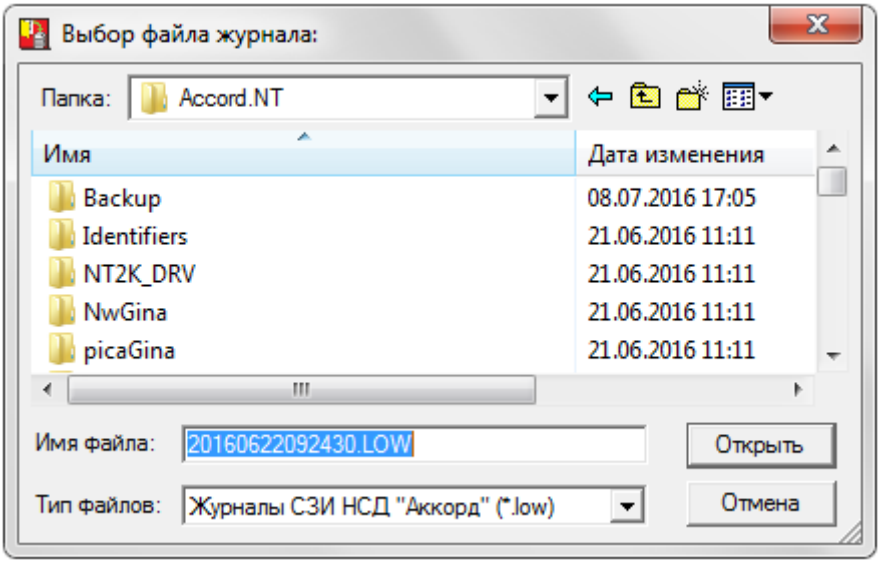

Рисунок 80 - Выбор файла журнала регистрации событий

в главном окне программы AcProc.exe выбрать процессы, которые необходимы для выполнения должностных обязанностей пользователя и нажать кнопку <Экспортировать> (рисунок 81);

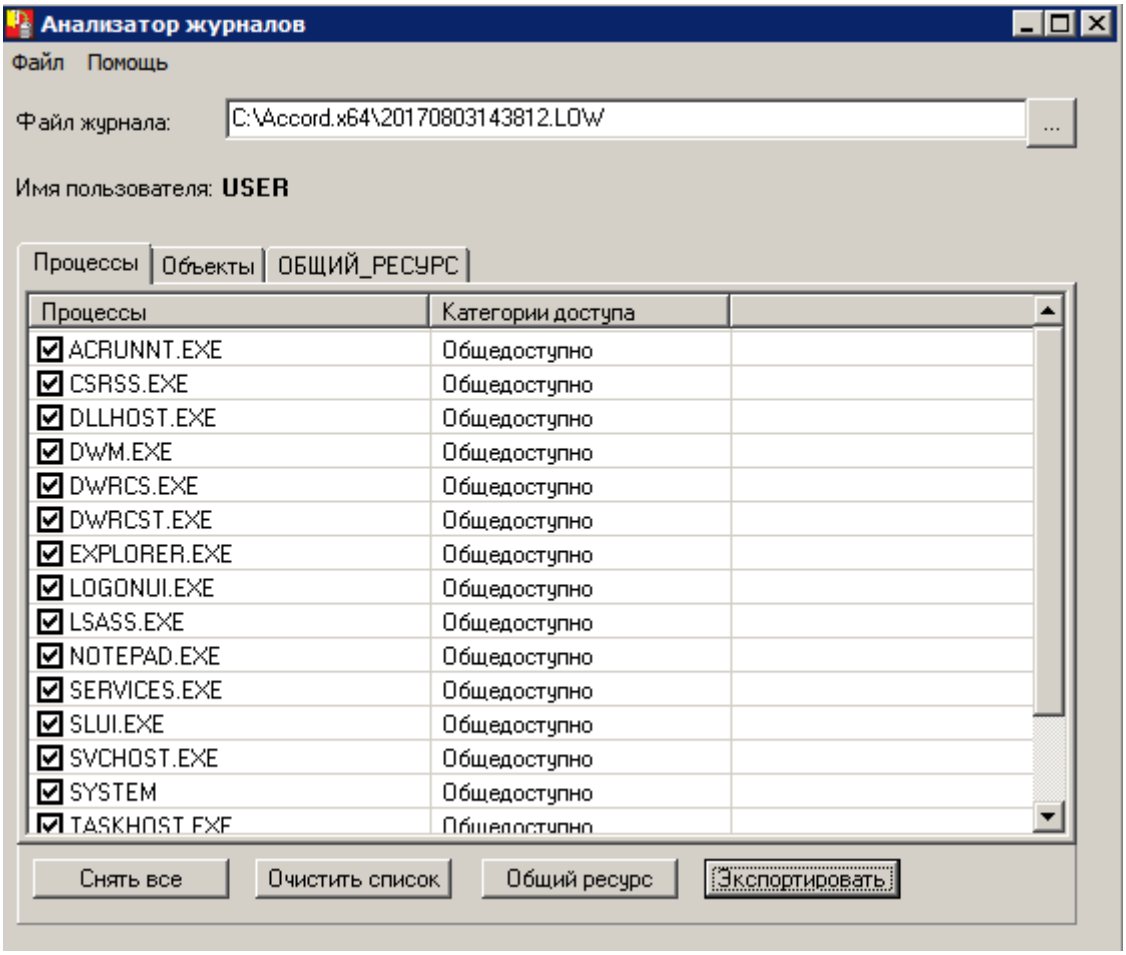

Рисунок 81 - Главное окно программы AcProc.exe. Выбор процессов

в появившемся на экране 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 82);

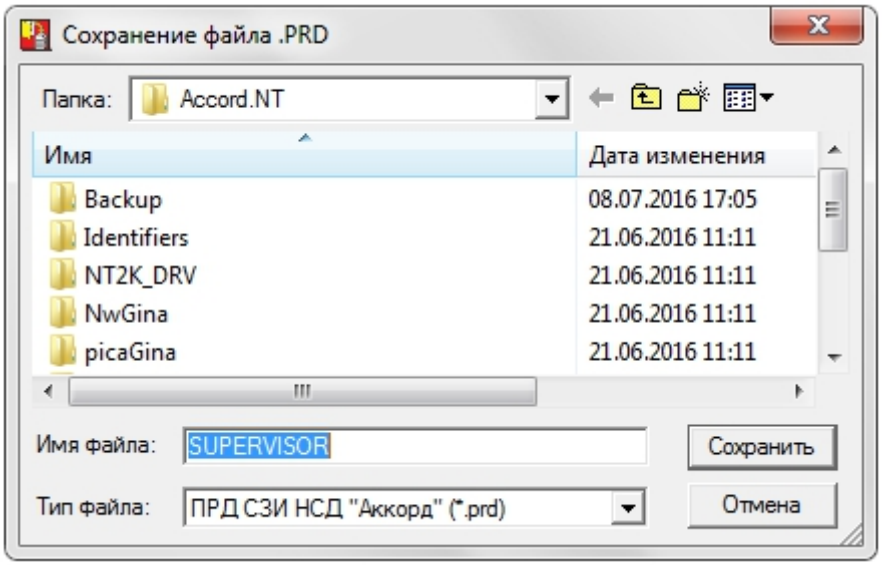

Рисунок 82 – Сохранение процессов в файл .prd

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 83);

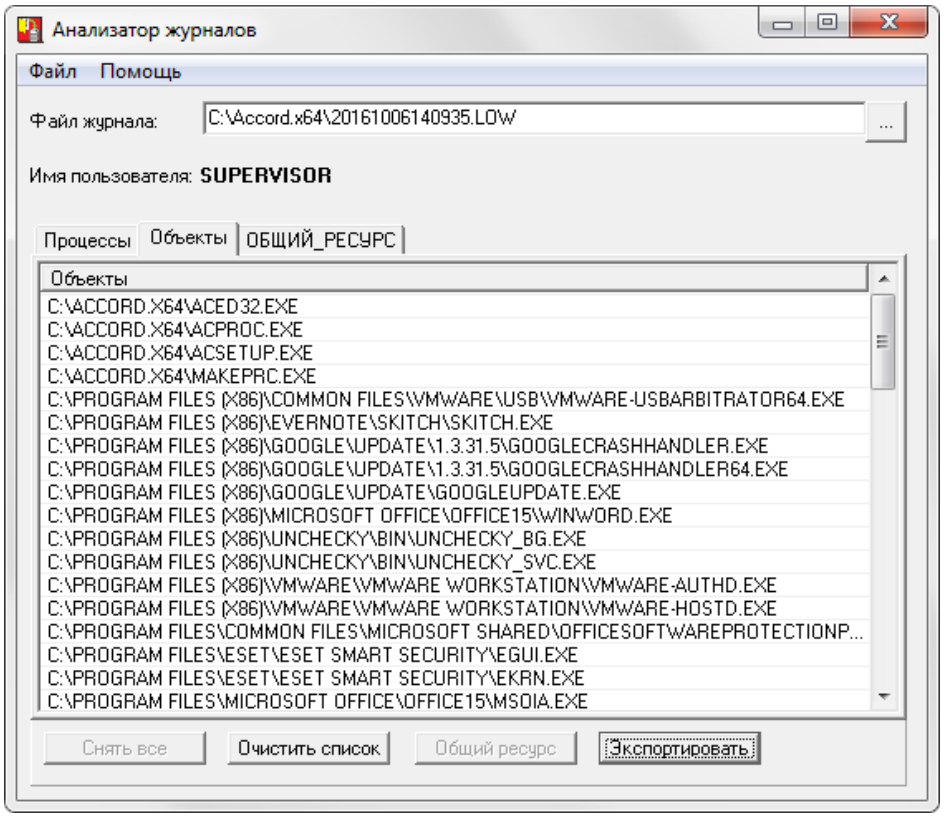

Рисунок 83 – Главное окно программы AcProc.exe. Вкладка «Объекты»

в появившемся на экране 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 84);

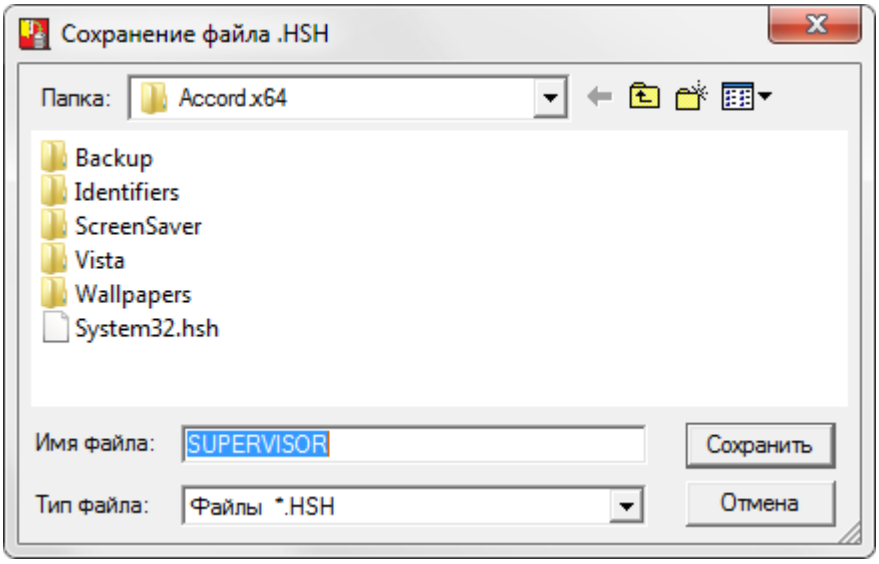

Рисунок 84 – Сохранение объектов в файл .hsh

затем необходимо вновь запустить утилиту «Редактор прав доступа» (Программы\Аккорд\Редактор прав доступа) и выбрать меню Файл\Импорт ПРД (рисунок 85);

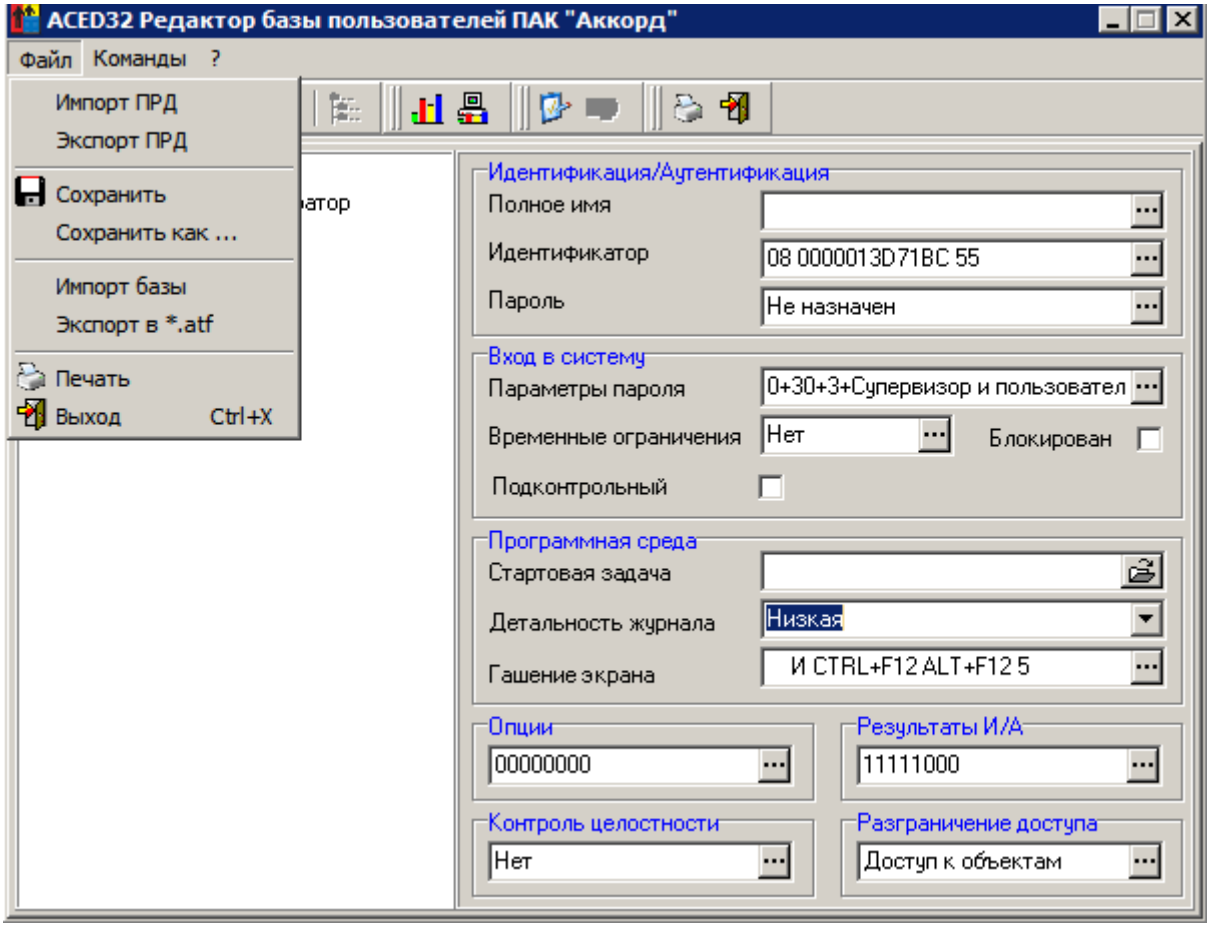

Рисунок 85 – Импорт ПРД

после этого на экране появляется окно выбора файла со списком процессов (рисунок 86);

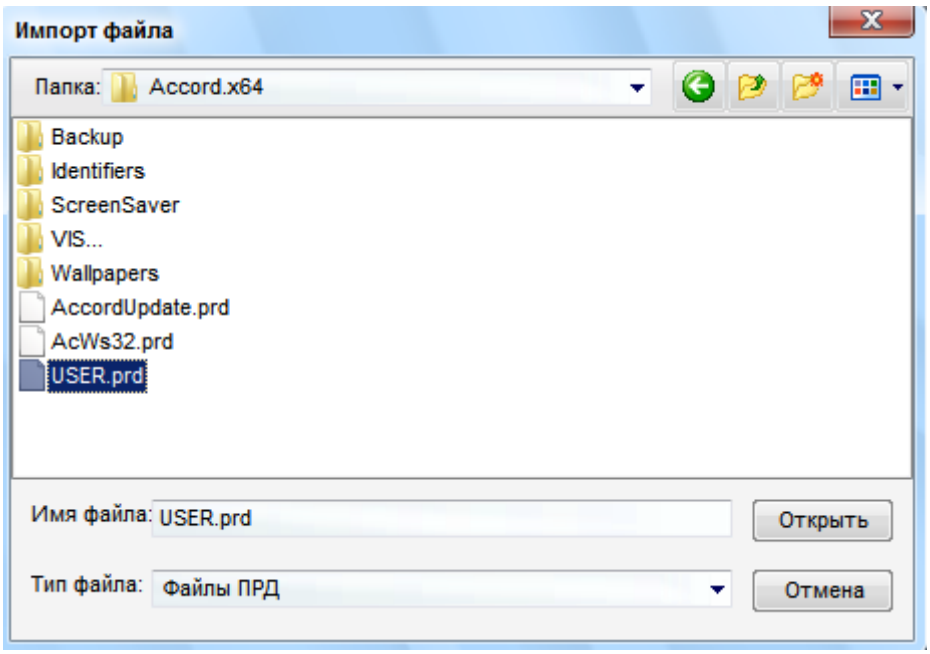

Рисунок 86 – Окно выбора файла со списком процессов

необходимо выбрать файл (рисунок 86) и нажать кнопку <Открыть>;

в появившемся на экране окне следует установить флаг «Для процессов» и нажать кнопку <Импорт> (рисунок 87);

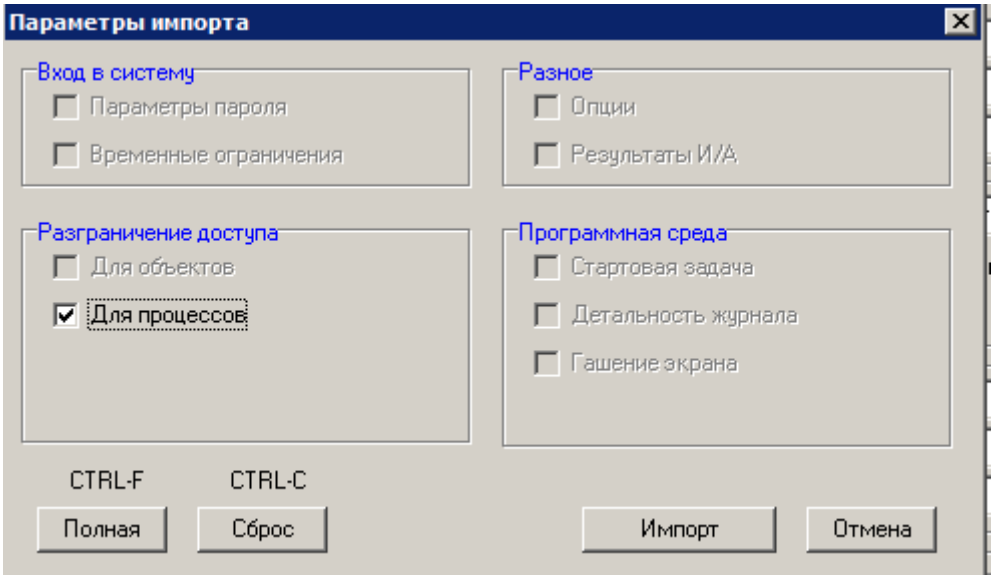

Рисунок 87 – Параметры импорта

в появившемся далее окне со списком импортированных процессов (рисунок 88) следует отметить необходимые (или же выбрать все процессы, нажав кнопку <Выбрать все>), а также (в случае необходимости) отметить флаги, показанные внизу окна 88, и нажать кнопку <OK>. Убедиться в корректности выполнения процедуры импорта можно нажав на кнопку <...> в поле «Разграничение доступа» главного окна программы ACED32;

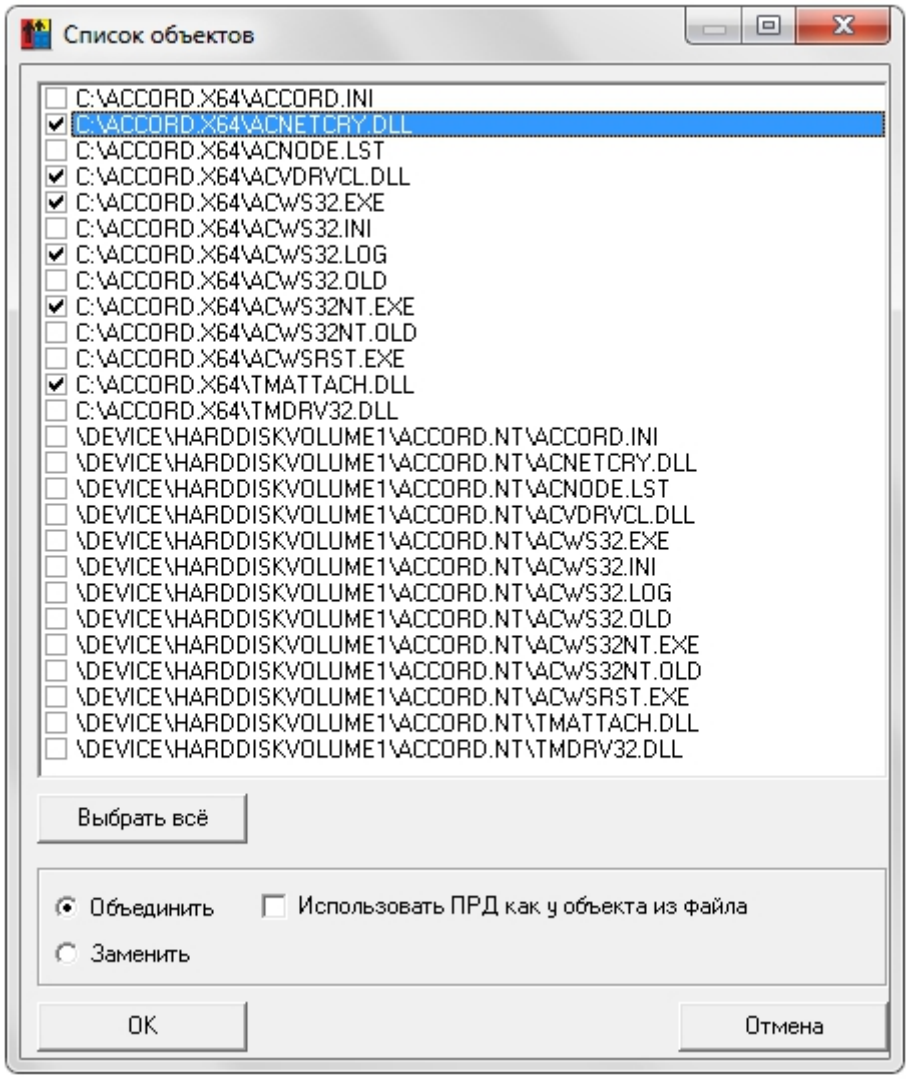

Рисунок 88 – Список импортированных процессов

далее в меню разграничения доступа для пользователя следует установить импортированным процессам соответствующие уровни доступа (при выполнении мандатного механизма разграничения доступа, рисунок 89), а также убедиться, что все необходимые процессы включены в список для контроля (при выполнении дискреционного механизма разграничения доступа, рисунок 90);

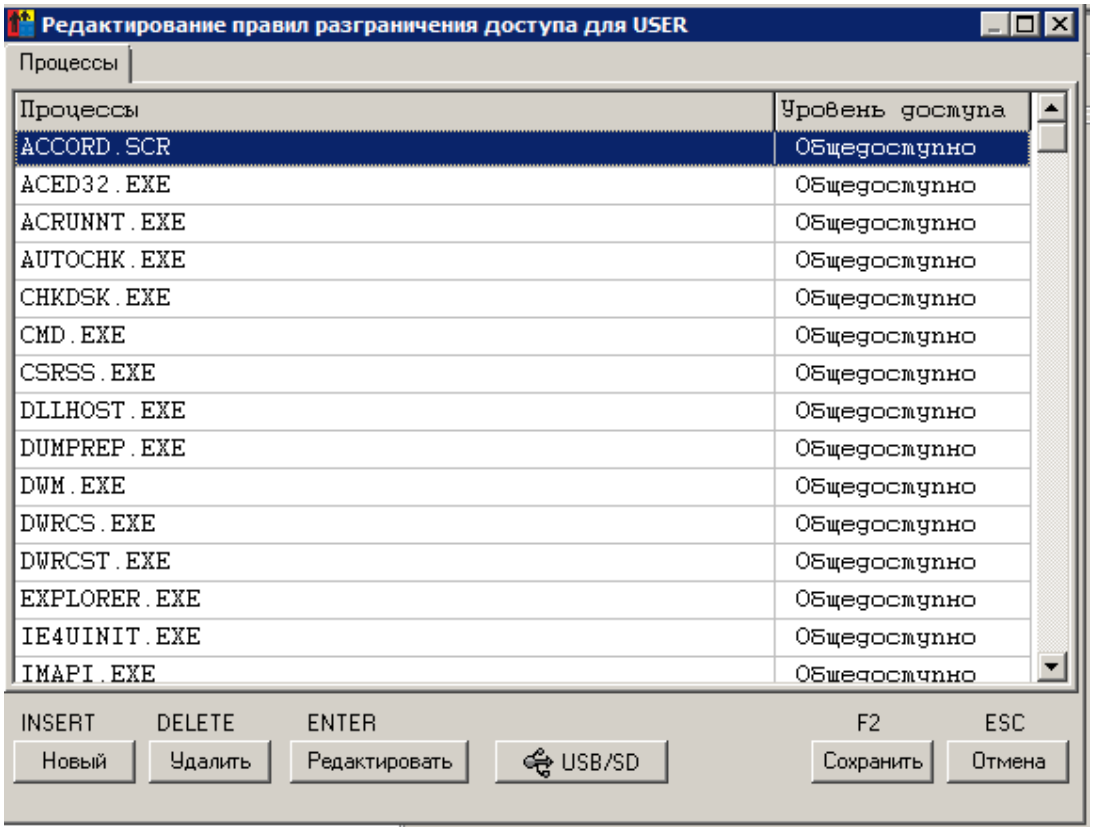

Рисунок 89 – Список импортированных процессов (мандатный механизм разграничения доступа)

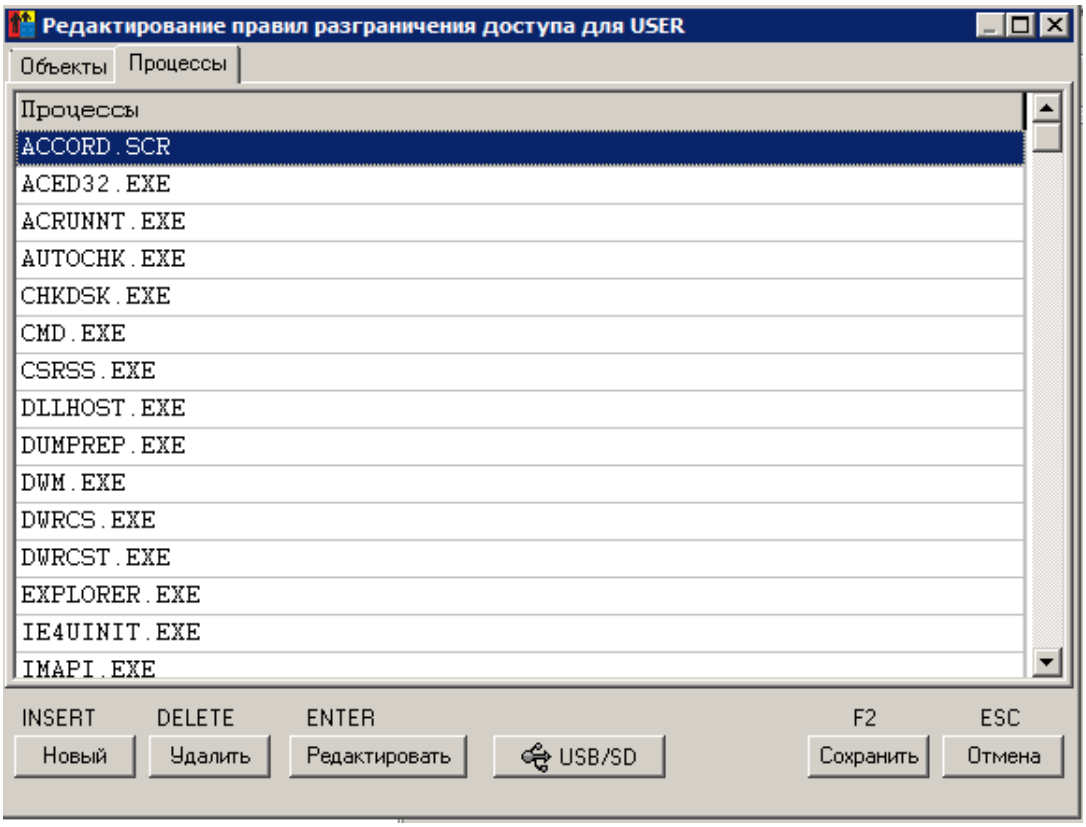

Рисунок 90 - Список импортированных процессов (дискреционный механизм разграничения доступа)

7.12.3.2. Установка динамического контроля целостности файлов из сформированного списка

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

в появившемся окне перейти во вкладку «Динамический» и нажать кнопку <Загрузить> (рисунок 91);

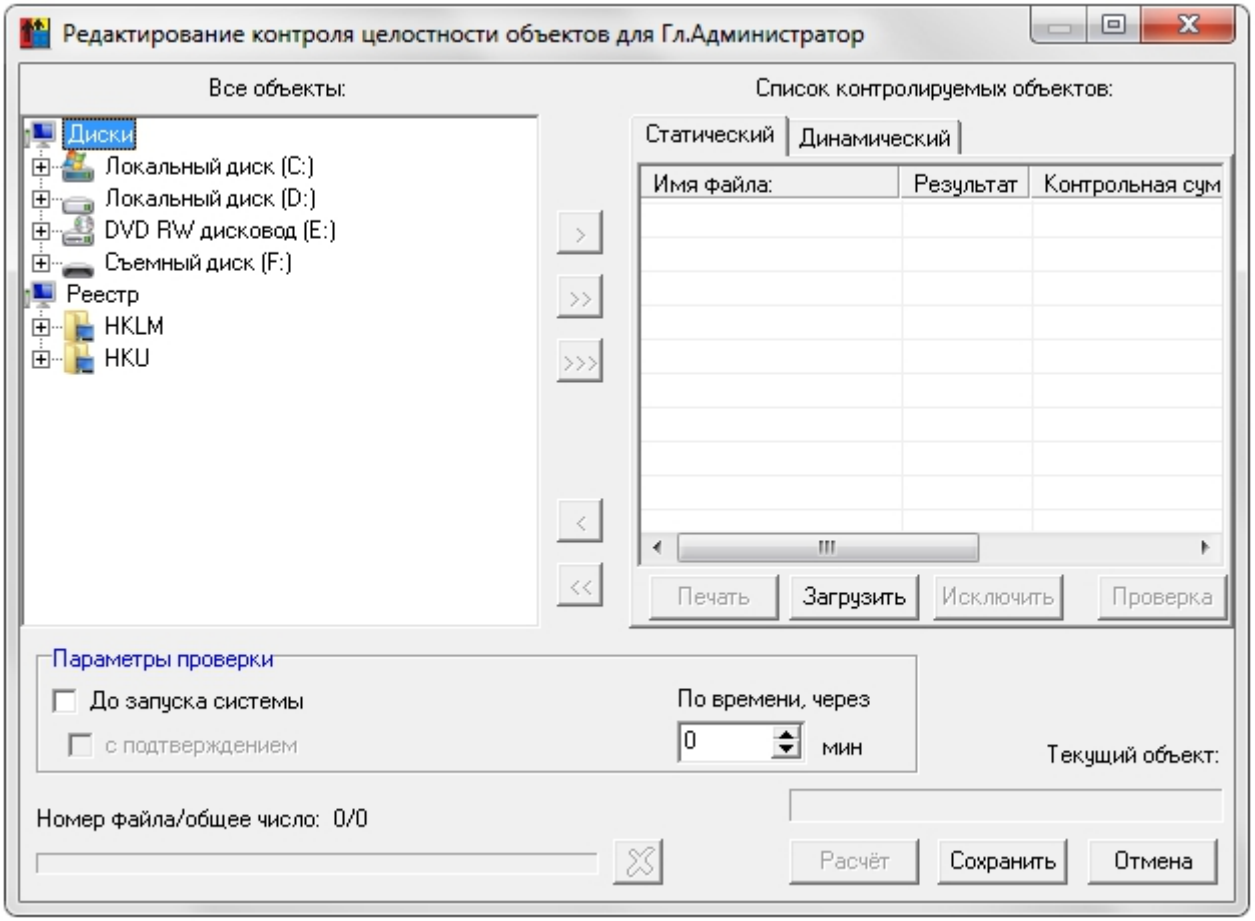

Рисунок 91 – Редактирование списков для контроля целостности пользователя

по нажатии кнопки на экране появляется окно выбора файла (рисунок 92). Необходимо выбрать файл со списком импортированных объектов, с которыми работал пользователь при выполнении должностных обязанностей (файл .hsh), и нажать кнопку <Открыть>;

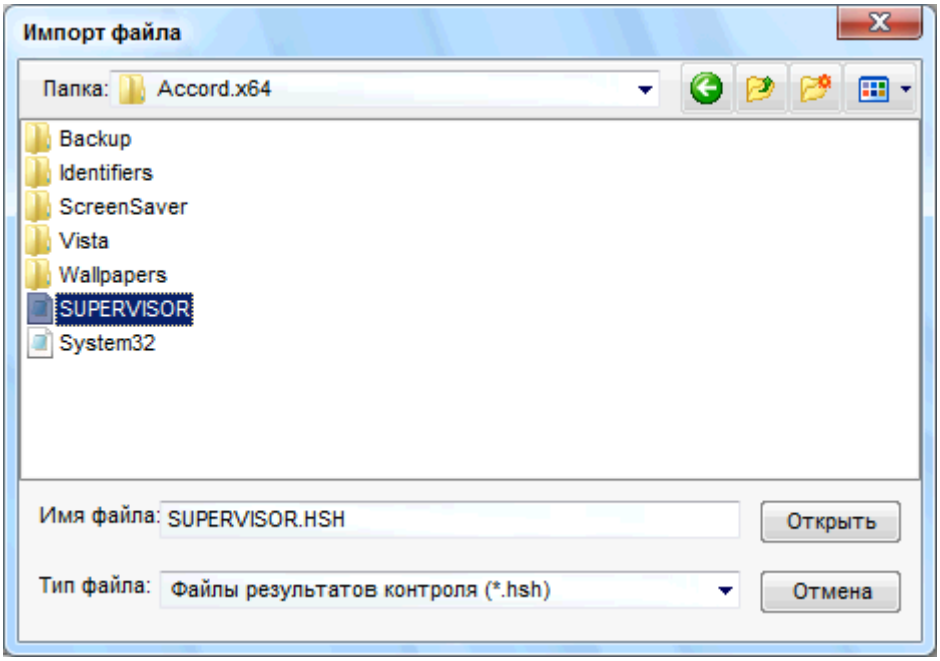

Рисунок 92 – Импорт файла со списком импортированных объектов

после этого окно для редактирования списков для контроля целостности примет вид (рисунок 93):

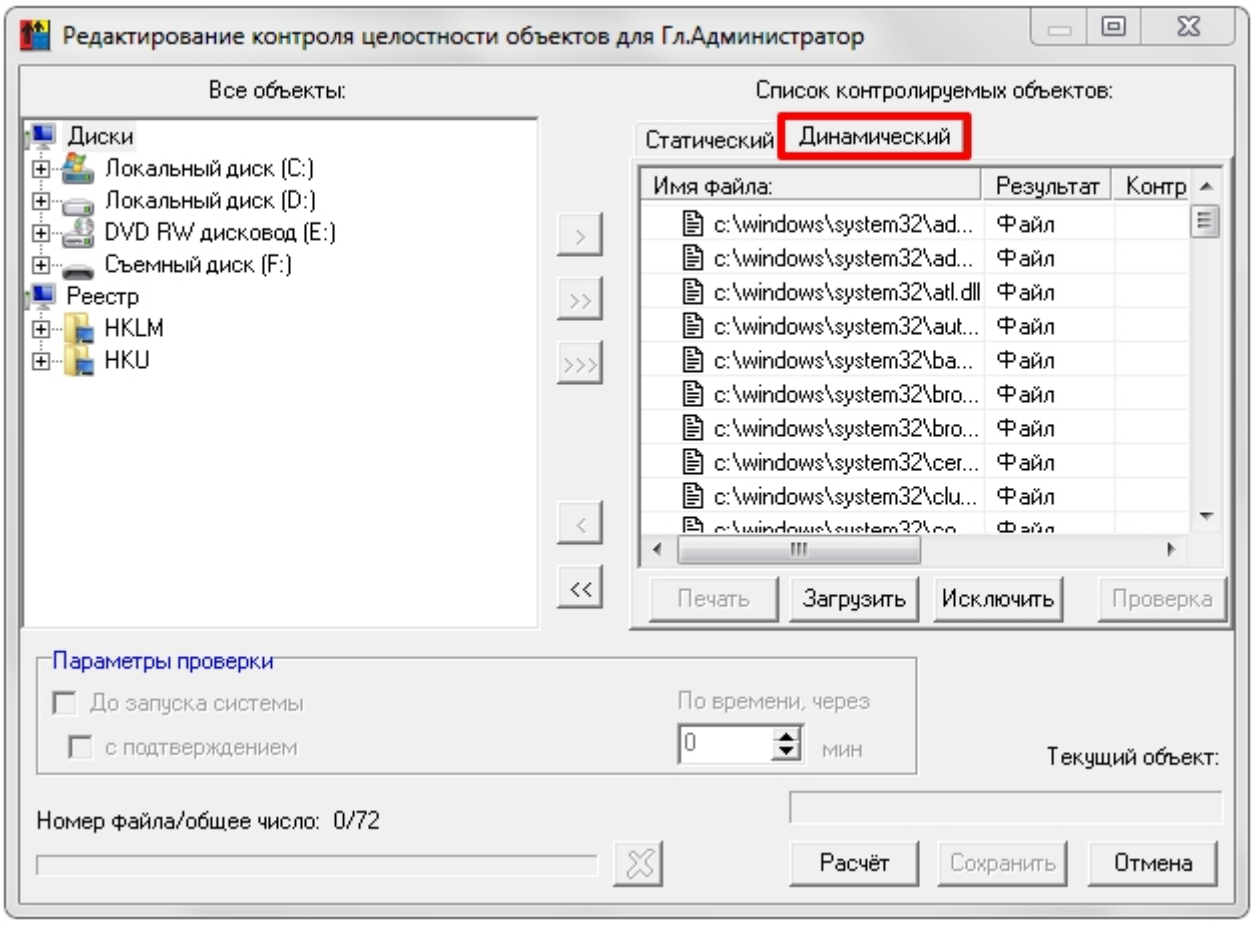

Рисунок 93 - Редактирование списков для контроля целостности. Импорт списка контролируемых объектов

затем необходимо выбрать объекты и нажать кнопку <Расчет> (рисунок 93);

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

после этого в графе «Контрольная сумма» появляются эталонные значения КС (рисунок 94);

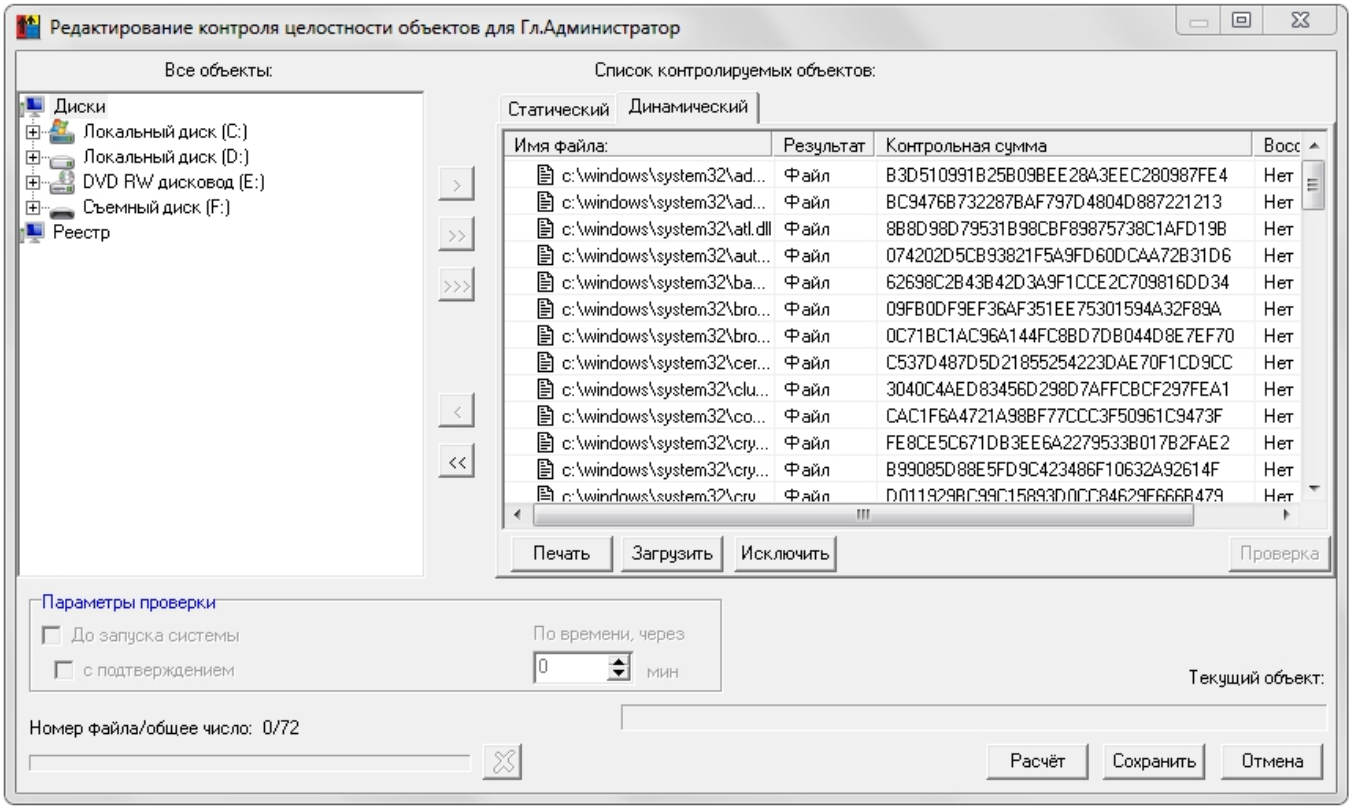

Рисунок 94 - Редактирование списков для контроля целостности. Контрольные суммы рассчитаны

по завершении процедуры расчета КС нужно нажать кнопку <Сохранить> (рисунок 94).

По окончании всех настроек убедитесь в том, что в программе настройки комплекса «Аккорд» **снят флаг «Мягкий режим»** (рисунок 77).

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 95).

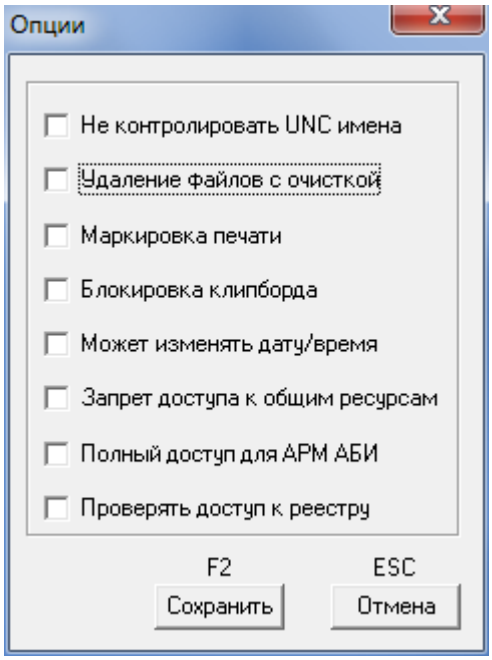

Рисунок 95 - Опции настройки

Дополнительные опции работы пользователя в СЗИ «Аккорд-Win64»:

- *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. При удалении файлы сразу очищаются в корзине;
- *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 ПАК СЗИ «Аккорд»» реализована дополнительная функция, существенная для работы защищенного СВТ в составе ЛВС. Это 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 96.

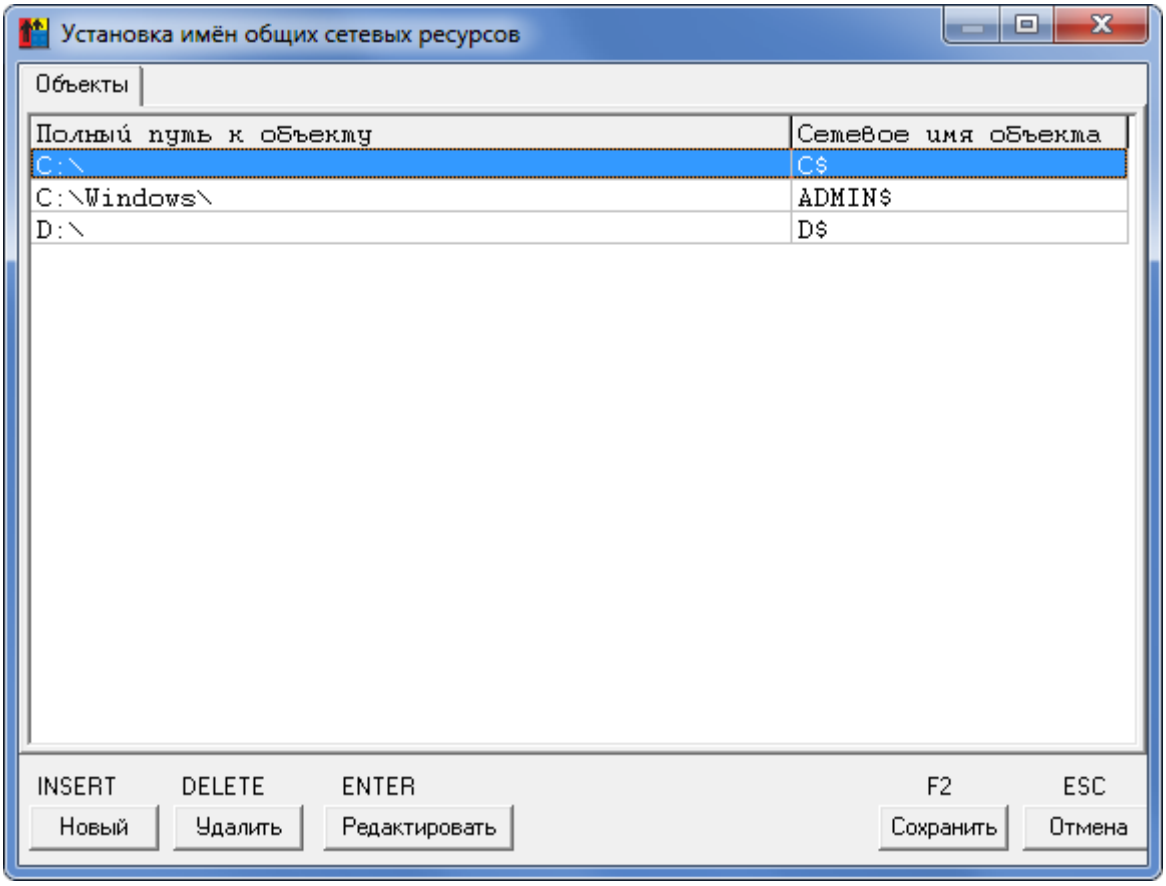

Рисунок 96 - Список ресурсов, выделяемых для общего доступа

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 установленной СЗИ «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, неуказанному 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 97).

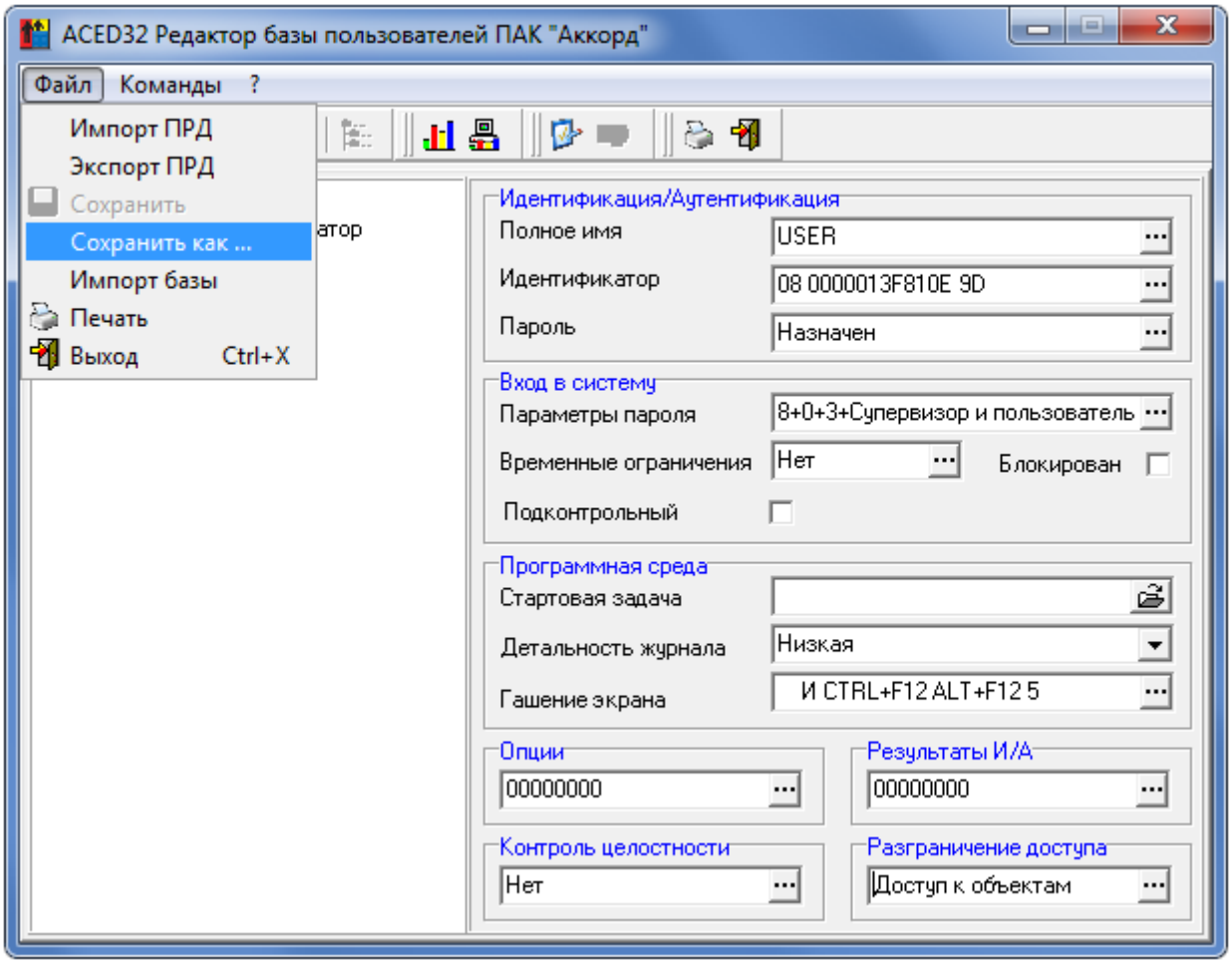

Рисунок 97 - Команды работы с базой данных пользователей

На экран выводится окно «Сохранить как» для выбора имени файла, показанное на рисунке 98.

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 сменный носитель и хранить как средство восстановления данных.

Восстановить настройки пользователей можно, скопировав резервную базу в папку Accord.x64 под именем accord.amz. Для синхронизации с контроллером АМДЗ и базой пользователей ОС достаточно после копирования

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

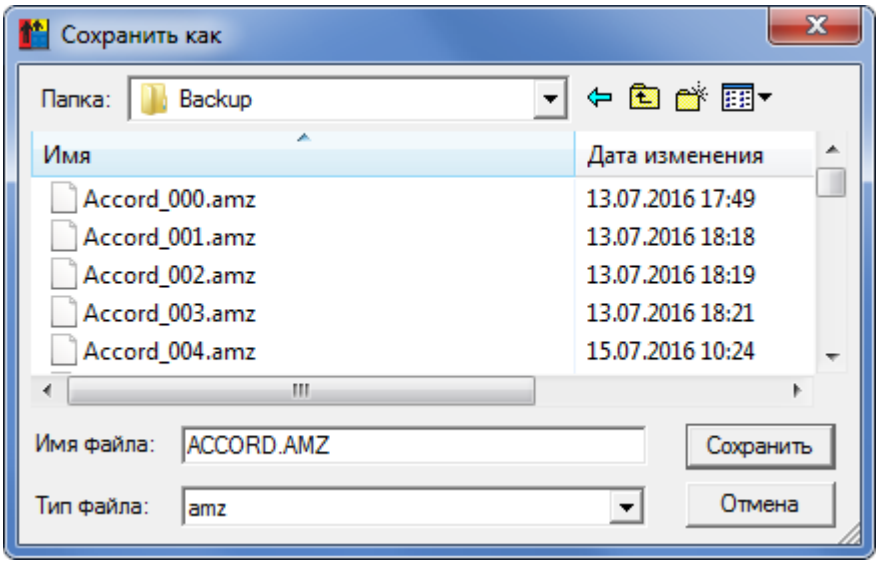

Рисунок 98 - Выбор имени файла для сохранения

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 99).

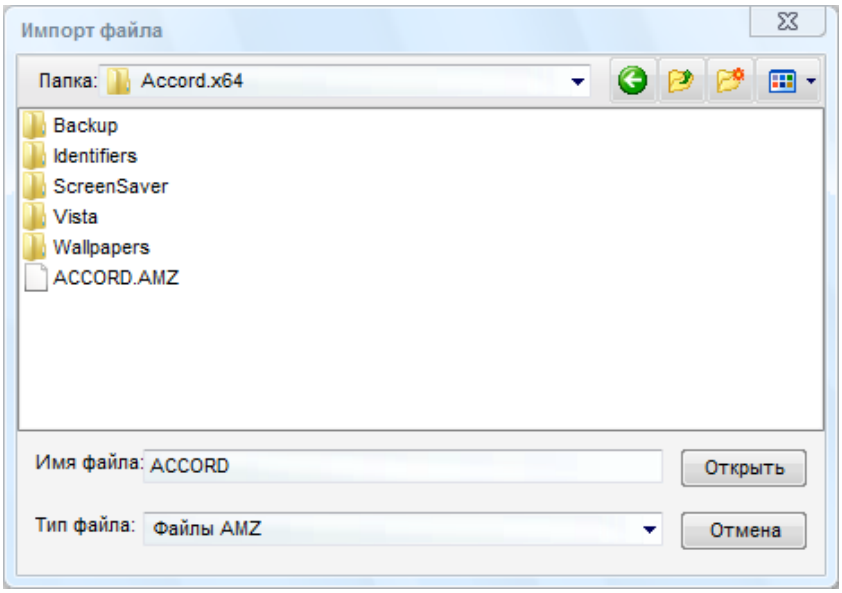

Рисунок 99 - Выбор файла для импорта базы данных пользователей

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 на дискете. После получения файла пользователь, выполняющий обязанности администратора удаленного компьютера, копирует его на жесткий диск и выполняет синхронизацию. При этом администратору удаленного компьютера достаточно самых простых, базовых знаний по настройке комплекса «Аккорд». В этой технологии может возникнуть еще одна проблема, если пользователь зарегистрирован в базе данных .amz, но отсутствует в памяти контроллера АМДЗ. Если в настройках комплекса включена синхронизация с базой АМДЗ, то при старте редактора ПРД AcED32.EXE база первоначально считывается из контроллера, и пользователи, отсутствующие в контроллере не учитываются. Для выхода из такой ситуации предназначена программа Acsync.exe. Запуск этой программы с параметром /1 позволяет считать список пользователей из платы в файл accord.amz. Запустив программу с параметром /2, Вы скопируете данные из файла accord.amz в плату контроллера АМДЗ. После этого можно запускать редактор ПРД и выполнить синхронизацию со списком пользователей в ОС.

Для обмена данными между платой и файлом accord.amz нужно предъявить идентификатор и ввести пароль пользователя, зарегистрированного в группе «Администраторы» в базе данных контроллера «Аккорд-АМДЗ».

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 100).

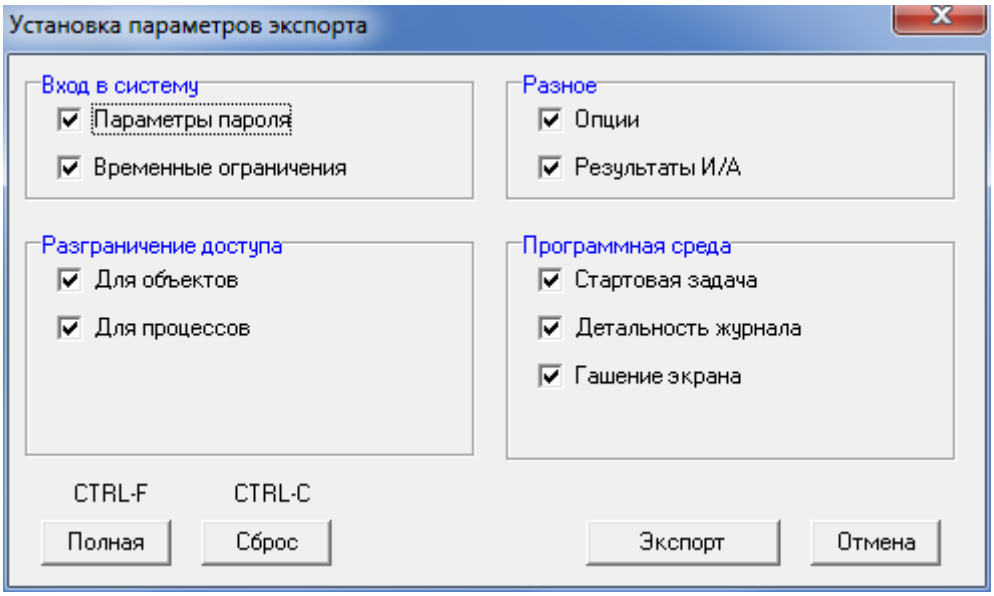

Рисунок 100 - Выбор параметров ПРД для экспорта

После выбора необходимого перечня экспортируемых параметров нажмите кнопку <Экспорт>. Выводится окно ввода имени файла для сохранения (рисунок 101).

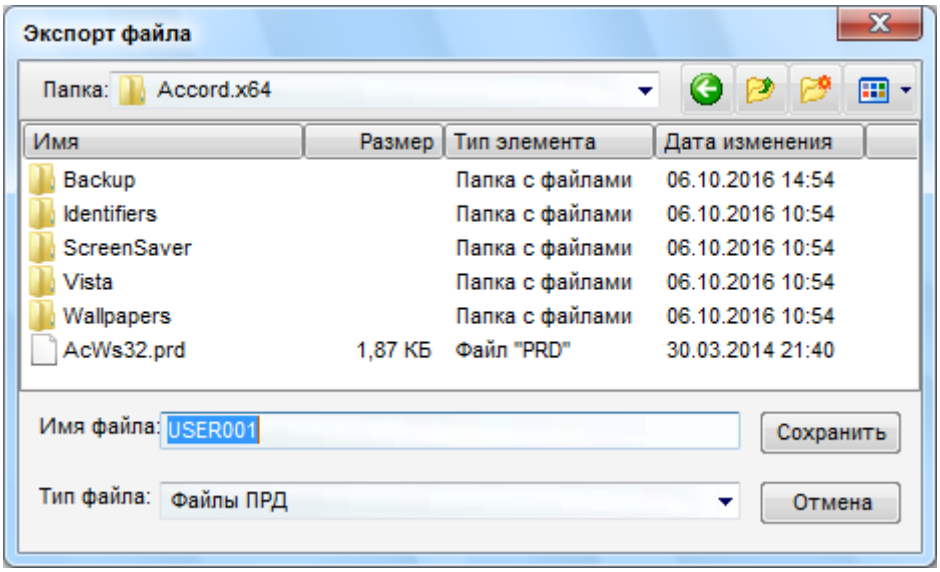

Рисунок 101 - Выбор имени файла для экспорта ПРД

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 102).

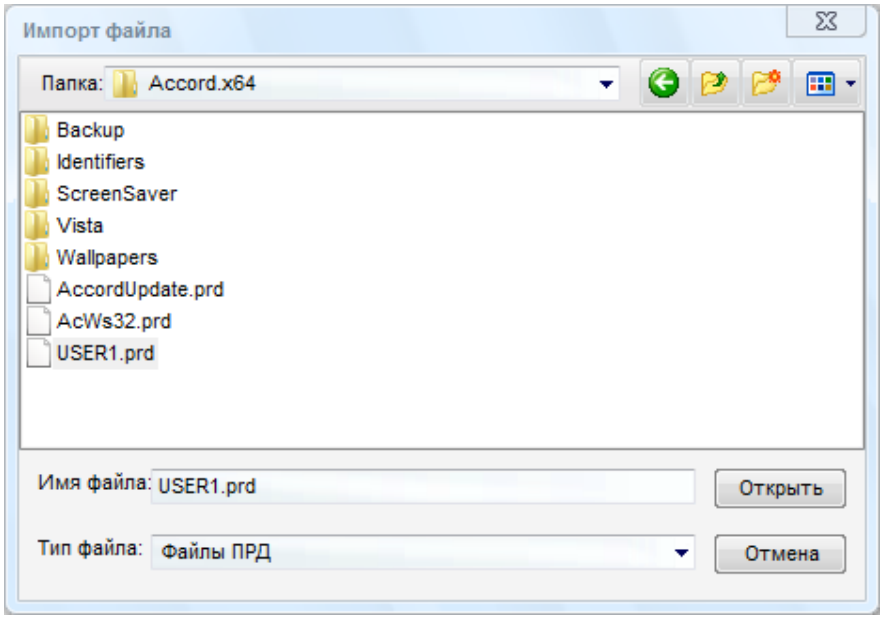

Рисунок 102 - Выбор имени файла для импорта ПРД

После ввода имени файла нажмите кнопку <Импорт>. После этого на экран выводится окно выбора параметров, которые предполагается импортировать данному пользователю (рисунок 103).

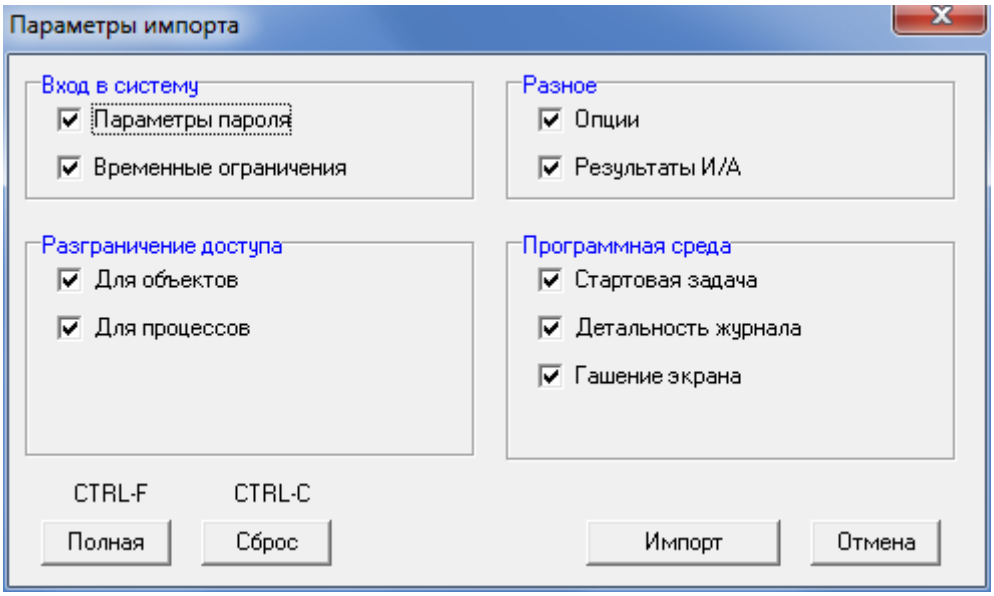

Рисунок 103 - Выбор параметров для импорта

Мышью следует выбрать параметры и нажать кнопку <Импорт>. На экран выводится окно выбора процедуры включения ПРД в настройки пользователя (рисунок 104).

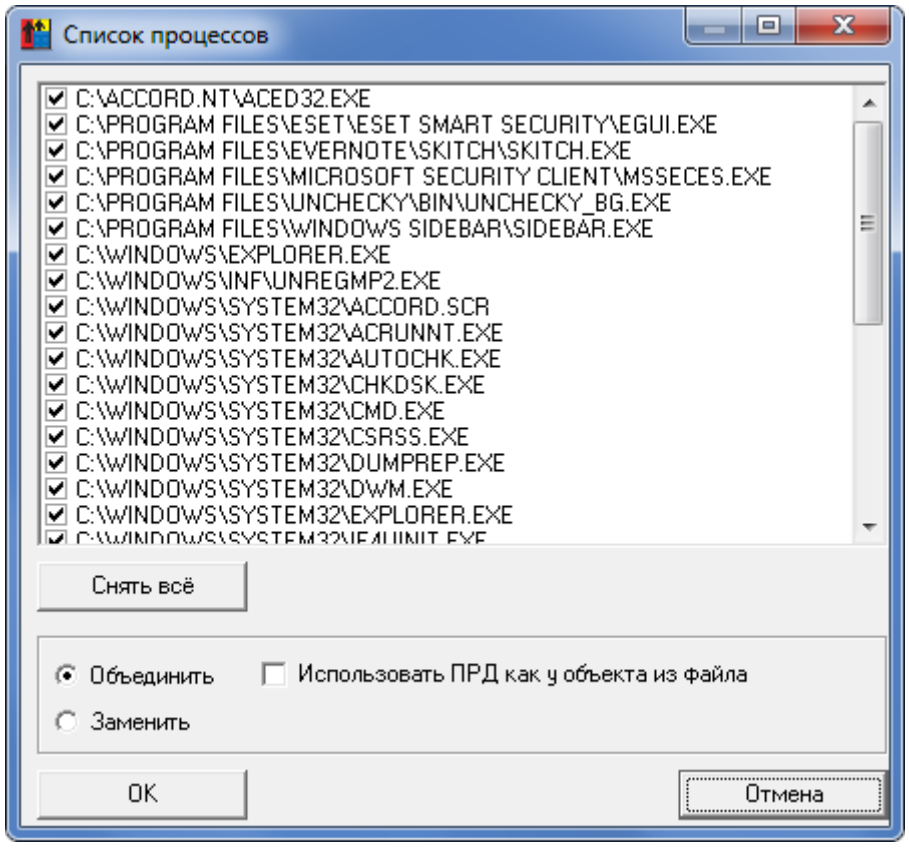

Рисунок 104 - Выбор процедуры формирования нового списка ПРД

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.x64 и выполняет запись в файл регистрации событий. В ПРД пользователя по умолчанию запрещен доступ к каталогу Accord.x64, чтобы пользователь не мог нарушить настройки системы защиты. В файле acws32.prd прописан набор правил доступа к тем файлам в каталоге 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 комплекса «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 СЗИ от НСД «Аккорд-Win64», «Аккорд-Win64» (TSE) 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 сменному 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 50) щелкнуть мышью по клавише <USB/SD>. Открывается окно редактирования списка устройств (рисунок 105).

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.

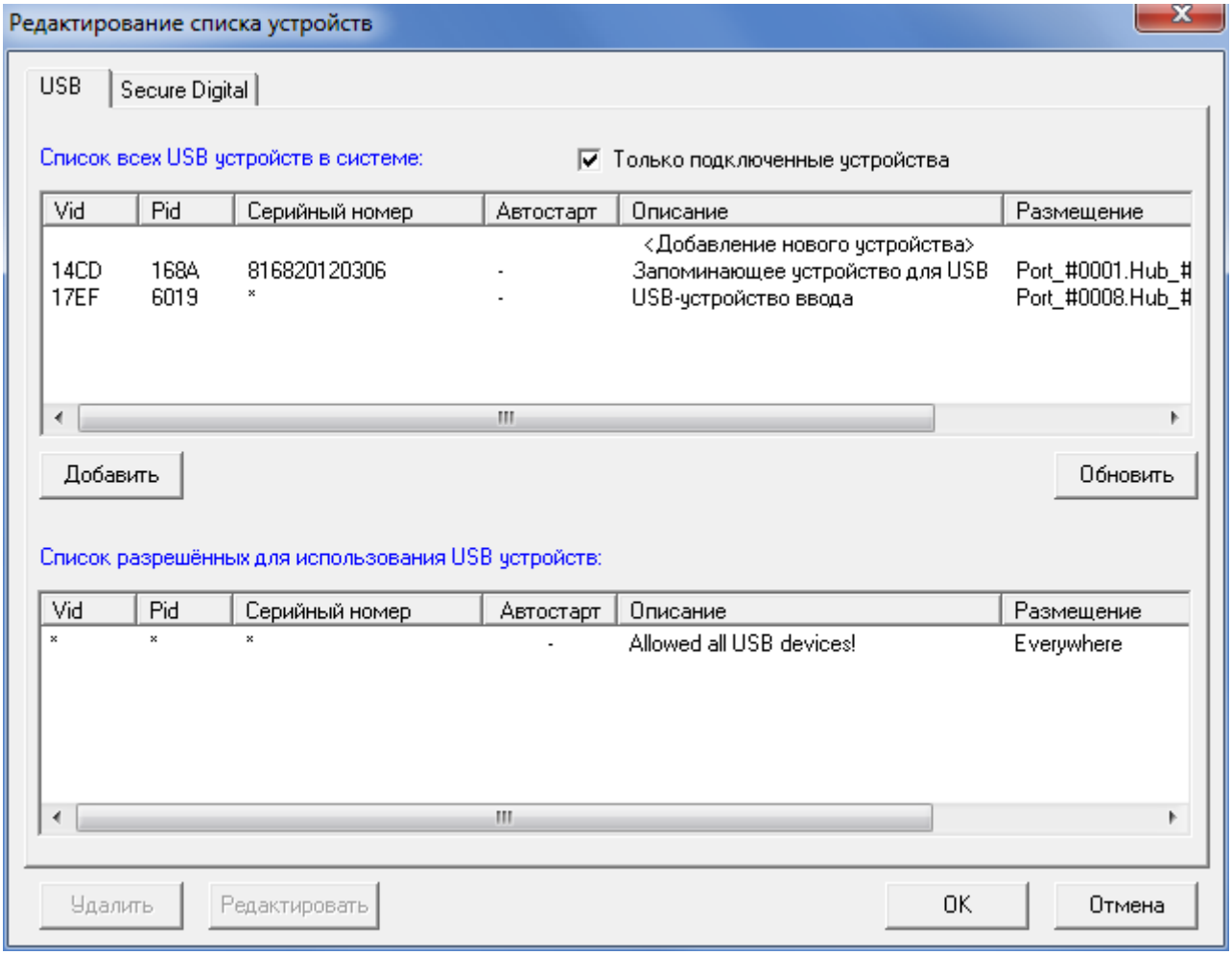

Рисунок 105 - Окно редактирования списка разрешенных USB устройств

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 106). 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 50).

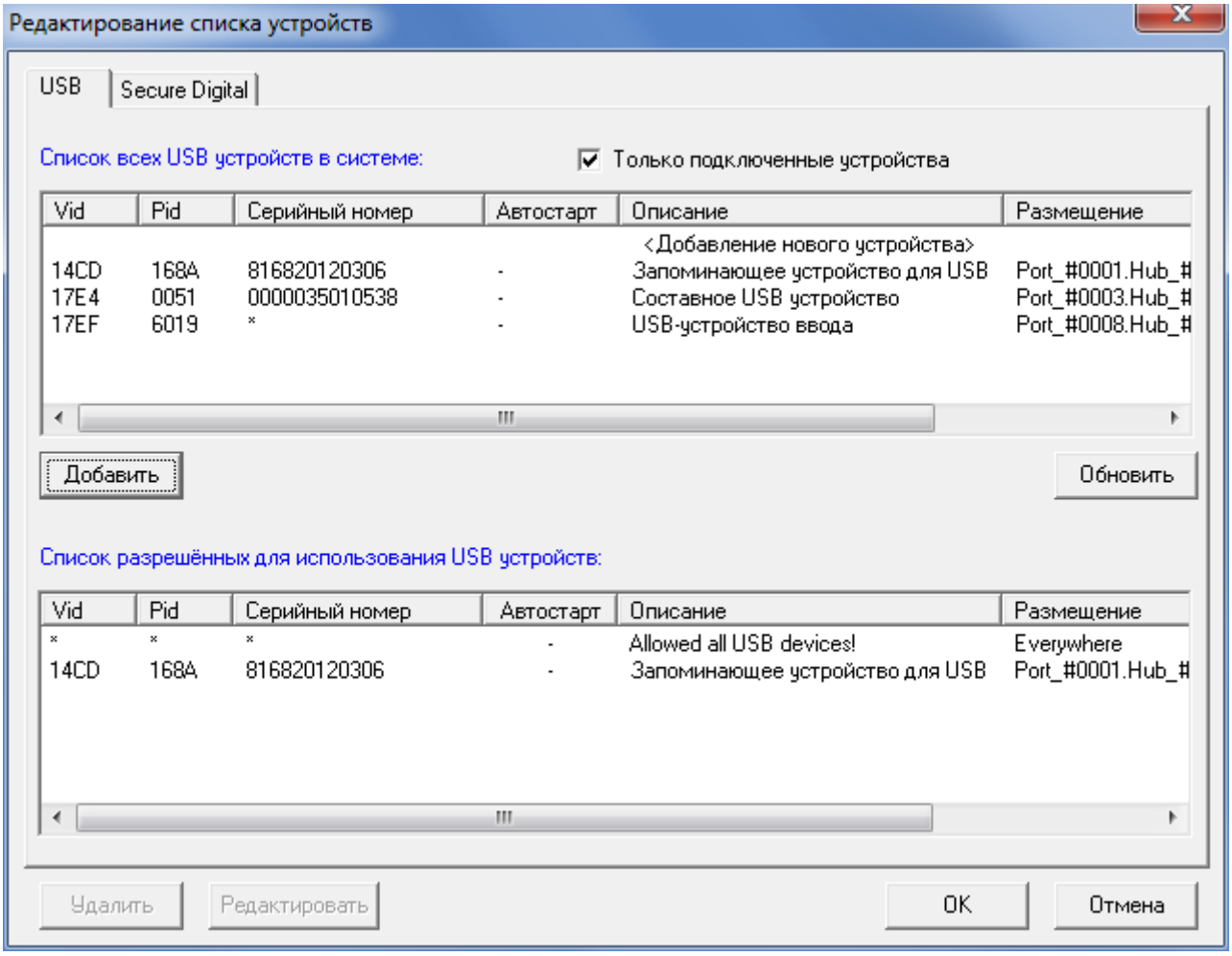

Рисунок 106 - USB устройство добавлено в список разрешенных

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[1].

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! Процедура описания правил доступа к съемным дискам выполняется корректно только в том случае, когда сменное устройство подключено к компьютеру ДО запуска программы ACED32.EXE и остается подключенным до завершения процедуры сохранения базы данных пользователей.

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 ПАК «Аккорд» (Программы\Аккорд\Редактор прав доступа);

2) из списка учетных записей пользователей выбрать учетную запись Администратора виртуальной инфраструктуры (Администратора ВИ);

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.

[1)] Такие правила разграничения доступа будут действовать, если у пользователя в привилегиях Администраторов снят хотя бы один из четырех первых флагов (п. 7): «Редактирование пользователей», «Редактирование контроля», «Управление журналом», «Редактирование настроек». Снятие флага «Контролер» на доступ Администраторов к USB-устройствам не влияет.

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 комплекса «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. После запуска программы на экран выводится главное окно (рисунок 107).

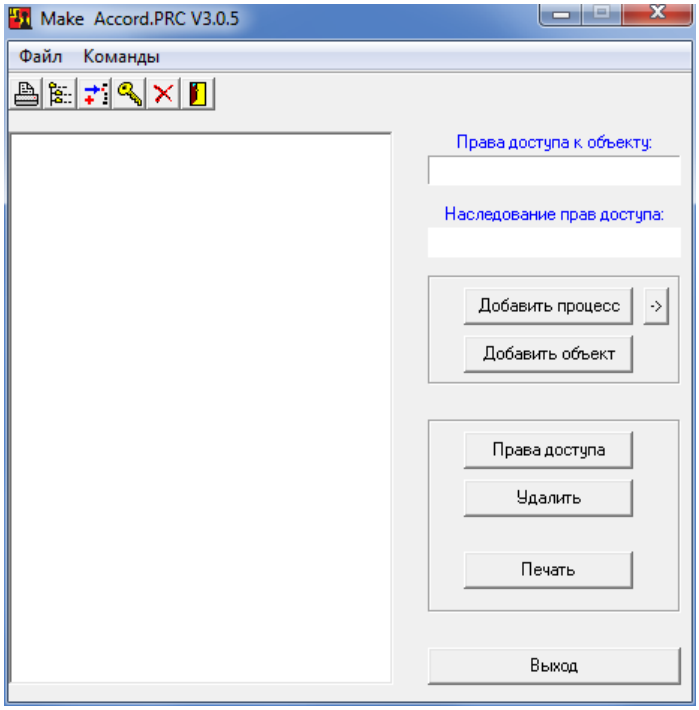

Рисунок 107 - Главное окно программы MakePrc

Необходимо добавить программу (процесс), для которой 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 108).

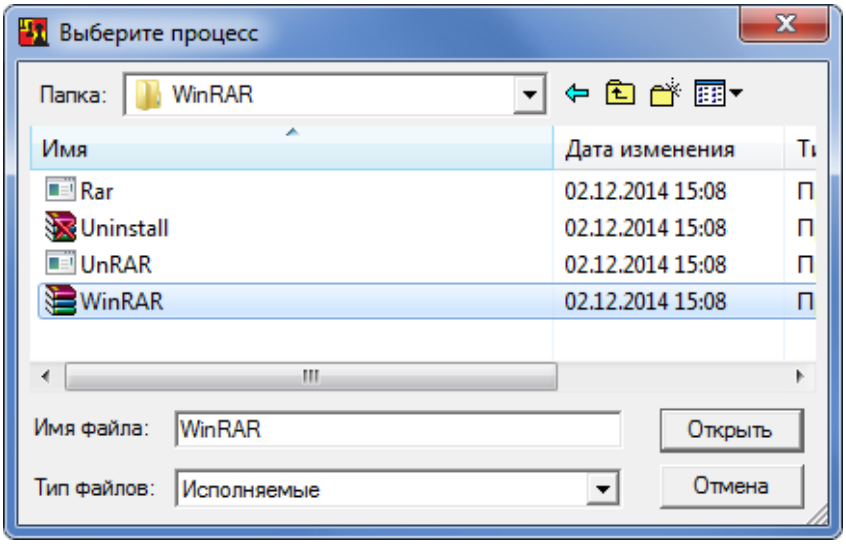

Рисунок 108 - Выбор процесса, для которого будут устанавливаться ПРД

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 сопоставить 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 109).

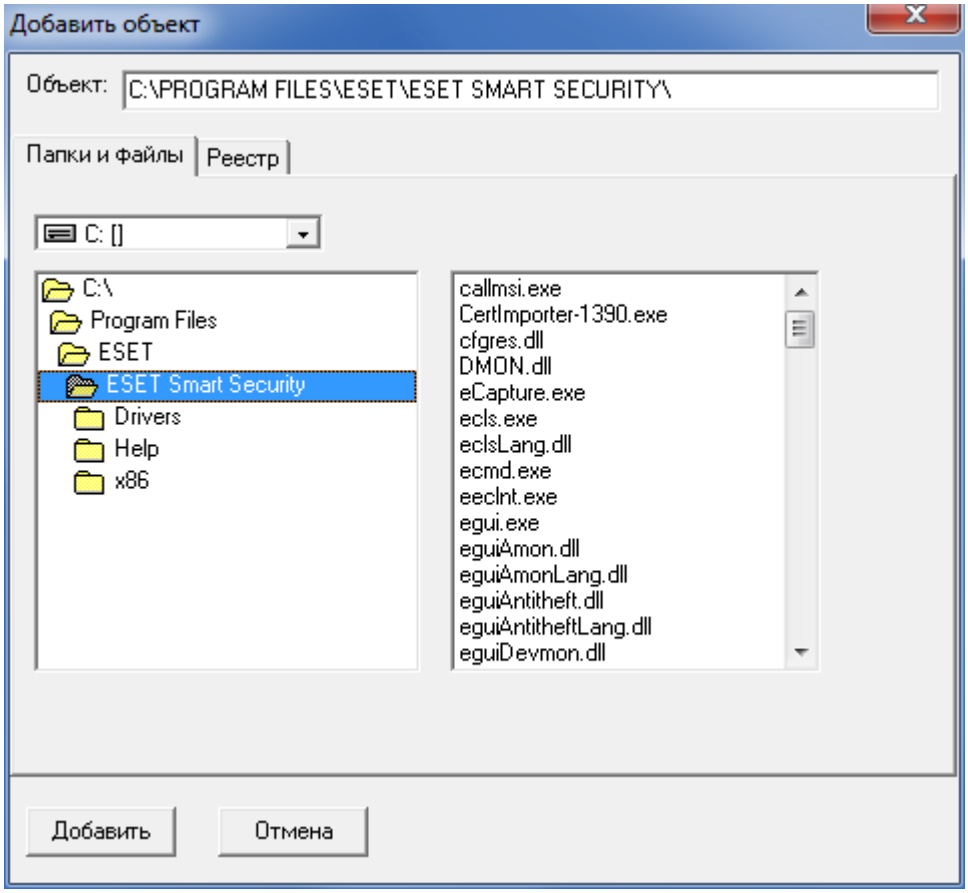

Рисунок 109 - Окно выбора файлов и каталогов

Отметьте необходимый каталог, нажмите кнопку <Добавить>. Выбранной 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 110). 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.

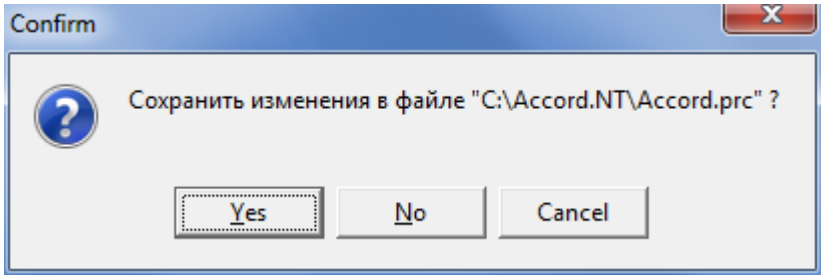

Рисунок 110 - Сохранение файла ПРД для выделенных процессов

Имеется возможность редактирования файла привилегированных процессов (*.PRC) в рамках работы программы ACED32.EXE. Для этого необходимо нажать кнопку <Редактирование списка привилегированных процессов>[1] на панели инструментов в главном окне программы ACED32.EXE (рисунок 8).

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» при синхронизации баз данных. Для того чтобы эта технология работала, в настройках комплекса 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 111).

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

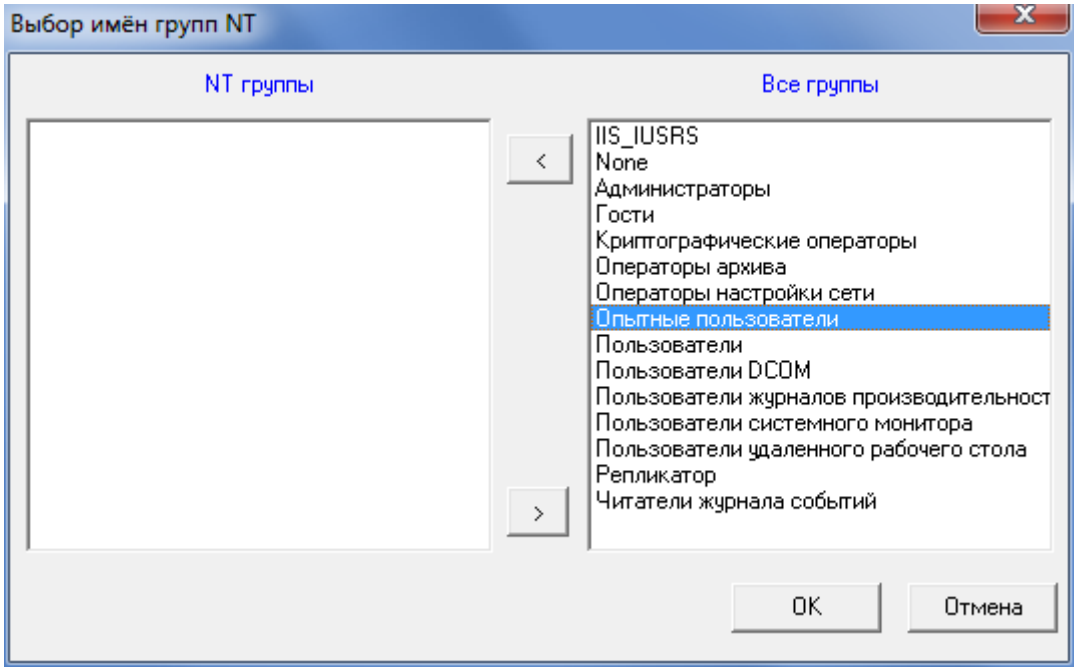

Рисунок 111 - Окно выбора групп пользователей

В правой половине окна перечислены все группы, в левую часть можно перенести одну, или несколько групп, к которой должны принадлежать пользователи ПАК СЗИ «Аккорд». Такой вариант показан на рисунке 112. 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», и «Обычные» соответствуют группе «Users/Пользователи» в зависимости от основного языка установленной ОС.

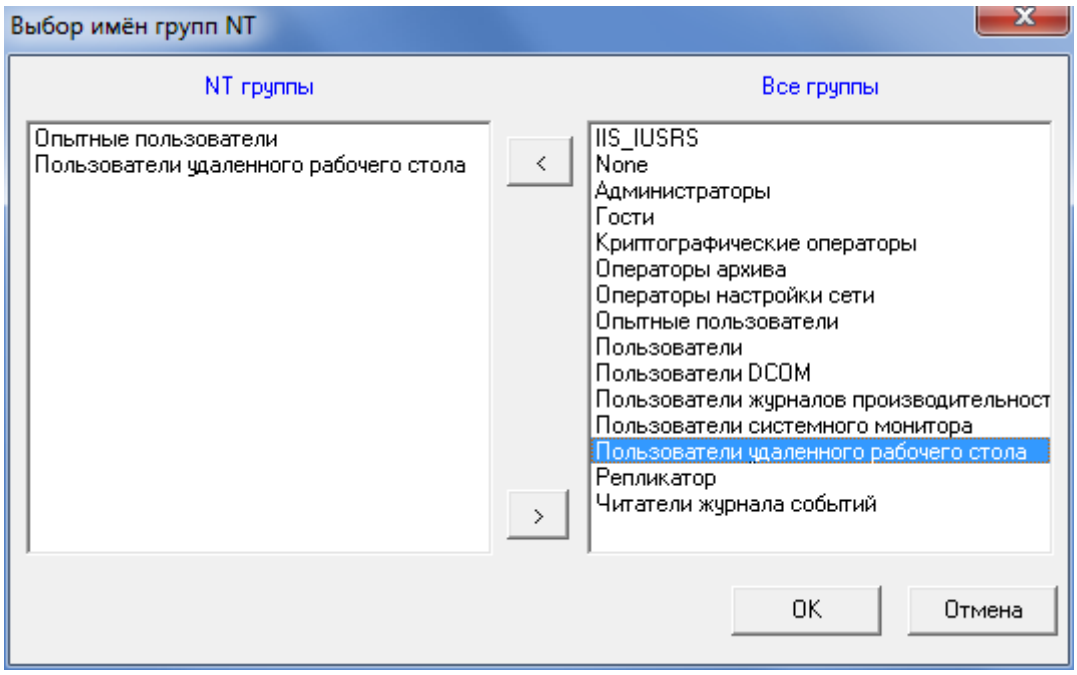

Рисунок 112 - Синхронизация пользователя СЗИ «Аккорд» с несколькими группами ОС

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 комплекса «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 проходит, поэтому данный флаг нужно выключить в программе настройки комплекса. 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.

Если все пользователи зарегистрированы в домене, а работать могут с разных компьютеров, то возникает проблема одновременной смены пароля на нескольких контроллерах АМДЗ. Может быть политика безопасности, которая вообще не предполагает локального входа пользователей на рабочие станции в составе домена.

Решить эту проблему средствами СЗИ Аккорд можно. Для начала регистрируем всех пользователей в одном контроллере АМДЗ. При регистрации пользователей в «параметрах пароля» минимальную длину ставим 0 (пароль не установлен). В «результатах И/А» включаются первые четыре флага (пароль не передавать). После регистрации всех пользователей выбираем команду «Экспорт», и сохраняем список на дискету, или TM DS1996.Следующий шаг - загрузка системы, установка драйвера контроллера АМДЗ и установка ПО «Аккорд». Сразу после установки запускаем программу настройки комплекса. В главном окне программы убираем флаг «Синхронизация с базой пользователей NT». Этот флаг отвечает за синхронизацию с локальной базой ОС, а в данной системе локальный вход нам не нужен. В меню «Параметры» - «Дополнительные опции» выбираем закладку «режим сессии» и включаем флаг «Использовать полное имя в учетных записях NT». Закрываем программу настройка с сохранением изменений. Теперь можно приступить к регистрации пользователей в программной части системы защиты. Запускаем редактор прав доступа. В момент первого запуска программа считывает список пользователей из контроллера АМДЗ (конечно только в том случае, когда предъявлен идентификатор администратора, зарегистрированный в плате). Рекомендуется в группе «Администраторы» в плате АМДЗ зарегистрировать пару резервных администраторов. Совершенно не важно, какие имена присваивать пользователям в плате АМДЗ, тем более, что аппаратная часть накладывает ограничения в 12 символов и английский алфавит. Следующий важный шаг - каждому пользователю, кроме администраторов, в поле «полное имя» ввести доменное имя пользователя, далее @<имя домена>. В поле «Пароль» задать пароль пользователя, который установлен на домене. Как поступить с

администраторами, решайте сами - можно задать полные имена как на домене и пароль соответствующий (для удаленного доступа), или управлять доменом с консоли, тогда полные имена не задавать, а в локальных базах завести таких администраторов, которые будут управлять только СЗИ. При выходе из редактора обязательно сохранить изменения. Теперь на любой носитель скопируем файл accord.amz из папки Accord.x64 и можно устанавливать систему Аккорд на других компьютерах. После установки платы в компьютер и начальной инициализации выбираем сразу команду «Импорт» в списке пользователей и загружайте сохраненную базу (кстати очень полезно и в дальнейшем иметь эту базу для быстрого восстановления в случае замены платы). В ОС устанавливаем драйвер контроллера, инсталлируем ПО, делаем все те же настройки, но редактор ПРД можно не запускать, а сразу скопировать файл accord.amz. Проделываем эту операцию на всех защищенных компьютерах, и дальше только остается активизировать систему защиты через ту же программу настройки комплекса. Обязательно нужен флаг "Автологин" в настройках. Пользователи теперь будут «включать» компьютер, т.е. проходить процедуру идентификации в АМДЗ с помощью идентификатора, а в момент загрузки ОС в процедуре WinLogOn поле «Имя» уже будет заполнено той информацией, которая была введена в пункте «Полное имя» (за это отвечает флаг «Использовать полное имя в учетных записях NT»). Пользователь может только ввести пароль, выбор локального входа ему тоже недоступен, т.к. в полном имени указан еще и домен. Смена паролей на домене выполняется администратором, или самим пользователем во время работы через Ctrl-Alt-Del и кнопку <Смена пароля>, если доменная политика это позволяет.

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» (11443195.4012-037 98).

Приложение 1.
Настройка Startup-пользователя

В ряде случаев для работы с терминальным сервером требуется наличие пользователя (Startup-пользователь), в обязанности которого входит процедура запуска терминального сервера.

В ПО ПАК «Аккорд-Win64» имеется возможность создания Startup-пользователя. При этом для Startup-пользователя рекомендуется выполнение следующих условий:

- учетная запись Startup-пользователя не должна существовать в ОС;
- Startup-пользователь выполняет процедуру идентификации в «Аккорд-АМДЗ»;
- во время выполнения процедуры идентификации в «Аккорд-АМДЗ» для Startup-пользователя не должны быть доступными функции администрирования «Аккорд-АМДЗ»;
- вход в ОС (локально или терминально) выполняется только по выполнении процедуры идентификации в «Аккорд-АМДЗ» и ввода пароля пользователя ОС.

Ниже приведен пример создания Startup-пользователя посредством ПАК «Аккорд-Win64».

1. если Startup-пользователь ранее был создан в ОС, то следует удалить его учетную запись из списка пользователей ОС;

далее следует запустить утилиту AcSetup.exe (Программы\ Аккорд.x64\ Настройка комплекса Аккорд), открыть вкладку Настройка комплекса Аккорд\ Параметры\ Дополнительные опции (рисунок 113):

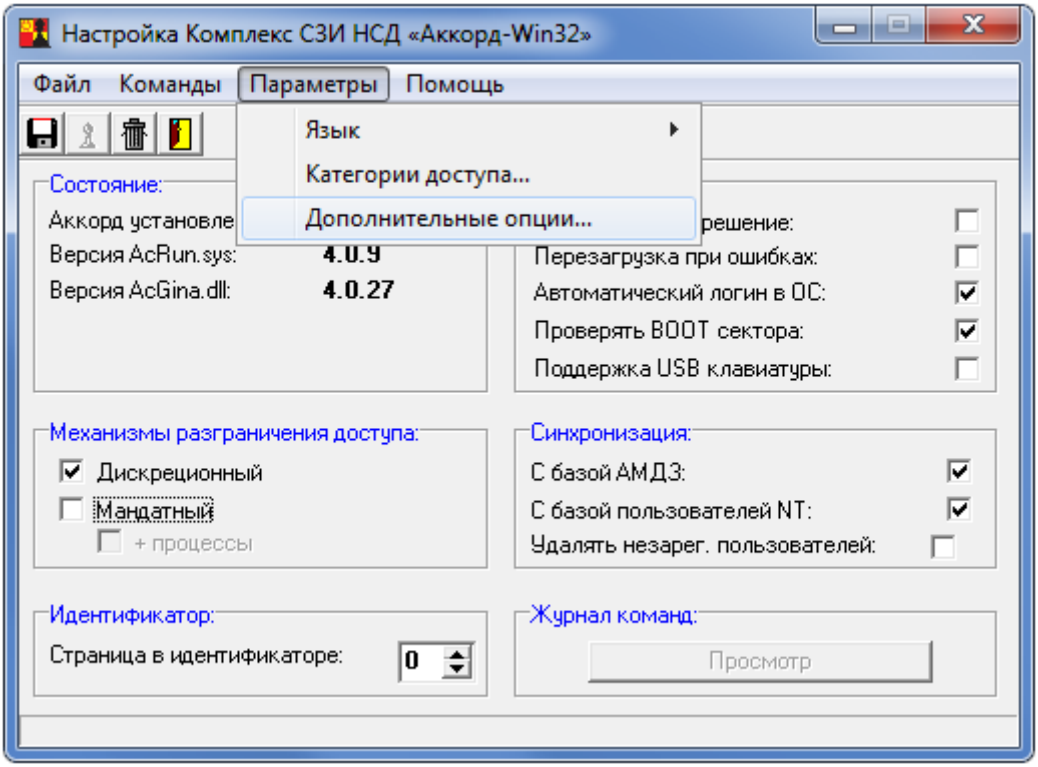

Рисунок 113 – Настройка комплекса Аккорд. Дополнительные опции

в появившемся на экране окне нужно открыть вкладку «Режим сессии» и если ранее флаг «Использовать полное имя в учетных записях Windows NT» не был установлен, то установить его (рисунок 114);

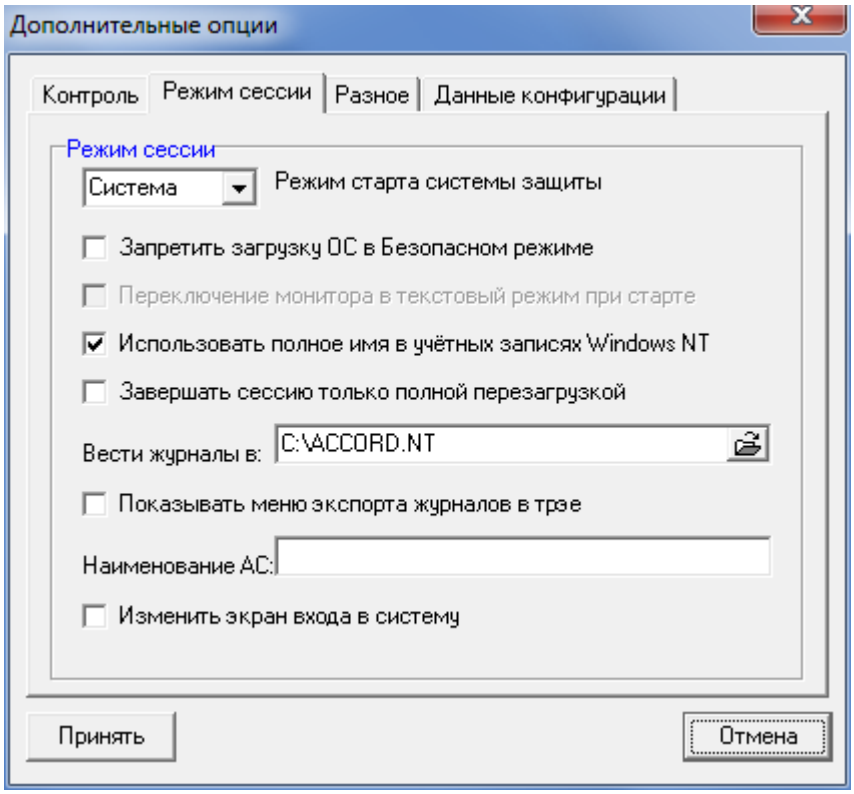

Рисунок 114 – Вкладка Настройка комплекса Аккорд\Дополнительные опции\Режим сессии

завершить работу приложения, сохранив выполненные изменения;

запустить утилиту Aced32.exe (Программы\Аккорд.x64\Редактор прав доступа), если учетная запись Startup-пользователя не была создана в базе ПАК «Аккорд», то нужно создать пользователя в группе «Обычные» (подробнее см. подраздел 5.1);

выделить в списке StartUp-пользователя (в рассматриваемом примере это пользователь USER, рисунок 115) и в поле «Полное имя» ввести любое имя **несуществующего** пользователя **несуществующего** домена. Например:

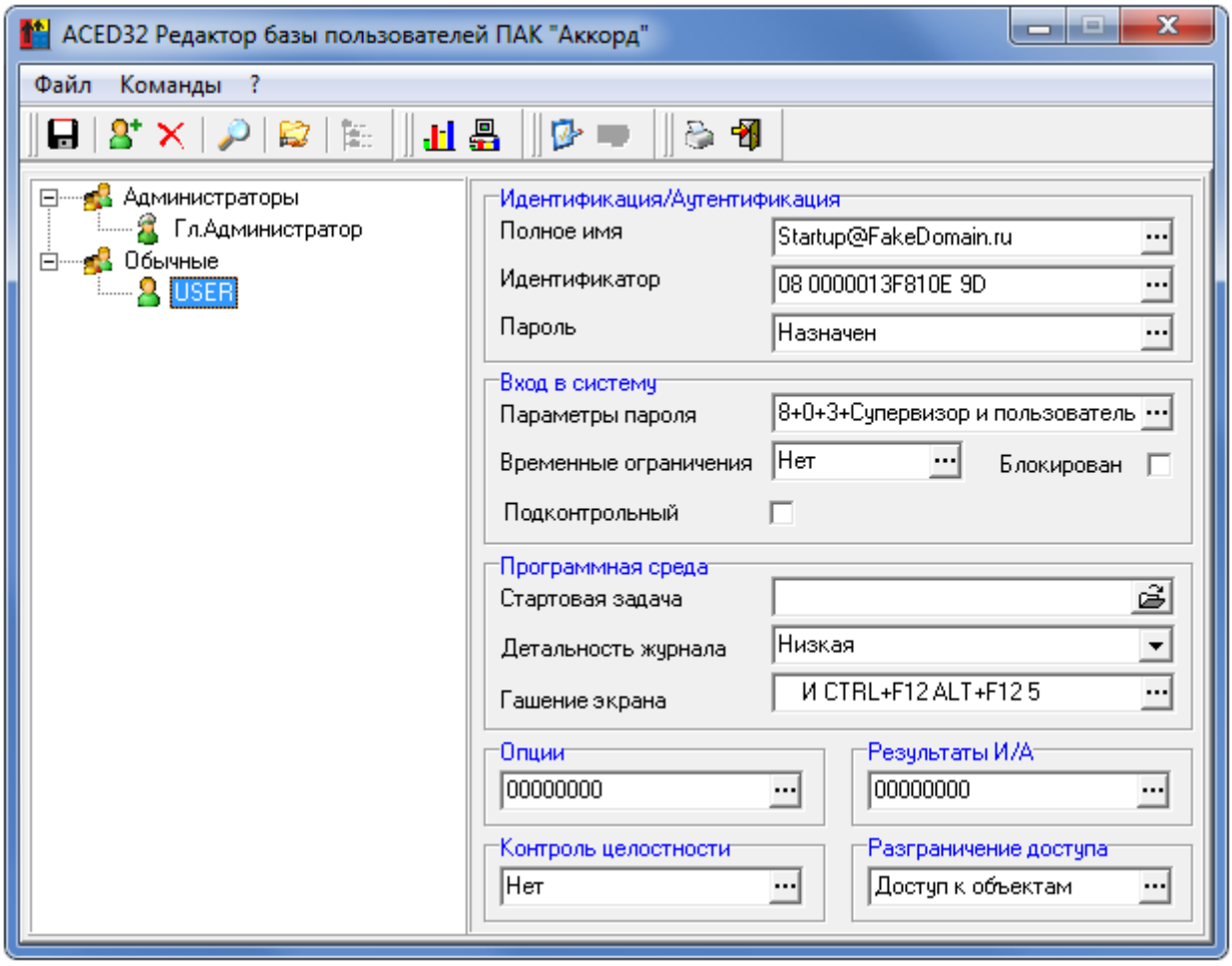

Рисунок 115 – Главное окно редактора прав доступа. Задание полного имени Startup-пользователя

далее, выбрав левой кнопкой мыши из списка учетную запись Startup-пользователя, перейти в меню разграничения доступа (рисунок 116);

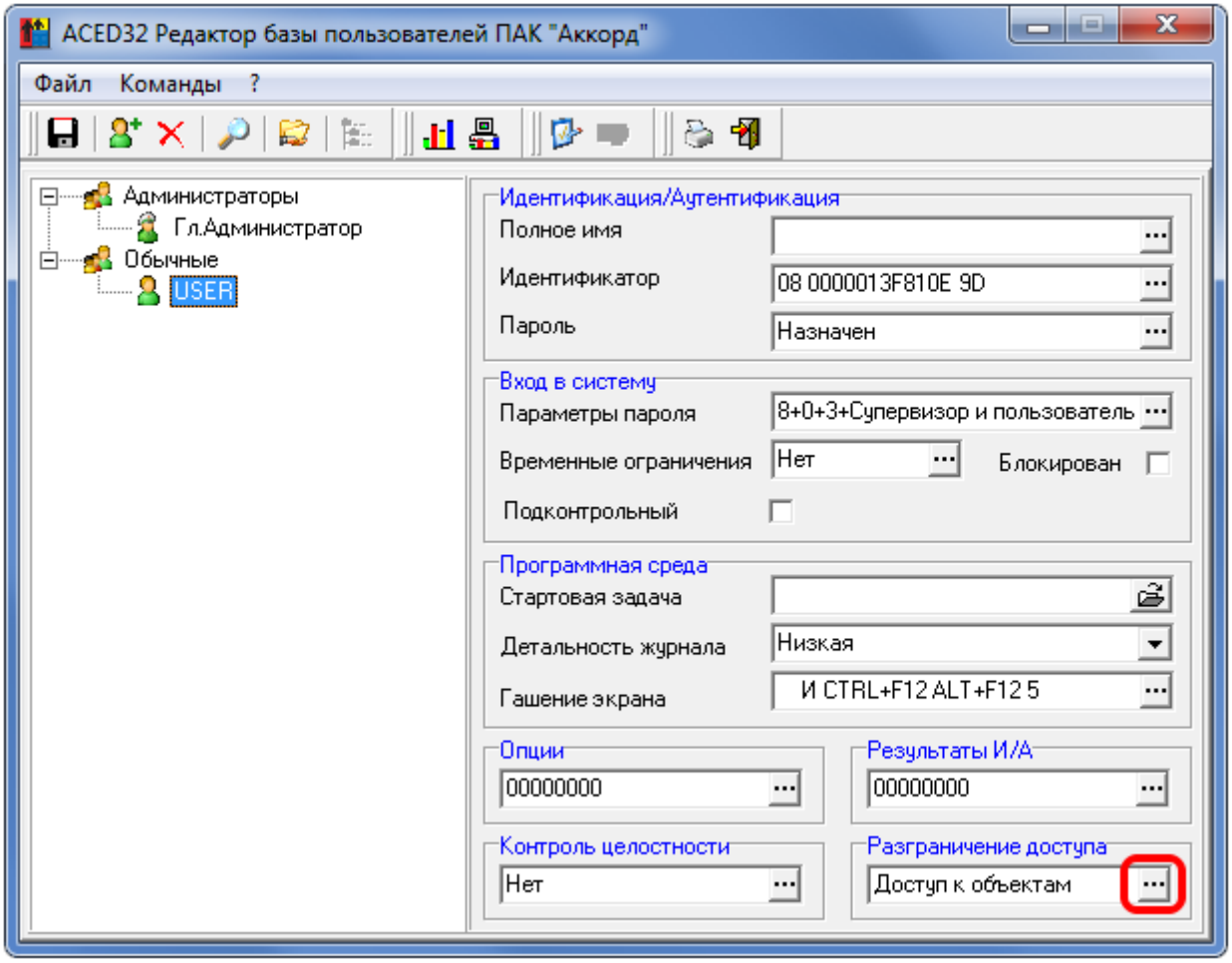

Рисунок 116 – Главное окно редактора прав доступа. Выбор меню разграничения доступа для Startup-пользователя

в меню разграничения доступа Startup-пользователя следует удалить список объектов, кроме трех пунктов, показанных на рисунке 117, затем нажать на кнопку <Новый> (рисунок 117);

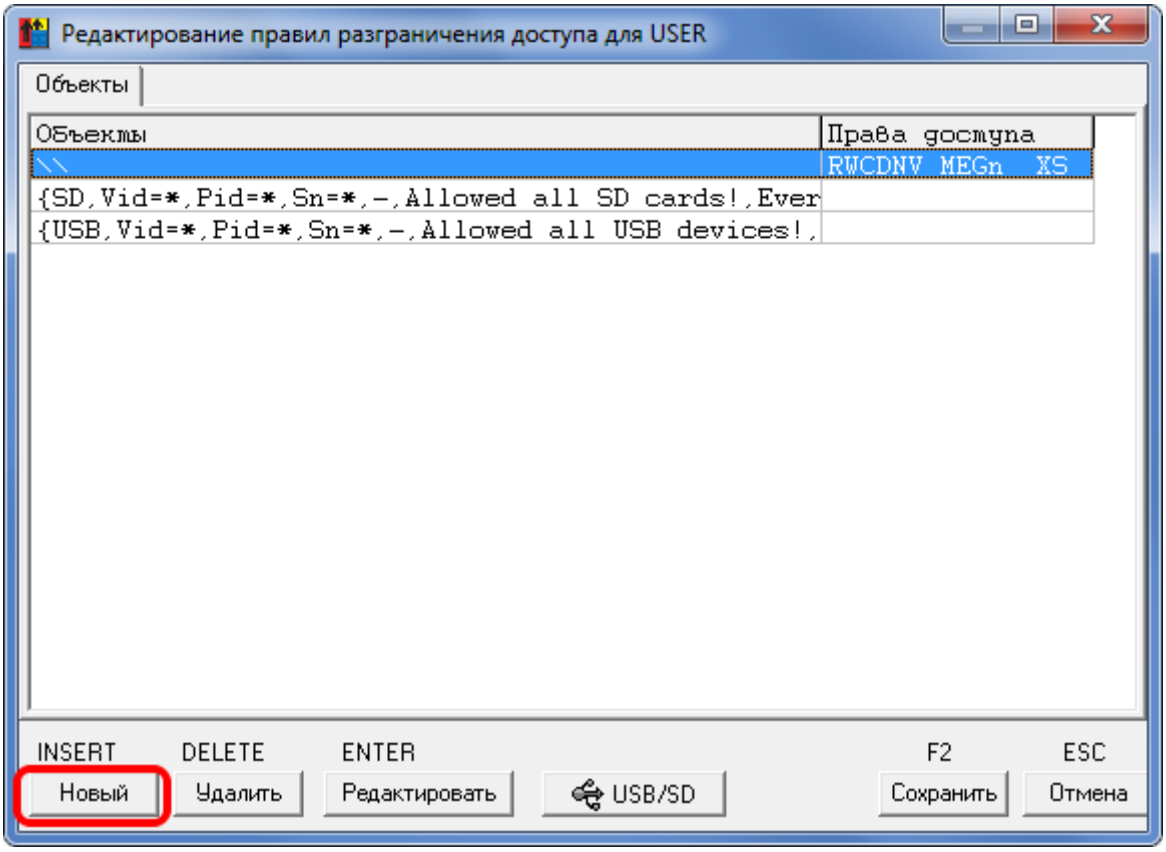

Рисунок 117 – Меню разграничения доступа Startup-пользователя

в появившемся на экране окне в поле «Имя объекта» необходимо ввести объект \DEVICE\ и предоставить объекту полный доступ (т.е. нажать кнопку <Полный> или выбрать комбинацию клавиш <Ctrl+F>, рисунок 118).

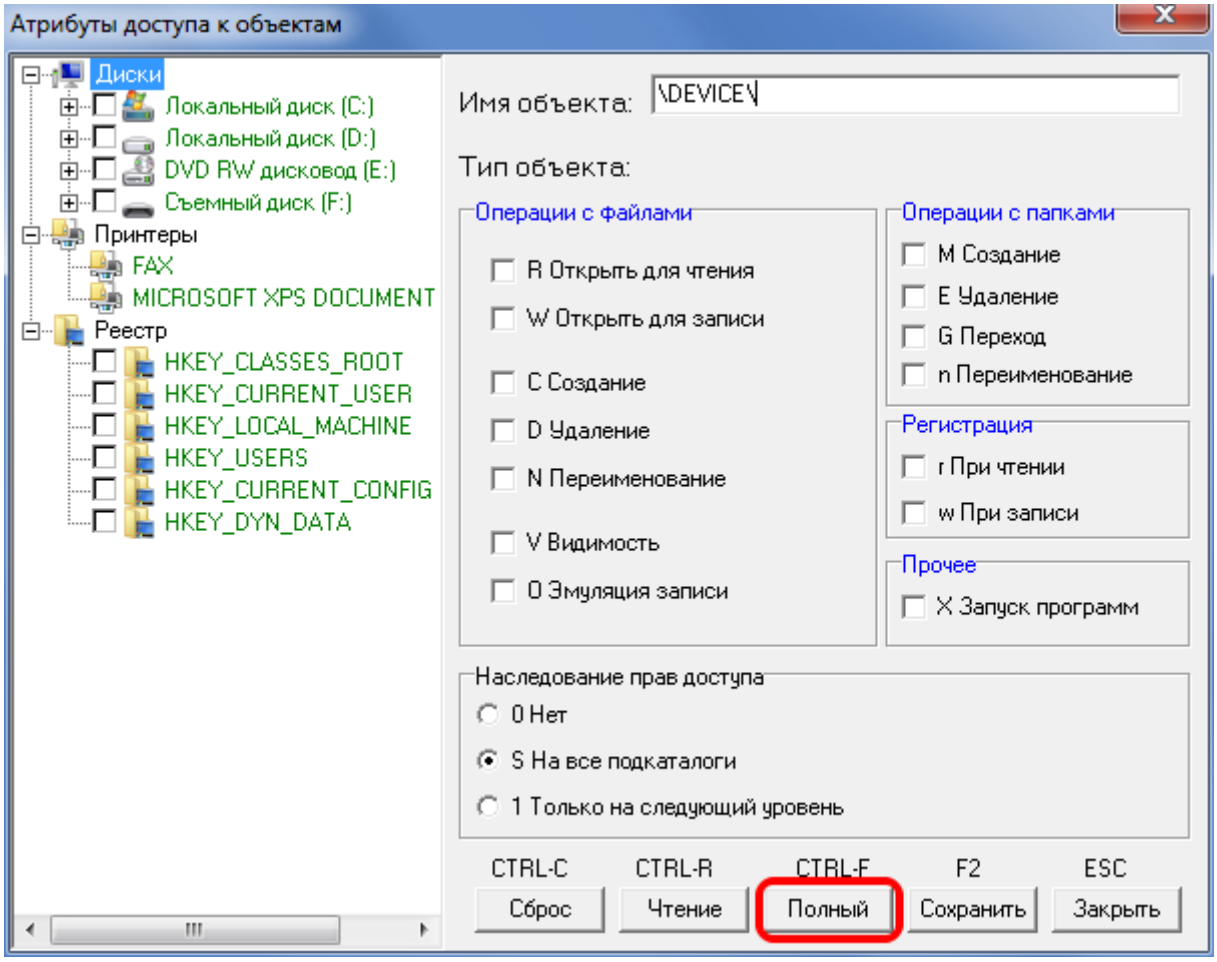

Рисунок 118 – Предоставление полного доступа объекту \DEVICE

далее следует сохранить выполненные изменения, нажав кнопку <Сохранить>, затем – кнопку <Закрыть> (рисунок 118);

по нажатии кнопки <Закрыть> на экране появляется сообщение (рисунок 119), в котором следует нажать кнопку <Нет>[1];

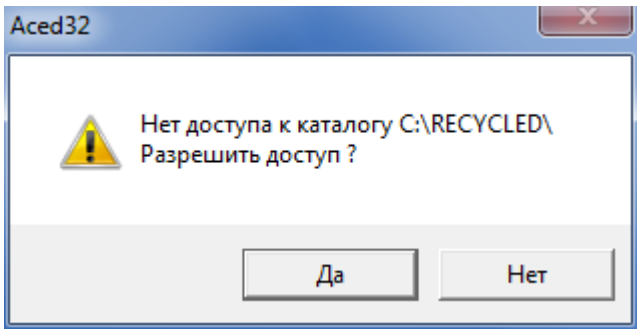

Рисунок 119 – Оповещение о необходимости назначения прав доступа для каталога \RECYCLED

[1] Назначение прав доступа каталогу \RECYCLED\ для Startup-пользователя (т.е. выбор кнопки <Да> в оповещении 119) не приведет к ошибке. Однако строгая необходимость в выполнении данной процедуры отсутствует, так как для объекта \DEVICE\ установлен полный доступ со стороны Startup-пользователя, что означает наличие полного доступа ко всей файловой системе

после выполнения действий 8)-11) список доступа для Startup-пользователя приобретает следующий вид[1] (рисунок 120):

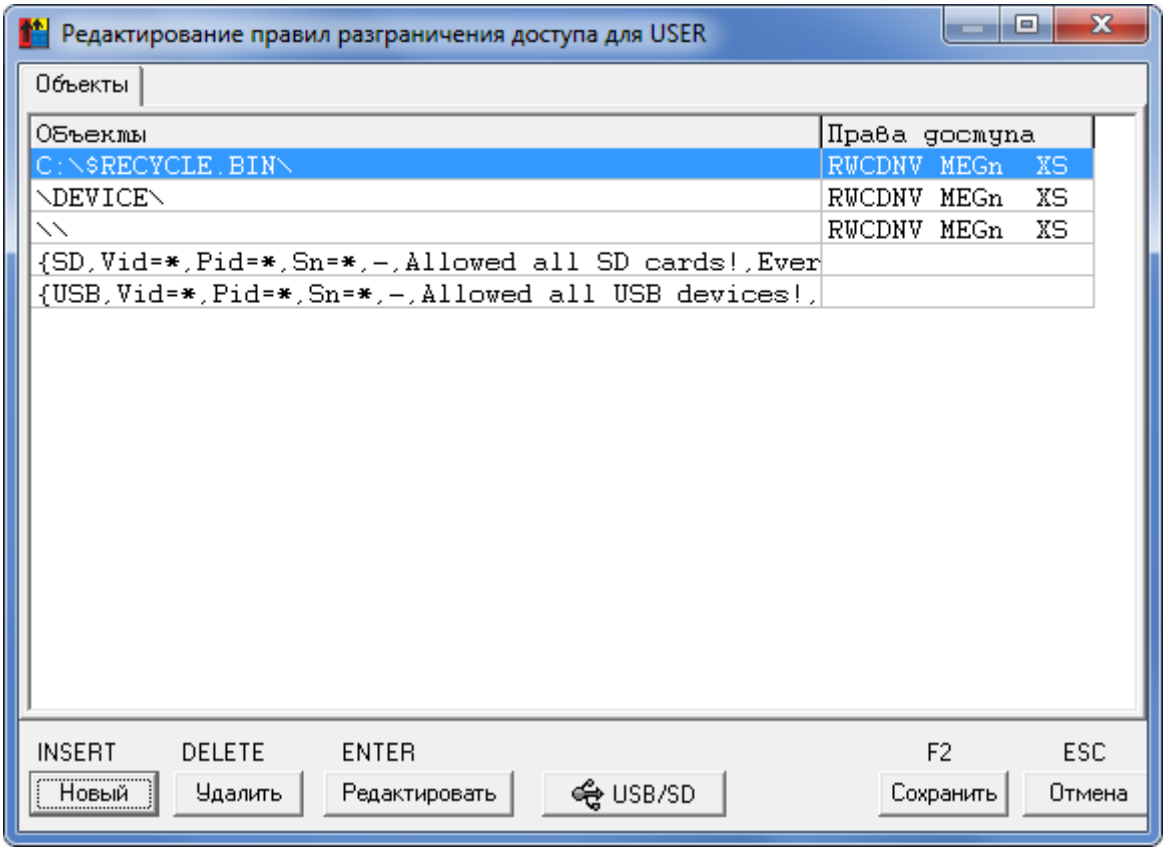

Рисунок 120 – Список доступа Startup-пользователя

далее рекомендуется выполнить следующие действия:

- выбрать левой кнопкой мыши из списка учетную запись Startup-пользователя, нажать на раскрывающийся список в поле «Параметры пароля» (рисунок 121);

[1] В зависимости от выполненных действий в п. 11) объект C:\RECYCLED\ может присутствовать или отсутствовать в списке доступа Startup-пользователя

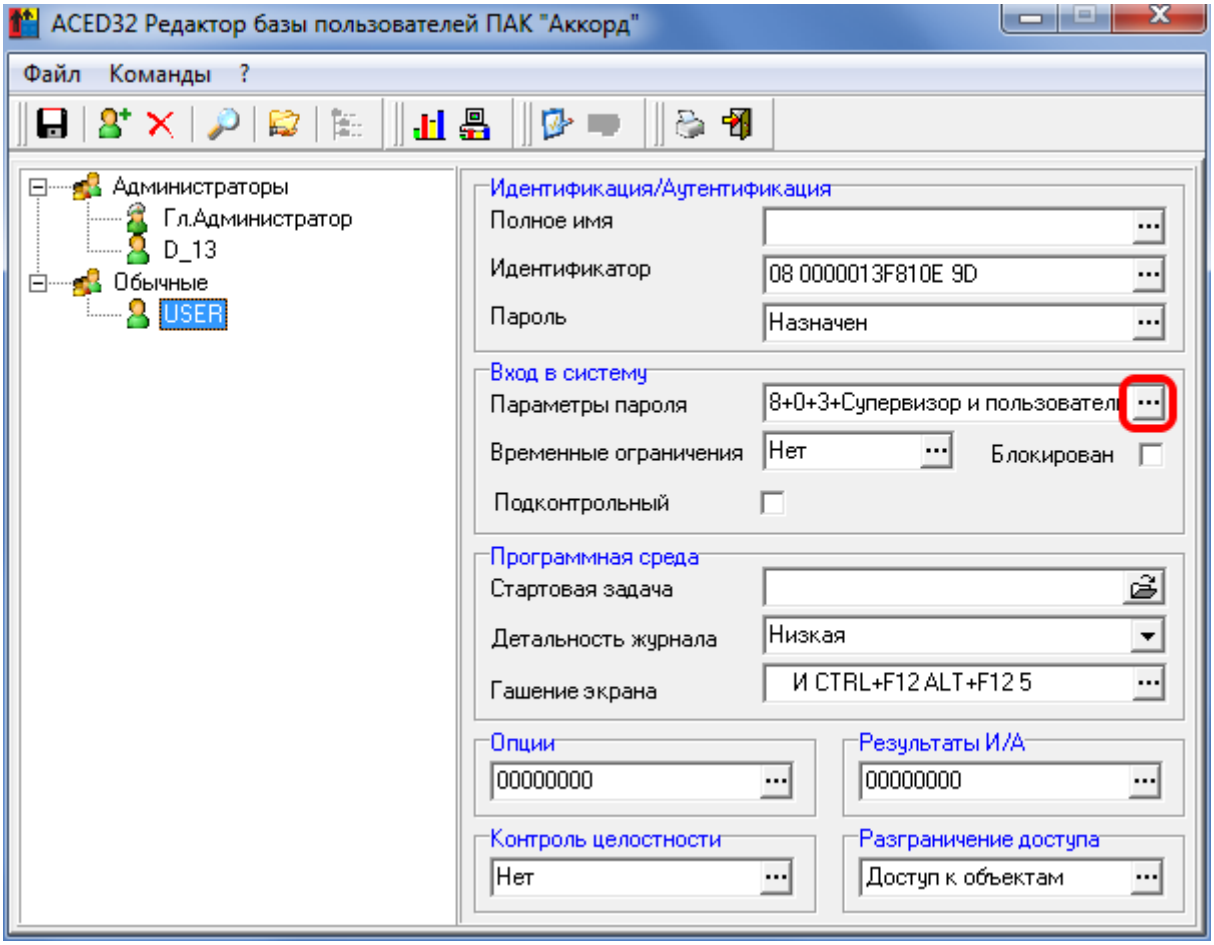

Рисунок 121 - Главное окно редактора прав доступа. Выбор меню «Параметры пароля»

- в случае необходимости (или в соответствии с политикой безопасности, принятой в организации) следует в поле «Кто может менять пароль» установить значение «Только супервизор»;
- при отсутствии необходимости в использовании флага «Не менять пароль в АМДЗ» (например, в соответствии с политикой безопасности, принятой в организации) следует снять данный флаг (рисунок 122);

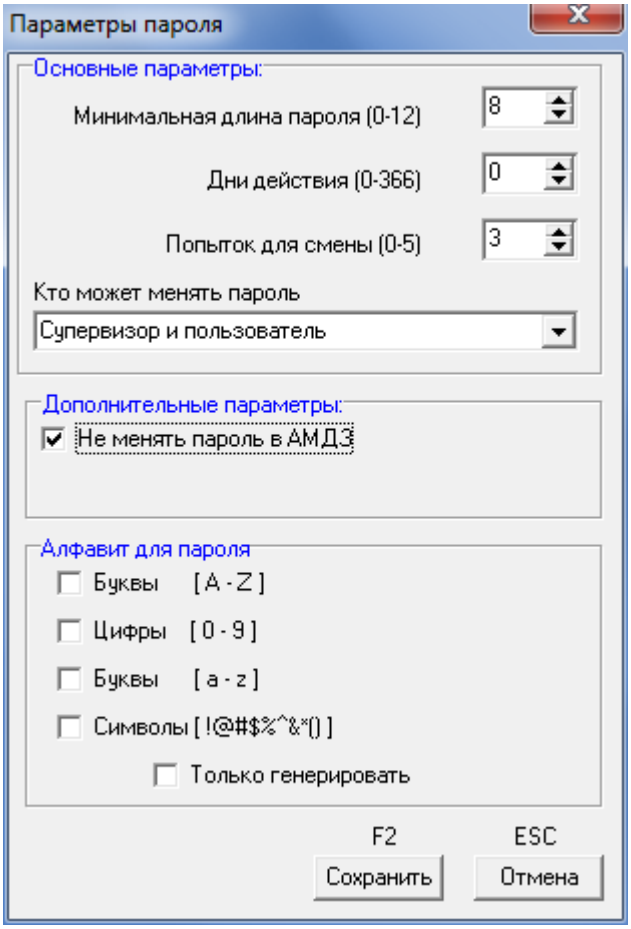

Рисунок 122 – Параметры пароля

для остальных пользователей системы поле «Полное имя» можно не заполнять[1];

после выполненных действий следует завершить работу приложения «Редактор прав доступа» с сохранением изменений;

далее необходимо выполнить процедуру перезагрузки СВТ.

Итог: после выполнения действий, описанных в Приложении 1, в базе ПАК «Аккорд» создается Startup-пользователь (в описанном выше примере – пользователь USER группы «Обычные»).

Startup-пользователь выполняет процедуру запуска терминального сервера, ему назначен идентификатор и «пустой» пароль в «Аккорд-АМДЗ». Во время выполнения процедуры идентификации «Аккорд-АМДЗ» функции администрирования ему не доступны.

Учетная запись Startup-пользователя отсутствует в ОС, следовательно, несанкционированный вход (например, от имени другого пользователя ОС) под его учетной записью в ОС осуществить невозможно.

Startup-пользователю предоставлен полный доступ к файловой системе. Таким образом, во время выполнения процедуры запуска терминального

[1)] Заполнять поле «Полное имя» для пользователей необходимо в случае, когда имя пользователя в ОС отличается от имени пользователя в базе «Аккорд»

сервера для Startup-пользователя загружаются необходимые приложения и драйверы ОС с необходимыми для выполнения его должностных обязанностей правами доступа к объектам. Если в процессе работы терминального сервера происходит запуск новых приложений ОС, то им также предоставляется полный доступ ко всем объектам, необходимым для выполнения должностных обязанностей Startup-пользователя.

Все администраторы системы имеют возможность посредством терминального соединения подключаться к серверу и запускать все утилиты, находящиеся в каталоге C:\Accord.x64\.

Приложение 2. Файл ACCORD.INI – файл конфигурации СЗИ НСД «Аккорд»

Описание параметров, задаваемых в файле accord.ini, которые могут быть изменены администратором СЗИ 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 пользователя. 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 комплексом 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 аттрибута 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, через который принудительно перегружается компьютер, если сеанс не удалось завершить корректно (с закрытием всех приложений). Задается в минутах.

DisableSessionLogOff – принудительная перезагрузка по завершению 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 - 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 ПО ПАК «Аккорд». Если параметру присвоено значение «1», значит на СВТ установлено ПО ПАК «Аккорд-Win64».

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

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

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

UseVirtualDisk - параметр определяет режим работы специального ПО ПАК «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

UseAmdzBase – использование базы пользователей АМДЗ в программе ACED32. Значения: «Yes» – АМДЗ используется. «No» – АМДЗ не используется.

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.

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. При этом 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, не доступных 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.

[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 аппаратной части СЗИ (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 комплекса. 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	Проведена доработка документации в связи с выходом версии x.0.10.53.		
2			
3			
4			
5			
6			