ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.4012-036 97-ЛУ

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

# Редактор прав пользователей виртуальной инфраструктуры

# Программа AcedVI

**11443195.4012-036 97**

**Версия 1.0.6**

Москва

2024

# АННОТАЦИЯ

Программа AcedVI – редактор параметров (атрибутов) доступа пользователей к объектам виртуальной инфраструктуры - предназначена для описания (установки) правил разграничения доступа (ПРД) пользователей в соответствии с их полномочиями.

Программа используется администратором БИ комплекса СЗИ НСД «Аккорд-Win32» v.4.0 (далее - комплекс «Аккорд», комплекс) 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, наделенных правами администратора) и содержит описание программы AcedVI 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

# 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 AcedVI – редактор параметров (атрибутов) доступа пользователей при использовании дискреционного и мандатного[1] механизмов к объектам виртуальной инфраструктуры – предназначена для администрирования подсистемы разграничения доступа комплекса «Аккорд».

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

Программа AcedVI входит в состав специального ПО комплекса и инсталлируется на жесткий диск СВТ (РС) при установке комплекса.

---

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

# 2. Запуск редактора прав доступа

## 2.1. Порядок запуска программы AcedVI

Старт редактора параметров (атрибутов) доступа пользователей комплекса начинается с запуска файла C:\ACCORD.X32\AcedVI.exe (Пуск -> Все программы -> Аккорд-Win32 -> Редактор прав доступа). Невозможен одновременный запуск AcedVI с программами Aced32, AcSetup или запуск нескольких копий AcedVI. При обнаружении уже запущенных программ появится соответствующее предупреждение.

При запуске AcedVI проверяется наличие файла базы данных (БД) пользователей редактора прав доступа (Accord.amz). При его отсутствии появляется окно с соответствующим сообщением и предложением создать новый файл БД (рисунок 1).

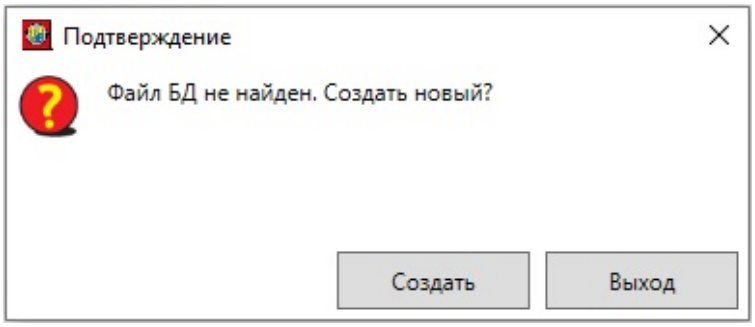



**Рисунок 1 – Сообщение при отсутствии файла БД при старте программы AcedVI**

По кнопке <Выход> можно прервать запуск программы. При нажатии <Создать> появляется главное окно программы (рисунок 2).

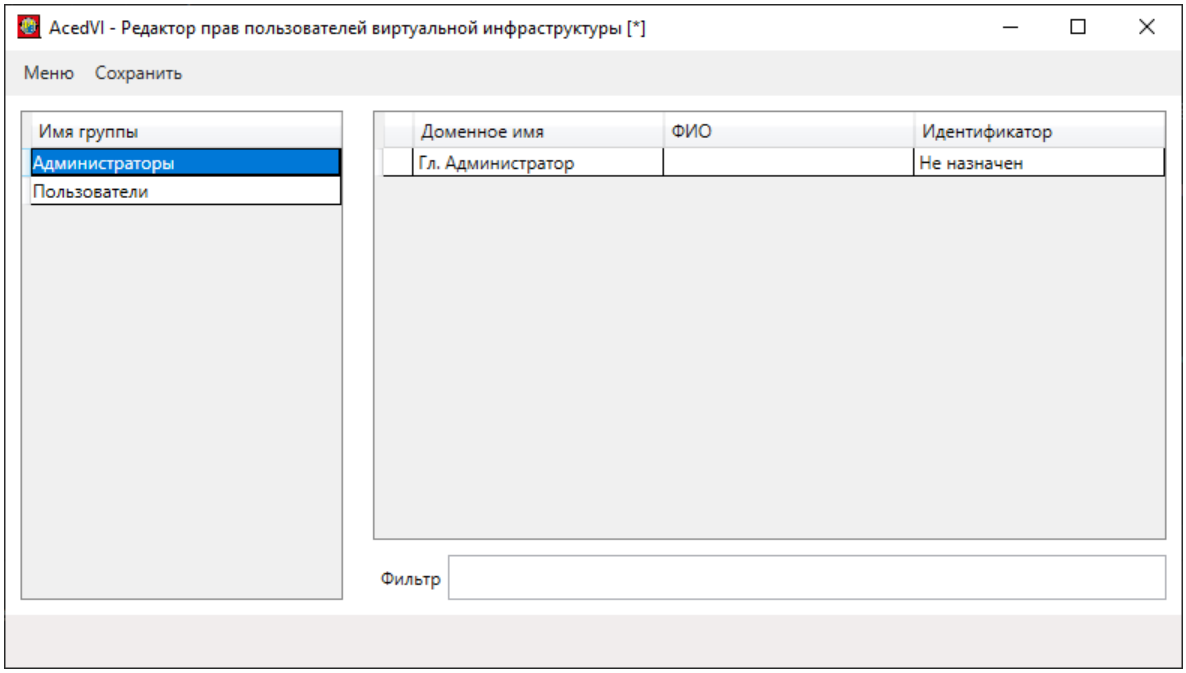



**Рисунок 2 – Главное окно программы AcedVI при создании новой БД**

В этом окне есть две группы – «Администраторы» и «Пользователи» - а в группе «Администраторы» создан пользователь «Гл.Администратор».

Следует учитывать, что файлы БД при этом еще не сформированы. Основной (Accord.amz) и вспомогательный (Accord.db) файлы БД будут созданы только при первом сохранении любых изменений.

Если программа AcedVI при запуске обнаружит файл БД, появляется окно идентификации пользователя (рисунок 3).

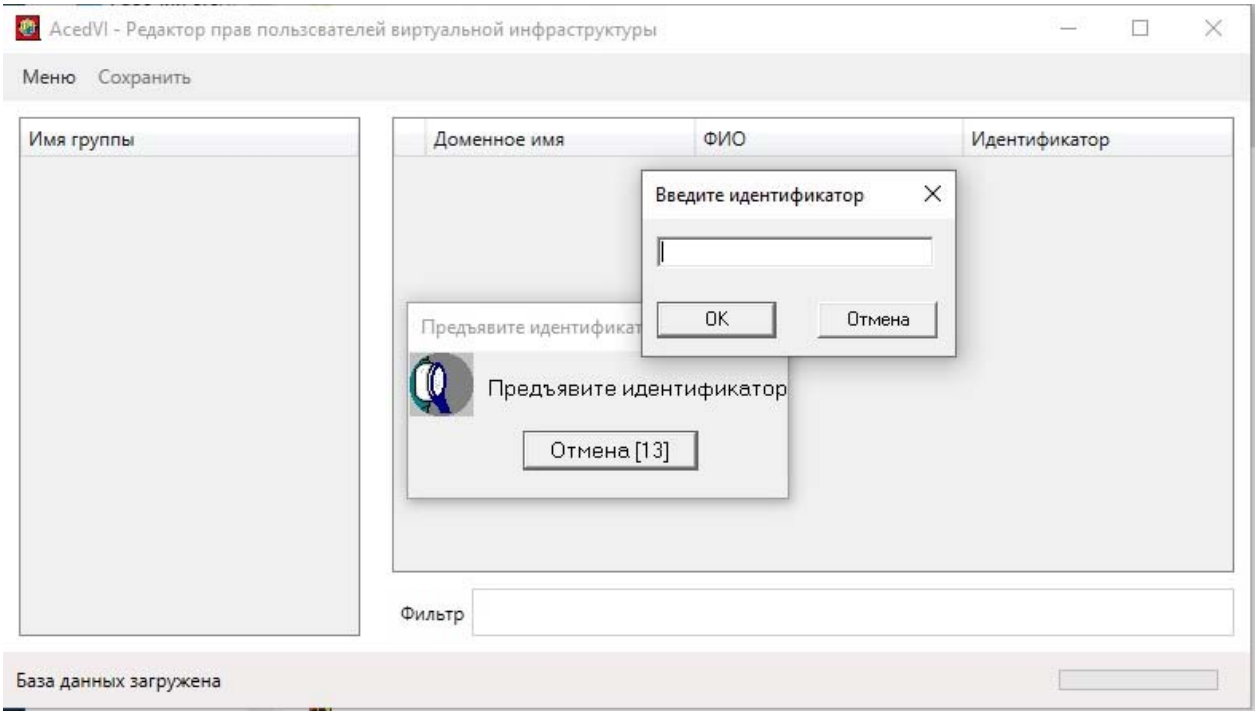



**Рисунок 3 – Запрос идентификатора пользователя при наличии файла БД**

Далее запрашивается пароль пользователя (рисунок 4).

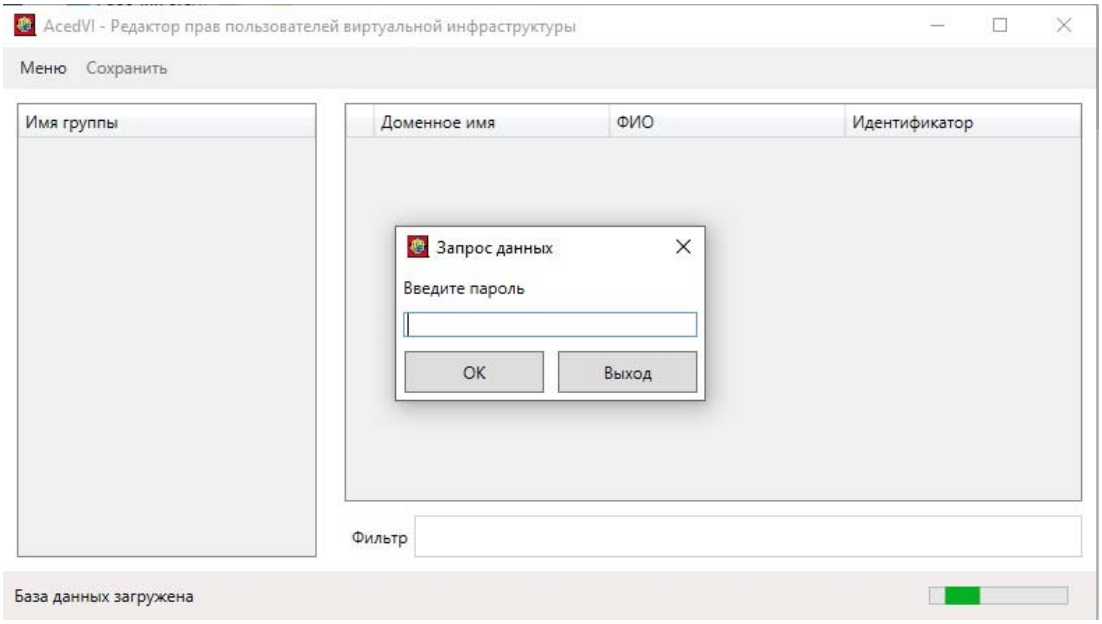



**Рисунок 4 - Запрос пароля пользователя**

По кнопке <Выход> в этом окне можно прервать дальнейший запуск программы.

Если данные идентификации/аутентификации введены неправильно, то будет показано сообщение «Пользователь не найден» (поиск осуществляется по идентификатору во всех группах) или «Некорректные данные» (неправильный пароль пользователя, предъявившего корректный идентификатор).

После закрытия информационного окна вновь появится окно с запросом идентификатора (рисунок 3) и далее – пароля (рисунок 4).

Обратите внимание, что перед появлением окна запроса идентификатора происходит проверка параметра NtAccessStyle в файле настроек Accord.ini, и если его значение не выставлено в «Yes», то появится дополнительное окно о запросе смены значения этого параметра (рисунок 5).

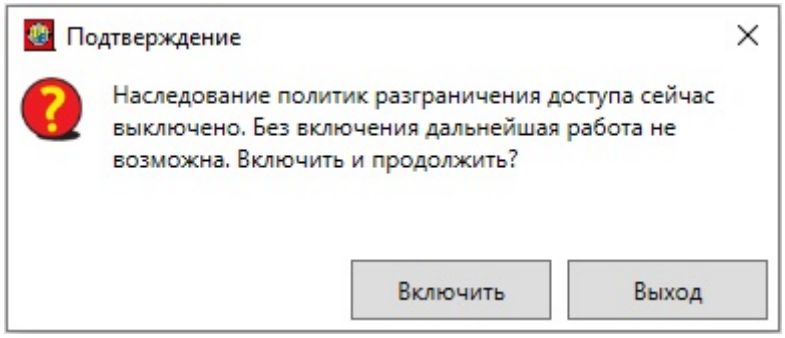



**Рисунок 5 – Окно запроса установки параметра NtAccessStyle**

При подтверждении (кнопкой <Включить>) в этом окне программа изменяет значение параметра в настройках Accord.ini, после чего запрашивает идентификатор пользователя (рисунок 3). Можно отказаться от изменения настроек и нажать кнопку <Выход>, при этом запуск программы будет прерван.

Если процедура идентификации/аутентификации прошла успешно, и пользователь, который предъявил идентификатор и ввел правильный пароль, входит в группу «Администраторы», появляется главное окно программы, в заголовке которого будет отображено, каким именно пользователем произведен вход (рисунок 8).

Пользователю, не входящему в группу «Администраторы», будет отказано в запуске программы с сообщением «Редактор может использовать только Администратор».

Пользователю группы «Администраторы», не являющемуся Администратором ОС Windows, при условии выставления флага «Контроль процессов» в программе настройки комплекса «Аккорд» будет выдано сообщение о подтверждении запуска программы от имени Администратора Windows (рисунок 6). При согласии на перезапуск (кнопка <ОК>) появится окно для ввода имени и пароля Администратора Windows. При нажатии кнопки <Отменить> программа запустится, но при этом ее функции будут ограничены – станет недоступной настройка мандатных меток.

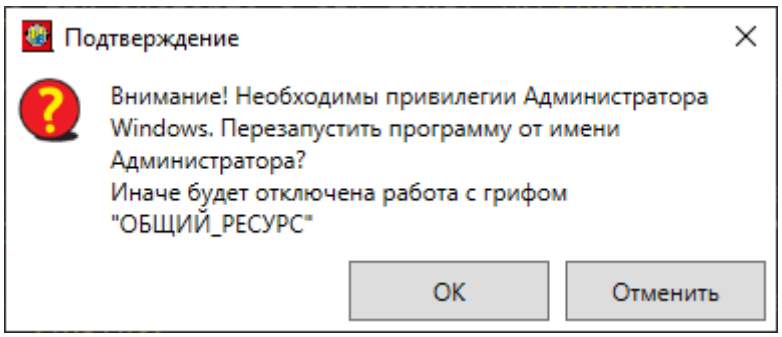



**Рисунок 6 – Подтверждение перезапуска программы от имени Администратора ОС Windows**

Если открываемая база с момента последнего сохранения претерпела изменения, связанные с настройками конфигурационного файла (параметр LowerCasedFullNames) или удалением списков ПРД пользователей, будет выдано предупреждение об этом (рисунок 7). Текст этого сообщения записывается в журнал регистрации. После нажатия кнопки <OK> база отобразится в измененном виде, требующем сохранения (станет активной команда «Сохранить» в верхней панели окна).

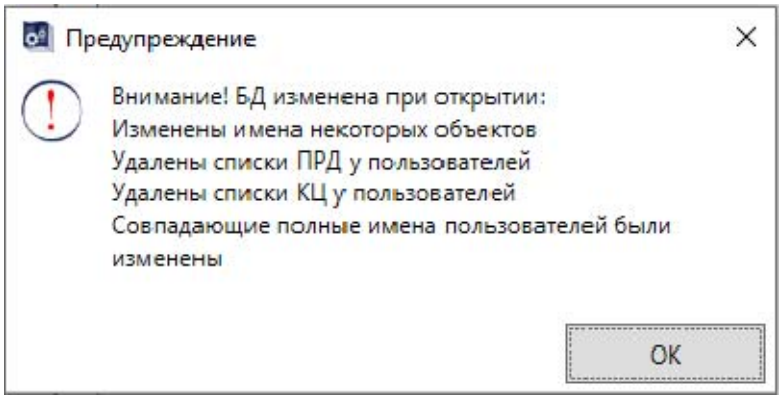



**Рисунок 7 – Предупреждение об изменениях в открываемой БД**

Особенности отображения БД подробно описаны в п. 3.5 настоящего документа.

На рисунке 8 представлено главное окно программы при введении корректных данных.

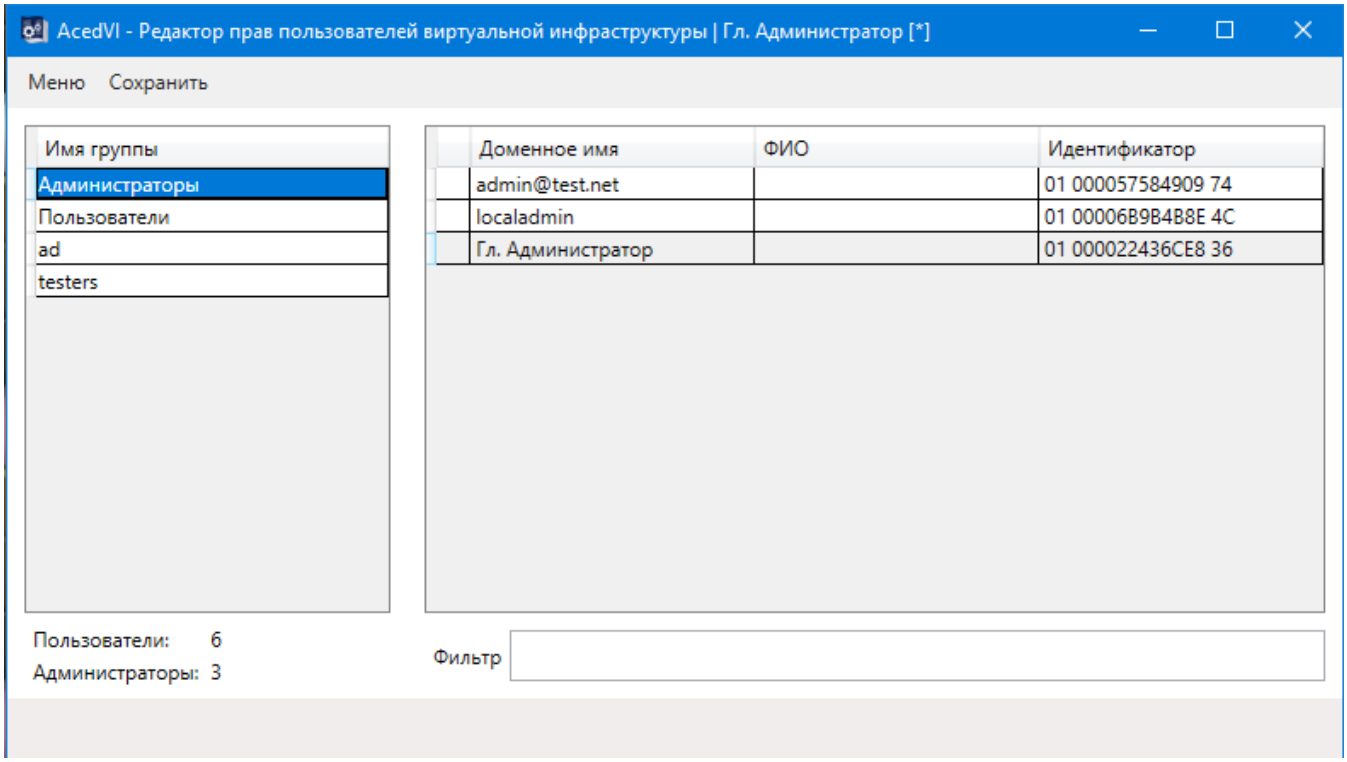



**Рисунок 8 – Главное окно программы при введении корректных данных при входе**

В заголовке главного окна программы по мере добавления новых данных появляется указатель [*] (рисунок 9) о том, что в данных появились изменения, и требуется сохранение БД.

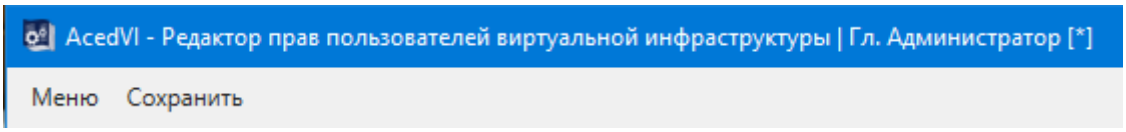



**Рисунок 9 – Указатель [*] в заголовке программы**

Главное окно программы состоит из следующих разделов:

- Контекстное меню в верхней части окна (рисунок 10), содержащее кнопки поиска пользователя по идентификатору и по имени (во всех группах), операций с мандатными метками (рисунок 11, рисунок 12), редактирования имен сетевых ресурсов, дополнительную кнопку выхода и кнопку сохранения БД (недоступна при отсутствии изменений);

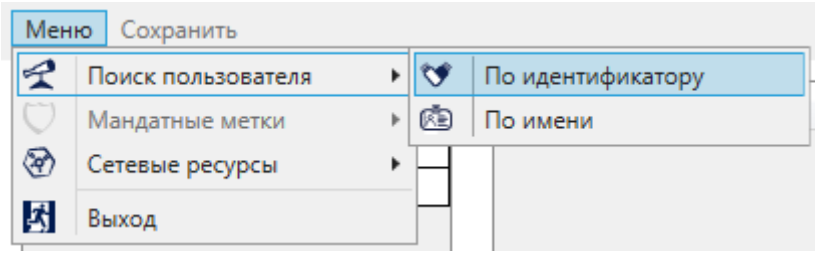



**Рисунок 10 – Контекстное меню главного окна программы. Поиск пользователя**

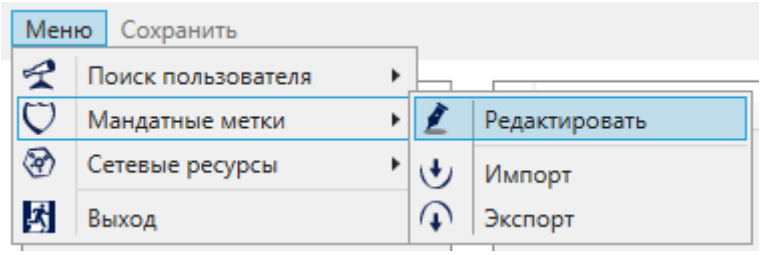



**Рисунок 11 - Контекстное меню главного окна программы. Мандатные метки**

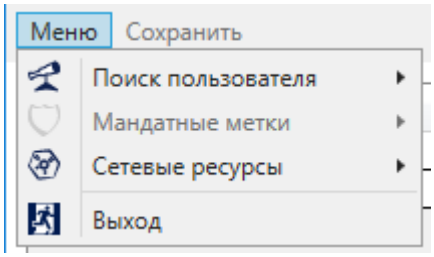



**Рисунок 12 – Мандатные метки недоступны при отключении мандатных политик в программе настройки комплекса «Аккорд» AcSetup или при входе пользователя с привилегией «Оператор пользовательских УЗ»**

- Таблица со списком групп в левой части окна. Изначально список групп отсортирован по дате добавления/создания группы. Если нажать на заголовок столбца «Имя группы», порядок сортировки изменится – группы будут отображаться по имени, и возврат к сортировке по времени создания станет невозможным. Кнопкой мыши в поле таблицы групп вызывается контекстное меню (рисунок 13), содержащее следующие команды:
  - Редактировать - открывает окно редактирования настроек группы (также может быть открыто двойным кликом мыши по строчке с именем группы);
  - Импортировать настройки из *.prd – позволяет импортировать правила разграничения доступа из файла *.prd в выделенную группу (подробнее в п.3.18.2);
  - Экспортировать настройки в *.prd – позволяет экспортировать правила разграничения доступа выделенной группы в файл *.prd (подробнее в п.3.18.2);
  - Добавить пользователя - после ввода имени нового пользователя (в дополнительном окне) в выбранную группу добавляется новый пользователь с указанным именем;
  - Импортировать пользователей из AD - открывает окно импорта пользователей из AD, в котором можно выбрать пользователей для добавления в указанную группу (подробнее в п.3.4);
  - Импортировать пользователей из *.amz - открывает окно импорта пользователей из базы пользователей комплекса «Аккорд» (accord.amz), в котором можно выбрать пользователей для добавления в указанную группу (подробнее в п.3.5);

- Импортировать пользователей из *.atf – позволяет импортировать информацию о пользователях группы из файла *.atf в выделенную группу (подробнее в п.3.6);
- Добавить группу - создает новую группу после ввода ее имени в дополнительном малом окне;
- Удалить группу – удаляет группу (возможно только для пустой группы);

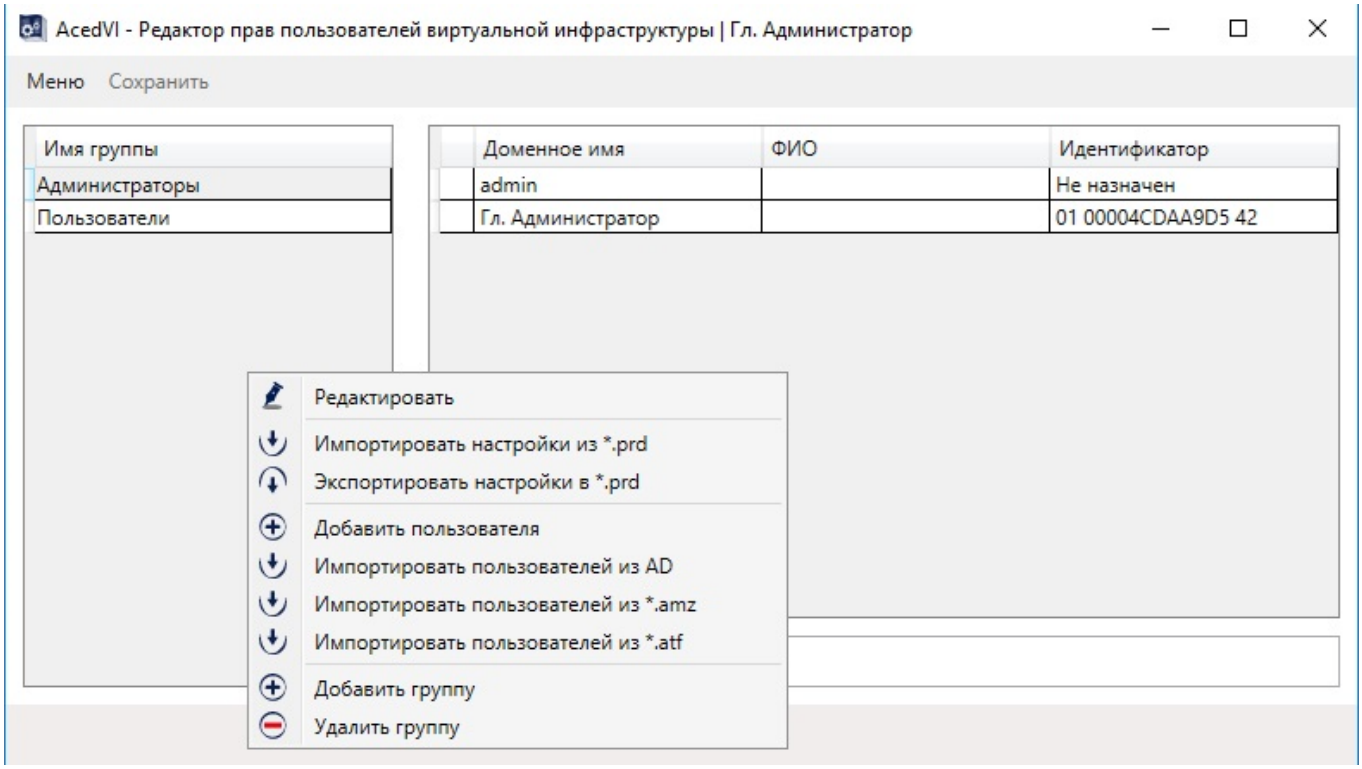



**Рисунок 13 – Контекстное меню таблицы со списком групп главного окна программы**

- Таблица со списком пользователей в правой части окна. Состоит из следующих столбцов: столбец, в котором звездочкой отмечается пользователь, добавленный в избранное (избранные пользователи всегда располагаются в верхней части списка); доменное имя пользователя; ФИО пользователя; назначенный идентификатор. Контекстное меню, вызываемое в этой таблице (рисунок 15), содержит команды:
  - Редактировать - открывает окно редактирования настроек пользователя (также может быть открыто двойным кликом мыши по строчке с именем пользователя);
  - Добавить в избранное;
  - Убрать из избранного;
  - Переместить в - позволяет переместить пользователя в другую группу. Есть возможность выбрать сразу несколько строк с пользователями (Ctrl+A или сочетания Ctrl и Shift с мышью);
  - Синхронизировать – при переносе отдельного пользователя (или нескольких, отмеченных с помощью клавиши <Ctrl>) в

другую группу можно изменить синхронизацию с настройками этой группы по некоторым параметрам. После выбора команды появляется окно синхронизации (рисунок 14), в котором галочками отмечены настройки, синхронизируемые для пользователя при изменении параметров группы.

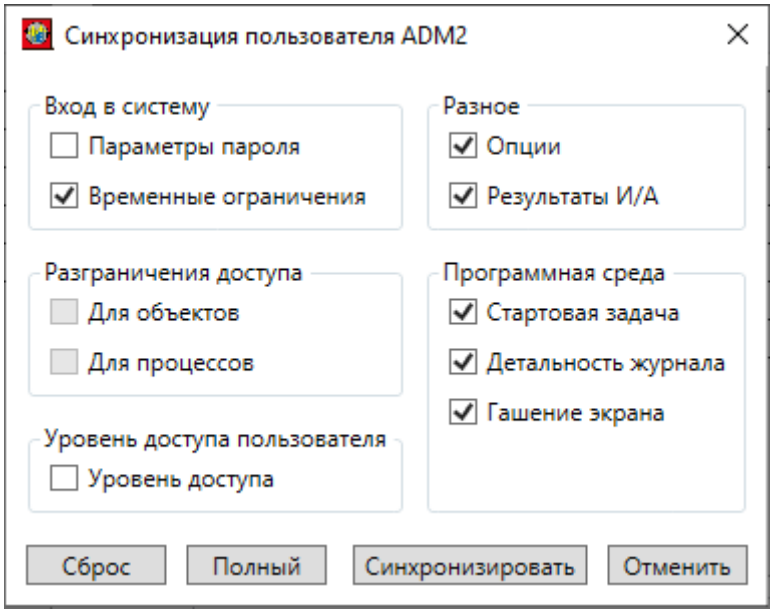



**Рисунок 14 – Окно синхронизации пользователя с параметрами группы**

Если в каком-то поле убрать галочку, можно зафиксировать данную настройку для пользователя в текущем ее состоянии, и при изменении этого параметра в новой группе настройка не будет синхронизироваться для указанного пользователя;

- Импортировать настройки из *.prd – позволяет импортировать правила разграничения доступа из файла *.prd выделенным пользователям (подробнее в п.3.18.2);
- Экспортировать настройки в *.prd – позволяет экспортировать правила разграничения доступа выделенных пользователей в файл *.prd (подробнее в п.3.18.2);
- Добавить пользователя - добавляет нового пользователя после ввода его имени в дополнительном малом окне;
- Удалить пользователей - есть возможность выделить несколько строк пользователей или удалить сразу всех (этим способом можно удалить группу с пользователями – сначала удалить всех пользователей в ней, а потом саму группу);
- Импортировать пользователей из AD - открывает окно импорта пользователей из AD, в котором можно выбрать пользователей для добавления в выбранную группу (подробнее в п.3.4);
- Импортировать пользователей из *.amz - открывает окно импорта пользователей из базы пользователей комплекса «Аккорд» (accord.amz), в котором можно выбрать

пользователей для добавления в выбранную группу (подробнее в п.3.6);

- Импортировать пользователей из *.atf – позволяет импортировать информацию о выделенных пользователях из файла *.atf в выбранную группу (подробнее в п.3.7);
- Экспортировать пользователей в *.atf – позволяет экспортировать информацию о выделенных пользователях в файл *.atf;

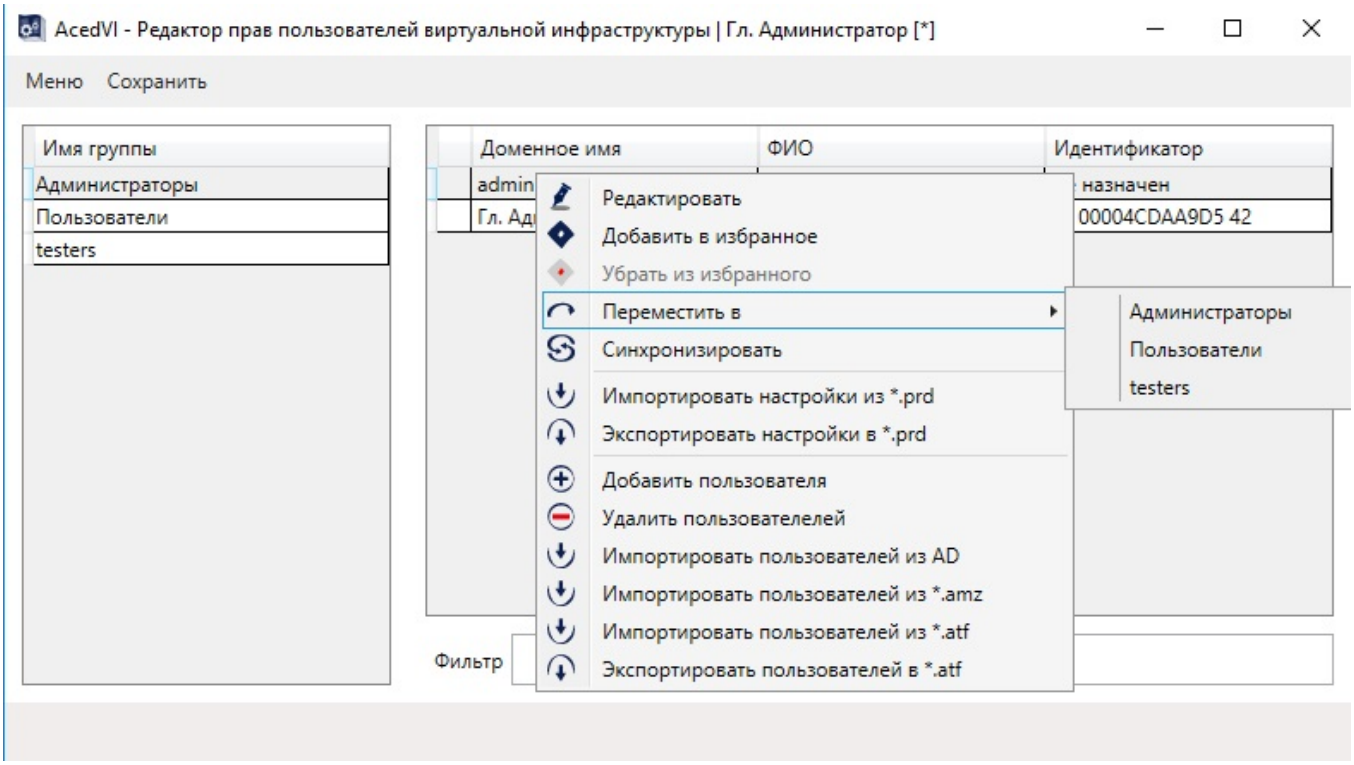



**Рисунок 15 - Контекстное меню таблицы со списком пользователей главного окна программы**

- Строка ввода текста для поиска пользователей в выбранной группе (Фильтр) – ищет в выделенной группе пользователей, имя или ФИО которых содержит введенный в строке текст (не зависит от регистра), при этом меняет список отображаемых пользователей в соответствии с результатом поиска (обновление списка происходит при нажатии клавиши <Enter>). При выборе другой группы фильтр сбрасывается, и при следующей необходимости требуется его повторный ввод;
- Строка статуса в нижней части окна, в которой отображаются текстовые сообщения (в том числе об ошибках) или показывается ход выполнения длительной операции (например, загрузка БД на рисунке 4).

## 2.2. Сохранение выполненных настроек и выход из программы

Кнопка <Сохранить> в главном окне программы (рисунок 2) становится активной, только если были произведены какие-либо изменения в этом окне или была загружена измененная ранее БД. Если при активной кнопке и указателе [*] в заголовке окна (рисунок 9) попытаться выйти из программы, нажав кнопку <Выход> или закрыв главное окно, появится запрос подтверждения выхода без сохранения БД (рисунок 16). Если в этом окне подтвердить выход, то будет осуществлен выход из программы, при этом все изменения не будут применены в файле БД (Accord.amz). При нажатии в окне запроса кнопки <Отменить> окно закроется, и появится возможность сохранения изменений.

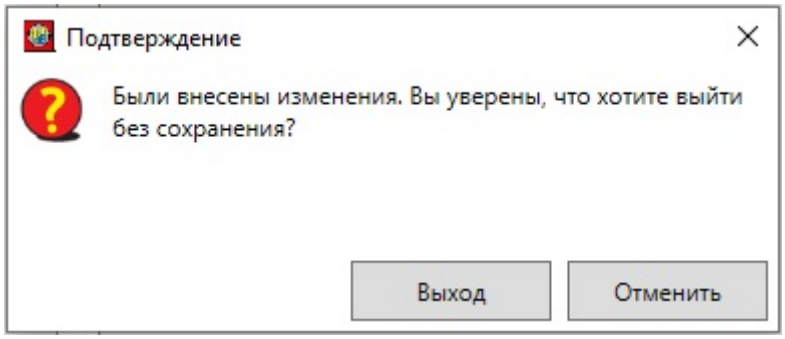



**Рисунок 16 – Окно подтверждения выхода без сохранения изменений**

Обратите внимание, что сохранение настроек возможно только в случае, если пользователю Гл. Администратор назначен идентификатор и задан пароль. Это гарантирует, что впоследствии будет как минимум один администратор, через которого можно войти в программу. В случае удаления пользователя Гл. Администратор следует создать нового пользователя с этим именем в рамках текущей рабочей сессии, в противном случае сохранение базы станет невозможным (рисунок 17).

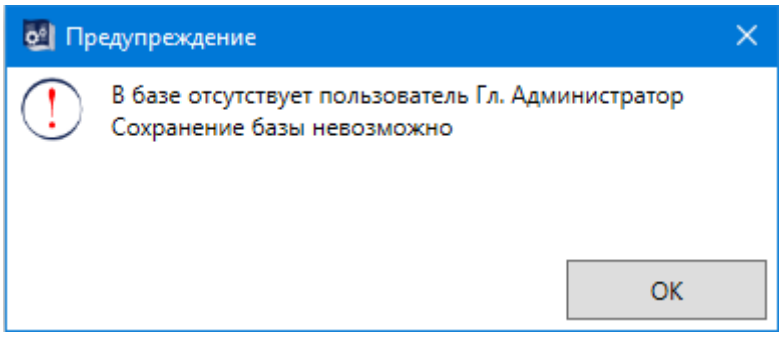



**Рисунок 17 – Предупреждение о невозможности сохранения базы, в которой отсутствует пользователь с именем Гл. Администратор**

# 3. Администрирование подсистемы разграничения доступа

После запуска программы AcedVI Администратор БИ регистрирует пользователей, назначает каждому идентификатор, задает пароль. К обязательным функциям администрирования также относятся редактирование параметров доступа групп пользователей к объектам комплекса «Аккорд» и составление списков контроля целостности файлов. В данном разделе подробно описаны все возможности администрирования подсистемы разграничения доступа.

## 3.1. Привилегии Администраторов

Все пользователи группы «Администраторы» обладают определенными привилегиями, изменять которые может только главный Администратор.

Доступны следующие привилегии (поле «Привилегии Администраторов» на рисунке 23):

- «Редактирование пользователей» – позволяет создавать и удалять пользователей и группы пользователей, а также редактировать их параметры (имя, идентификатор, пароль, параметры пароля);
- «Редактирование контроля» – позволяет устанавливать списки для контроля целостности;
- «Управление журналом» – позволяет выполнять процедуры просмотра, архивации, разархивации, удаления журналов событий;
- «Редактирование настроек» – позволяет устанавливать необходимые настройки с помощью утилиты AcSetup.exe (подробнее см. документ «Руководство по установке» 11443195.4012-036 98, подраздел 2.1);
- «Контролер» – позволяет контролировать доступ пользователей к рабочим станциям. Пользователь с привилегией «Контролер» контролирует 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» (подробнее см. п.3.14);
- «Оператор НШР» - может выполнять выход из Хранителя экрана других пользователей;
- «Оператор пользовательских УЗ» - установка этой привилегии позволяет выделенному Администратору осуществлять просмотр отдельных пользователей базы во всех группах (доступен поиск по имени и идентификатору), кроме группы «Администраторы» (рисунок 19), а также создавать (импортировать из AD и Amz), удалять (рисунок 20), изменять имя (в том числе доменное), идентификатор и пароль пользователей в этих группах. Блок «Привилегии Администраторов» при установке этой привилегии выглядит, как показано на рисунке 18.

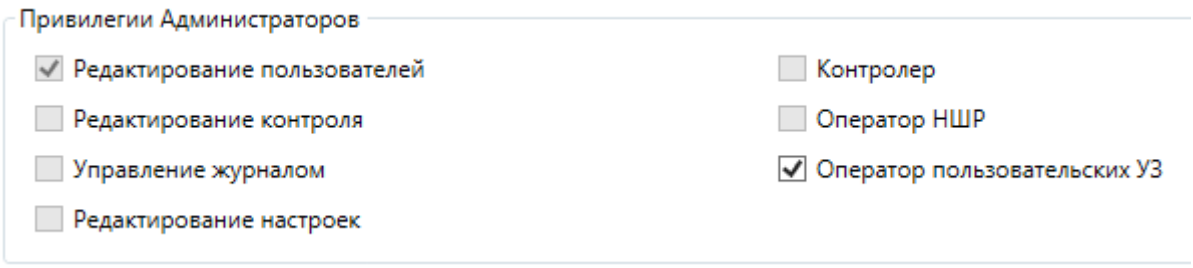



**Рисунок 18 – Блок «Привилегии Администраторов» при установке привилегии «Оператор пользовательских УЗ»**

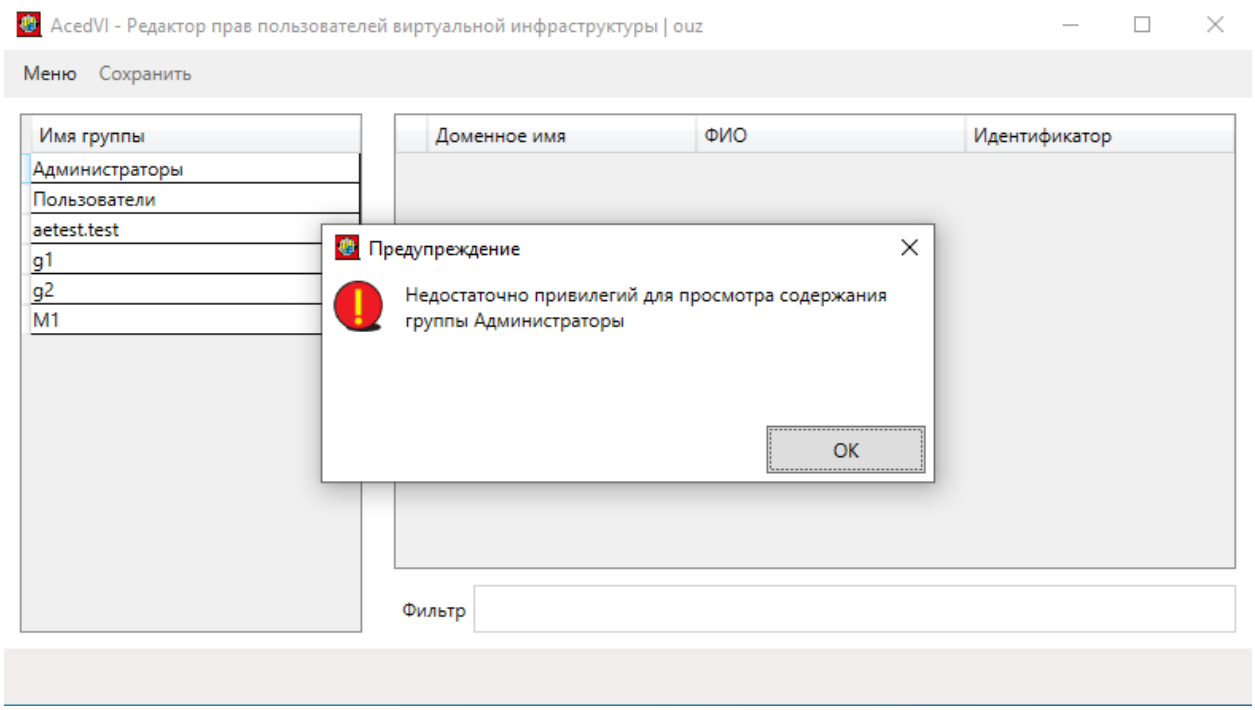



**Рисунок 19 - Главное окно программы для Оператора пользовательских УЗ при попытке выделить группу «Администраторы»**

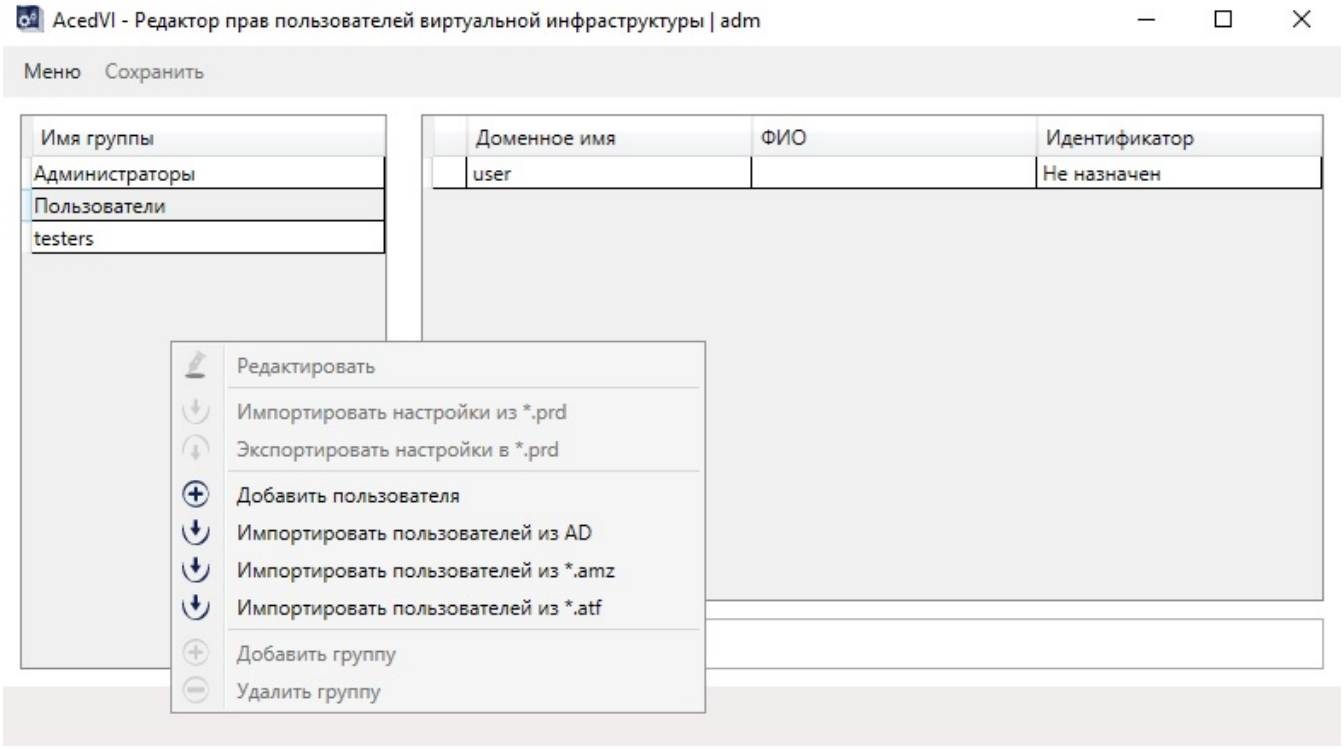



**Рисунок 20 - Контекстное меню таблицы групп для Оператора пользовательских УЗ**

Привилегиями «Контролер» и «Оператор НШР» могут наделяться пользователи, не входящие в группу «Администраторы».

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

- «Редактирование пользователей» – запрещено редактирование правил разграничения доступа пользователя (рисунок 21);

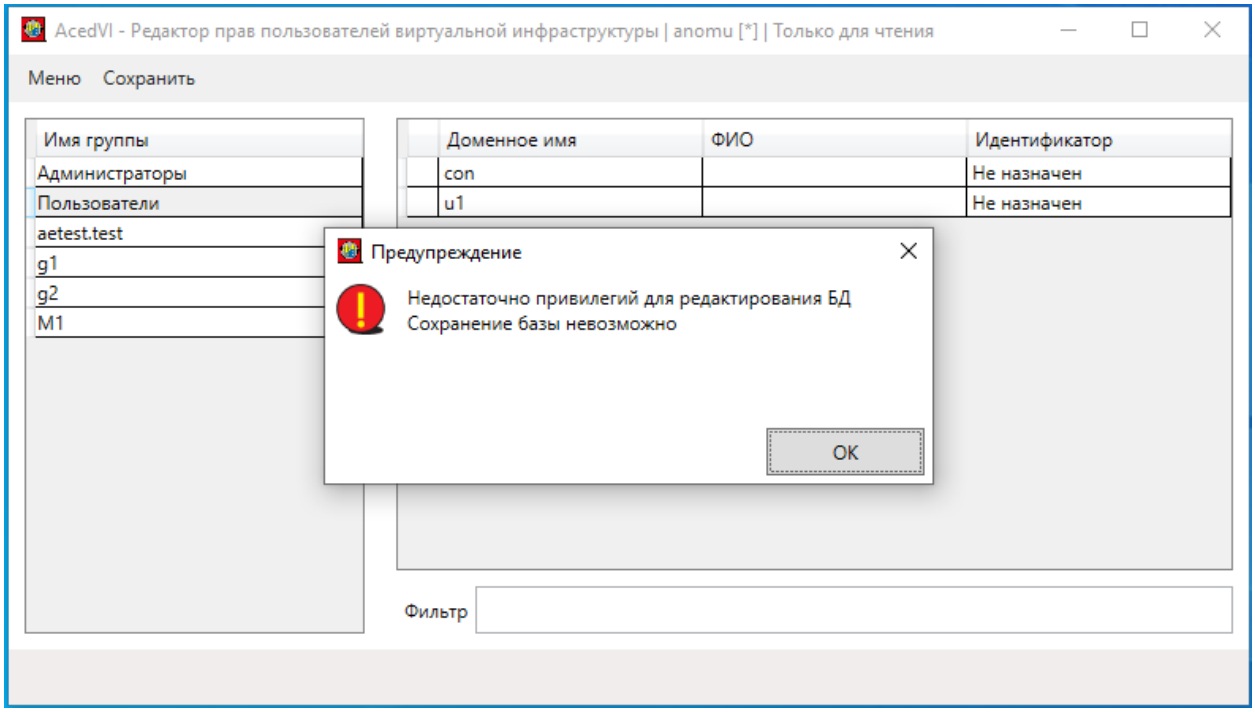



**Рисунок 21 - Запрет сохранения БД при отсутствии флага «Редактирование пользователей» у текущего администратора**

- «Управление журналом» – запрещена работа с журналами регистрации;
- «Редактирование настроек» – запрещена модификация файлов Accord.ini, AcTskMng.ini[2].

## 3.2. Регистрация группы пользователей

Группы «Администраторы» и «Пользователи» создаются при инициализации БД пользователей комплекса «Аккорд», и их нельзя переименовать или удалить – эти процедуры допустимы только для вновь создаваемых групп. Используя контекстное меню в полях со списком групп и списком пользователей главного окна, в группу можно добавить пользователей, в том числе из службы каталогов Windows или БД пользователей комплекса «Аккорд», и редактировать ее параметры (из меню команд списка групп). Параметры группы являются универсальным шаблоном для задания параметров пользователя и присваиваются по умолчанию каждому добавленному в нее пользователю, но следует учитывать, что для каждого пользователя можно изменить параметры в индивидуальном порядке (кроме настроек контроля целостности и разграничения доступа). При создании новой группы следует учитывать, что допустимыми символами в ее имени являются буквы латинского и русского алфавитов и символы @ _ . -.

На рисунке 22 изображено окно редактирования группы «Администраторы». Поля настроек этого окна подробно описаны в нижеследующих подразделах.

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

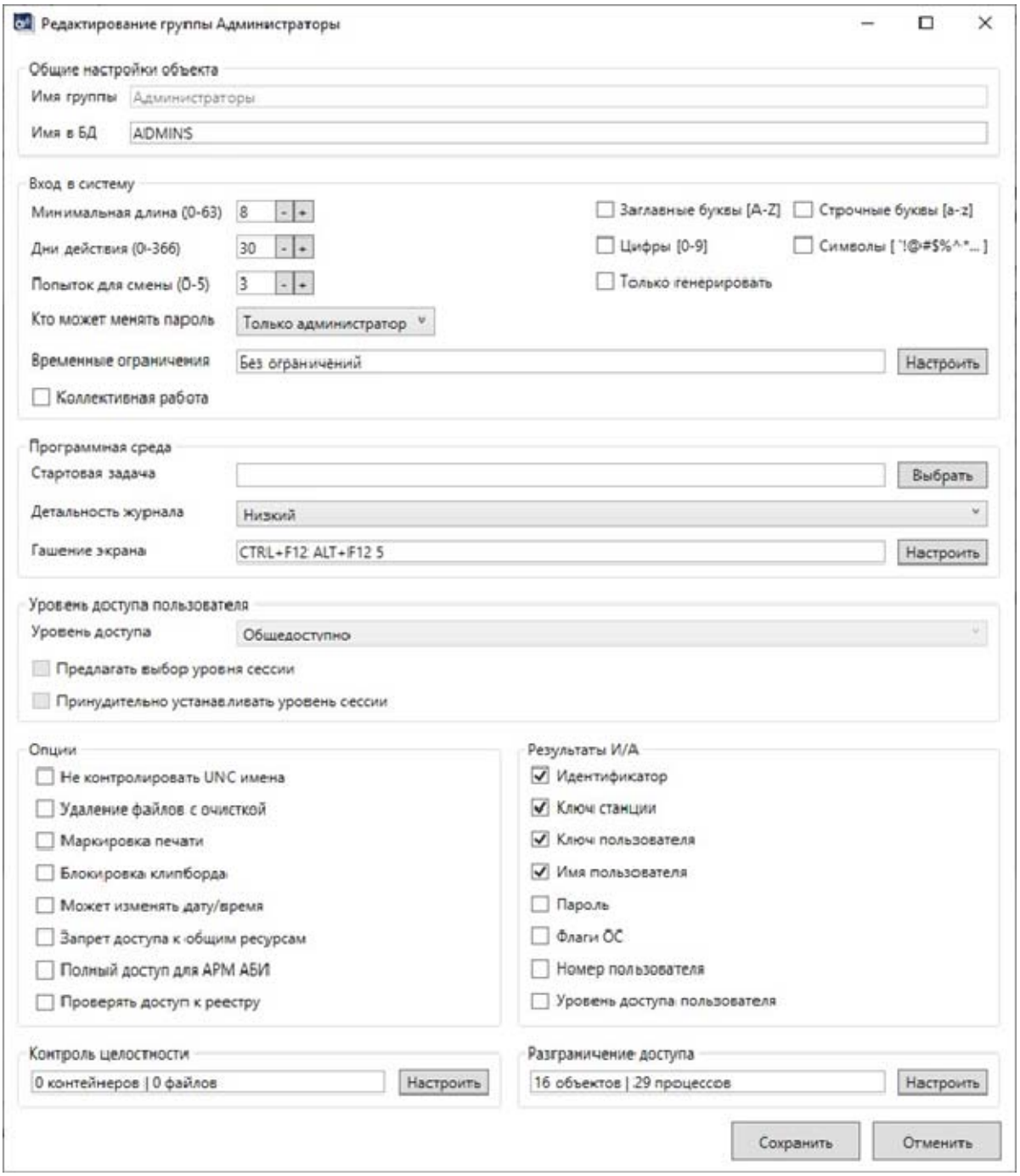



**Рисунок 22 – Окно редактирования группы «Администраторы»**

## 3.3. Регистрация пользователя

Добавить пользователя в группу можно при выполнении соответствующей команды контекстного меню в списке групп или в списке пользователей главного окна программы. При создании пользователя Администратор присваивает ему уникальное в данной вычислительной среде имя. Это имя отображается в окне редактирования пользователя (рисунок 23) в строке «Имя в БД» поля «Общие настройки объекта». Допустимыми символами для имени пользователя являются буквы латинского алфавита и символы @ _ . -. При

импорте пользователя из AD имя генерируется автоматически на основании доменного.

Если пользователю необходимо назначить несколько идентификаторов, отдельные буквы его имени можно записывать с измененным регистром. Зависимость полного имени пользователя от регистра прописывается в конфигурационном файле локальных настроек AcedVI (AcedVICLI) LocalConfig.json в параметре «LowerCasedFullNames». По умолчанию задано значение false, и этот режим различает регистры в полном имени пользователя. Если изменить значение параметра ("LowerCasedFullNames": true), все буквы имен пользователей будут принудительно приведены к строчному формату. В этом случае в БД могут появиться пользователи с одинаковыми полными именами, что приведет к невозможности открытия базы. Это надо учитывать при желании убрать зависимость от регистра в именах пользователей.

В строке «ФИО» можно дополнительно добавить ФИО пользователя. Остальные поля настроек окна редактирования пользователя подробно описаны в нижеследующих подразделах.

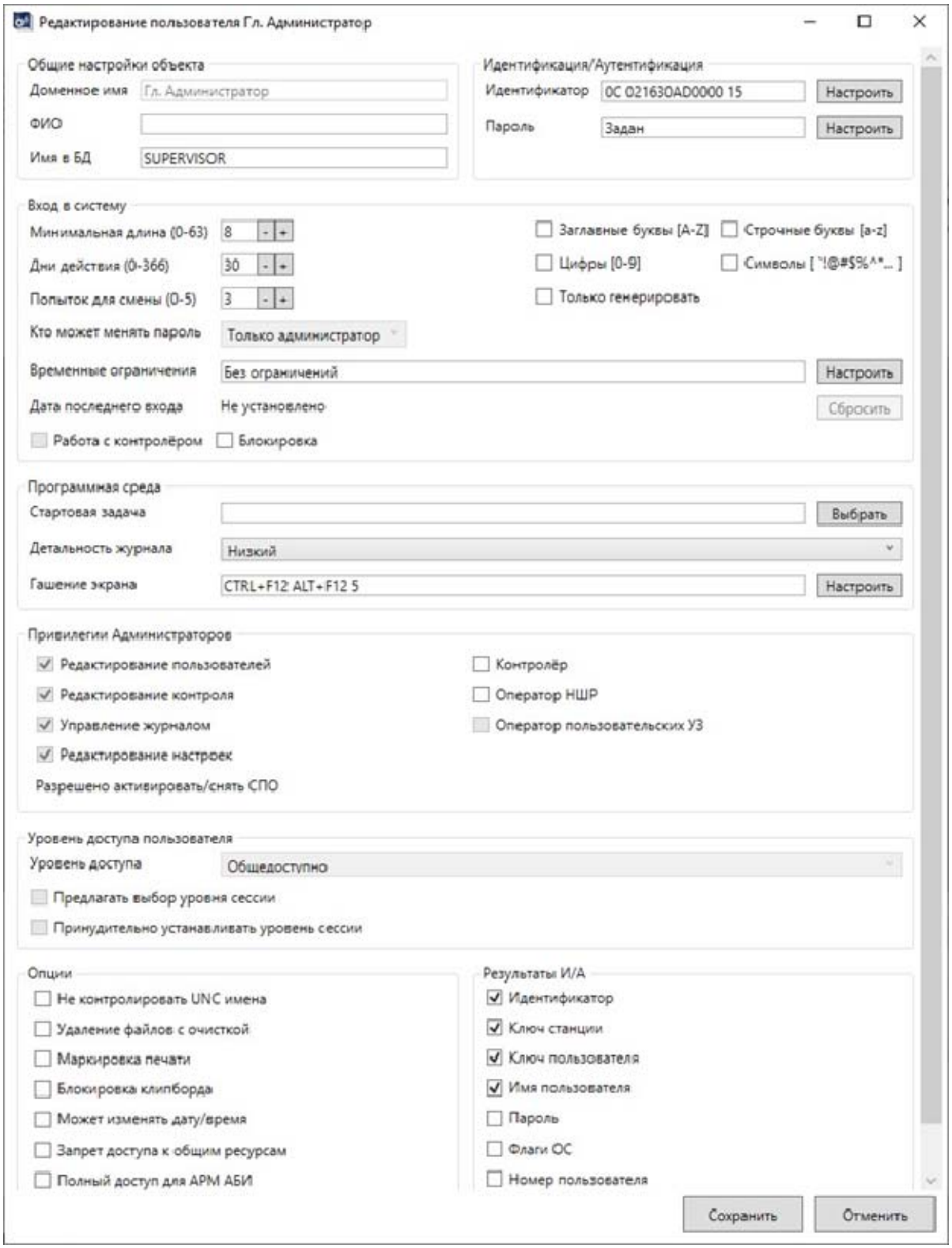



**Рисунок 23 – Окно редактирования пользователя Гл.Администратор**

## 3.4. Импорт пользователей из AD

При необходимости импортирования в БД комплекса «Аккорд» пользователей из службы каталогов Windows следует в главном окне

программы отметить нужную группу и выполнить команду контекстного меню поля со списком групп или списком пользователей «Импортировать пользователей из AD». В появившемся при выполнении этой команды окне импортирования (рисунок 24) следует заполнить строки «Сервер» (ввести адрес сервера в формате FQDN), «Логин» и «Пароль», после чего нажать кнопку <Загрузить>. При успешном подключении к серверу в строках «Сервер» и «Логин» отобразятся данные о последнем введенном пользователе (если ранее уже проводился импорт), а в правой части строки «Сервер» появится раскрывающийся список всех учетных данных, использовавшихся ранее. Имеется возможность удалить пользователя из этого списка клавишей <delete>.

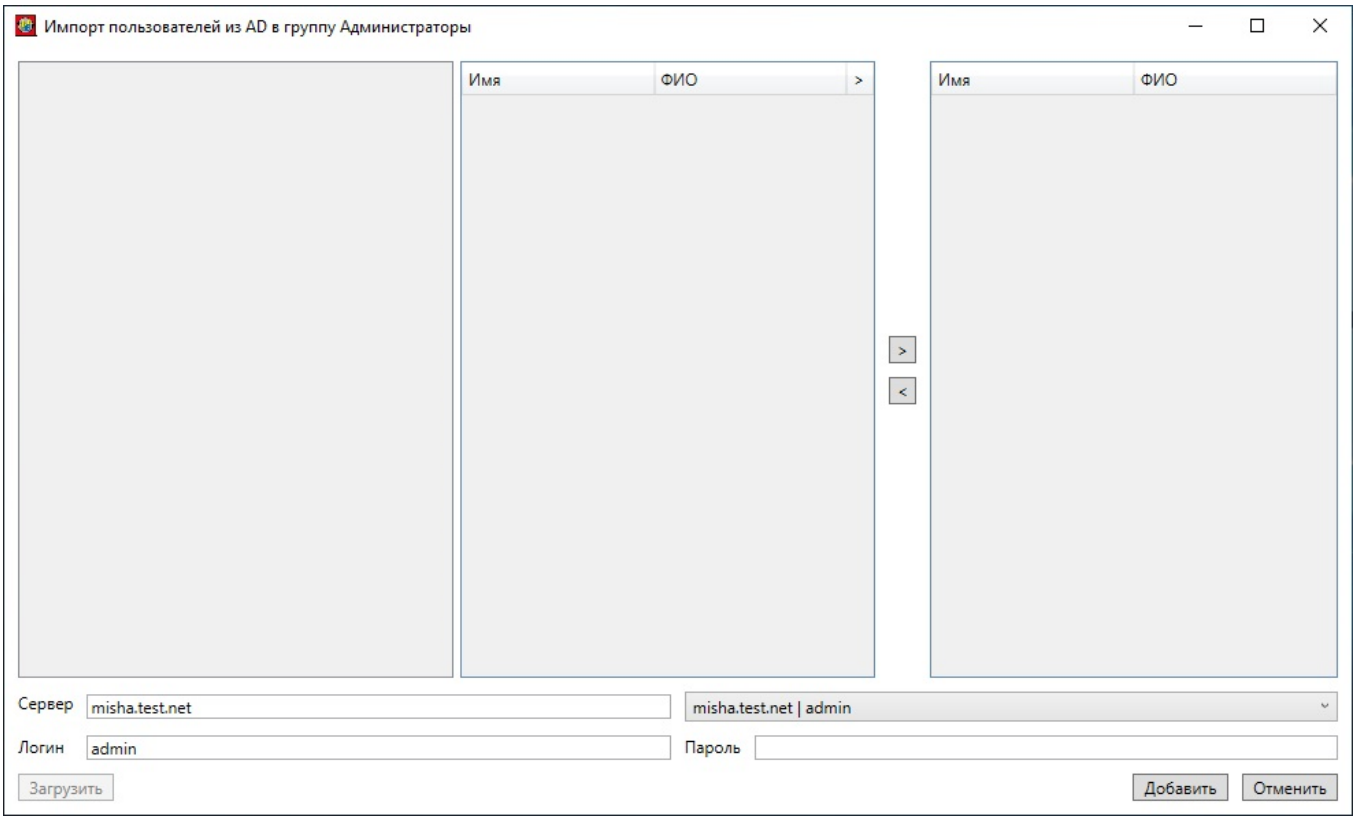



**Рисунок 24 – Окно импорта пользователей из AD**

При нажатии кнопки <Загрузить> начнется загрузка данных из AD. После полной загрузки в левой части окна отображается древовидный список подразделений (рисунок 25), каждая строка которого имеет следующую структуру: имя подразделения, количество выбранных пользователей в нем, общее количество пользователей в нем и количество вложенных подразделений (OU). При этом сразу после загрузки данных количество пользователей в списке не показано. Его можно увидеть, воспользовавшись командой контекстного меню левой таблицы «Раскрыть все». Все количественные данные соответствуют ближайшему уровню вложения.

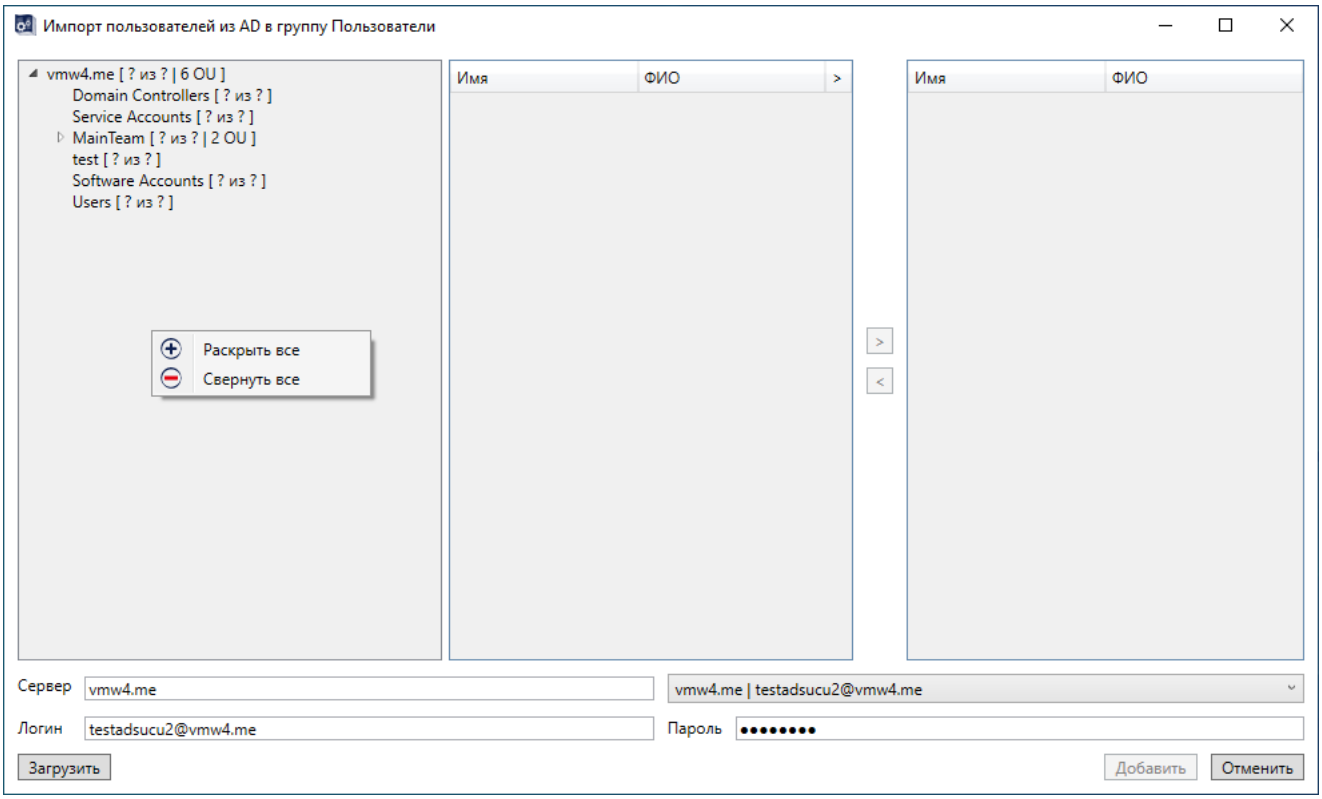



**Рисунок 25 – Отображение загруженных данных из AD**

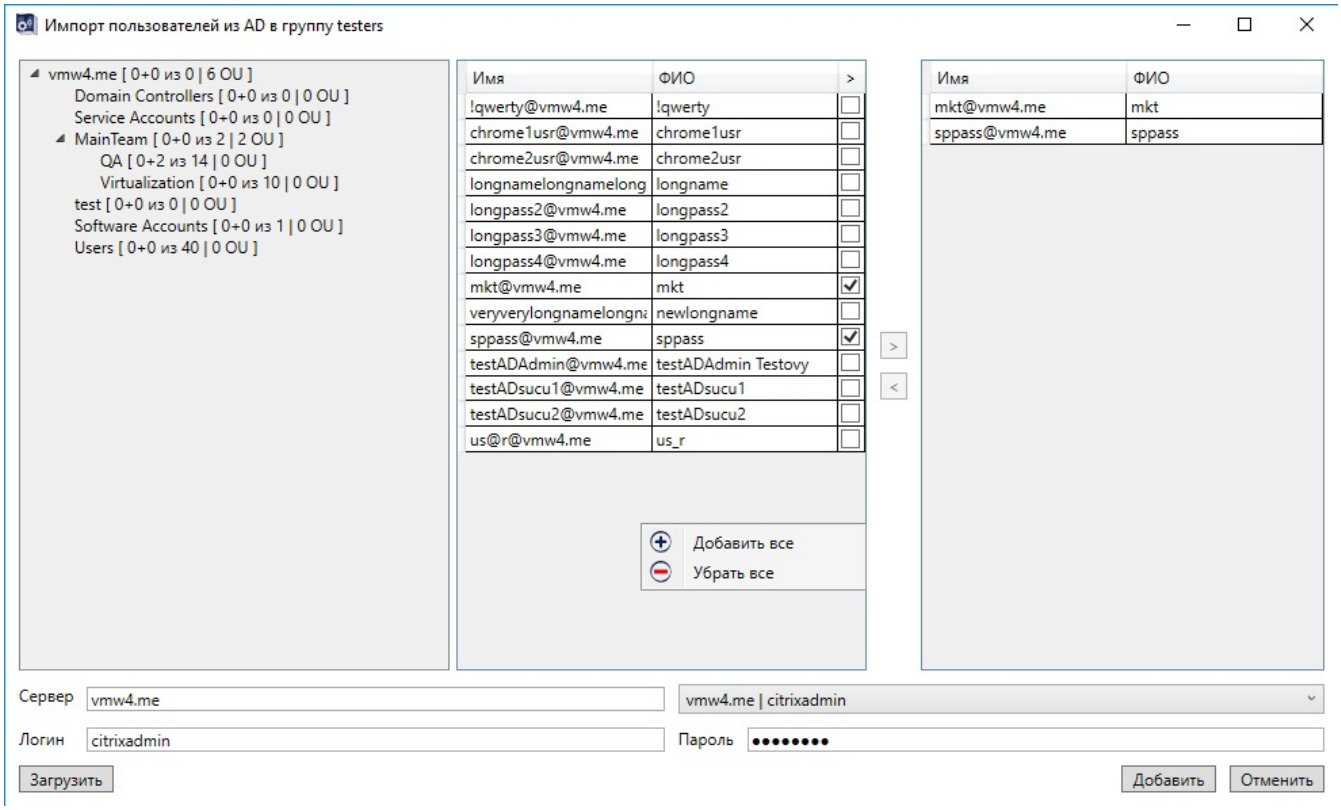



**Рисунок 26 – Отображение данных выбранного подразделения**

При выборе подразделения из списка левой таблицы в центральной таблице отображается список его пользователей (на том же уровне вложения,

рисунок 26). Выбор пользователей для добавления в БД комплекса «Аккорд» отмечается проставлением галочки или двойным щелчком на имени пользователя в соответствующих строках этой таблицы, при этом в правой таблице окна импортирования отображается список выбранных пользователей (из всех подразделений, а не только из отмеченного на данный момент). Если пользователь с указанным именем уже есть в БД, галочка в этой строке проставляется автоматически и недоступна для изменения (см. рисунок 26).

При необходимости отметить сразу нескольких пользователей для добавления следует выбрать нужные строки с пользователями в центральной таблице и нажать кнопку «>» - все выбранные пользователи будут отмечены галочками и добавлены в правую таблицу.

Аналогичным образом можно убрать нескольких пользователей из ранее составленного списка на добавление - выбрать строки с пользователями в правой таблице и нажать кнопку «<». При этом из центральной таблицы исчезнут отметки о добавлении, а из правой таблицы - сами пользователи.

Вызываемое мышью контекстное меню центральной таблицы содержит разделы "Добавить все" и "Убрать все", а меню правой таблицы - раздел «Очистить список».

После составления списка на добавление в БД следует нажать кнопку <Добавить>. Окно импортирования при этом закрывается, а список из правой таблицы добавляется в выбранную в главном окне группу (рисунок 27).

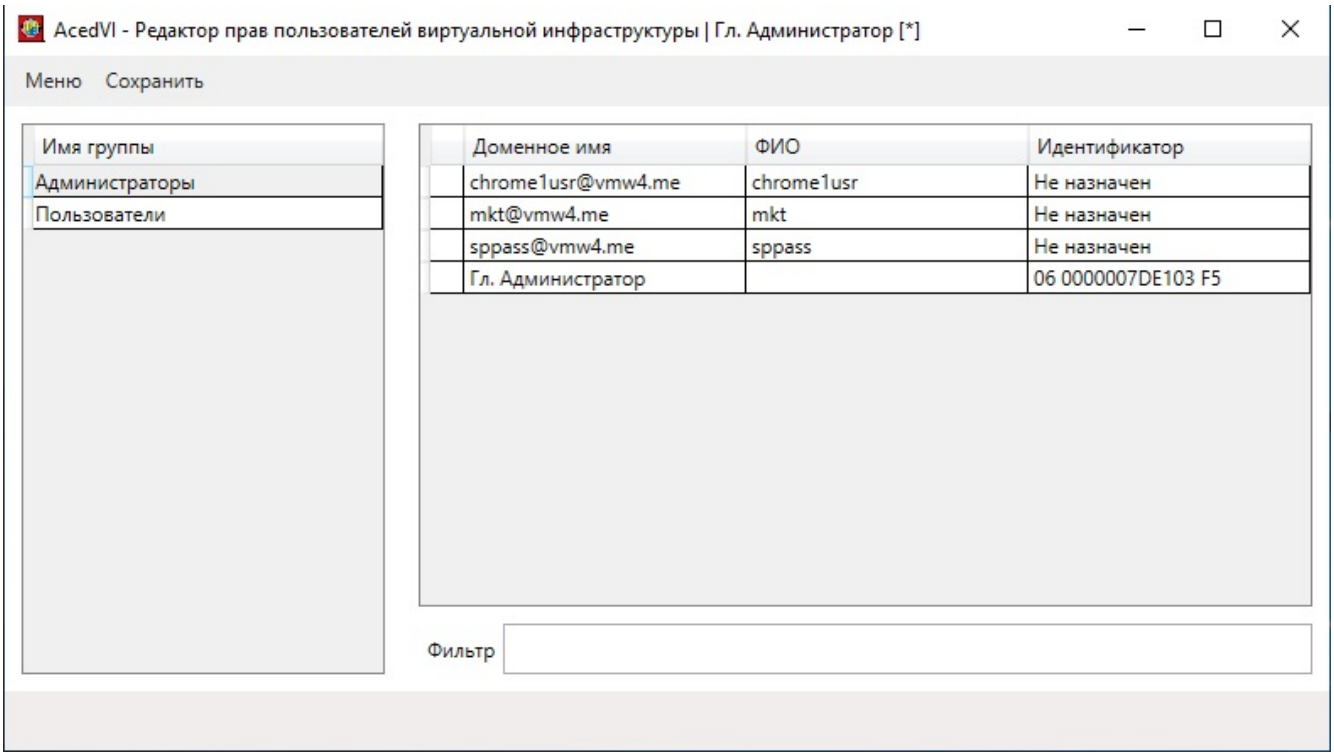



**Рисунок 27 – Добавление пользователей из AD в группу «Администраторы»**

## 3.5. Особенности преобразования БД Accord.amz при запуске программ AcedVI и AcedVICLI

В базе данных пользователей при каждом запуске программ AcedVI и AcedVICLI (работа с командной строкой) происходит анализ определенных параметров, результатом которого может стать модификация пользовательских данных до момента включения функциональности программ. Помимо этапа запуска программ, модификация происходит при выполнении импорта из .amz.

Основные преобразования БД связаны с параметрами конфигурационного файла локальных настроек AcedVI (AcedVICLI) LocalConfig.json. Так, значение параметра DuplicateNamesMode может привести к изменению БД в случае совпадения полных/доменных имен пользователей. Параметр имеет три значения: Abort (по умолчанию), Remove, Rename. Следует учесть, что если параметра DuplicateNamesMode в файле LocalConfig.json нет, то он появится со значением по умолчанию при первом запуске AcedVI[3]. И если в загружаемой базе при значении Abort обнаружатся пользователи с одинаковыми именами, то такая база отобразится пустой, а в нижней панели окна будет сообщение о причине ошибки открытия БД (рисунок 28).

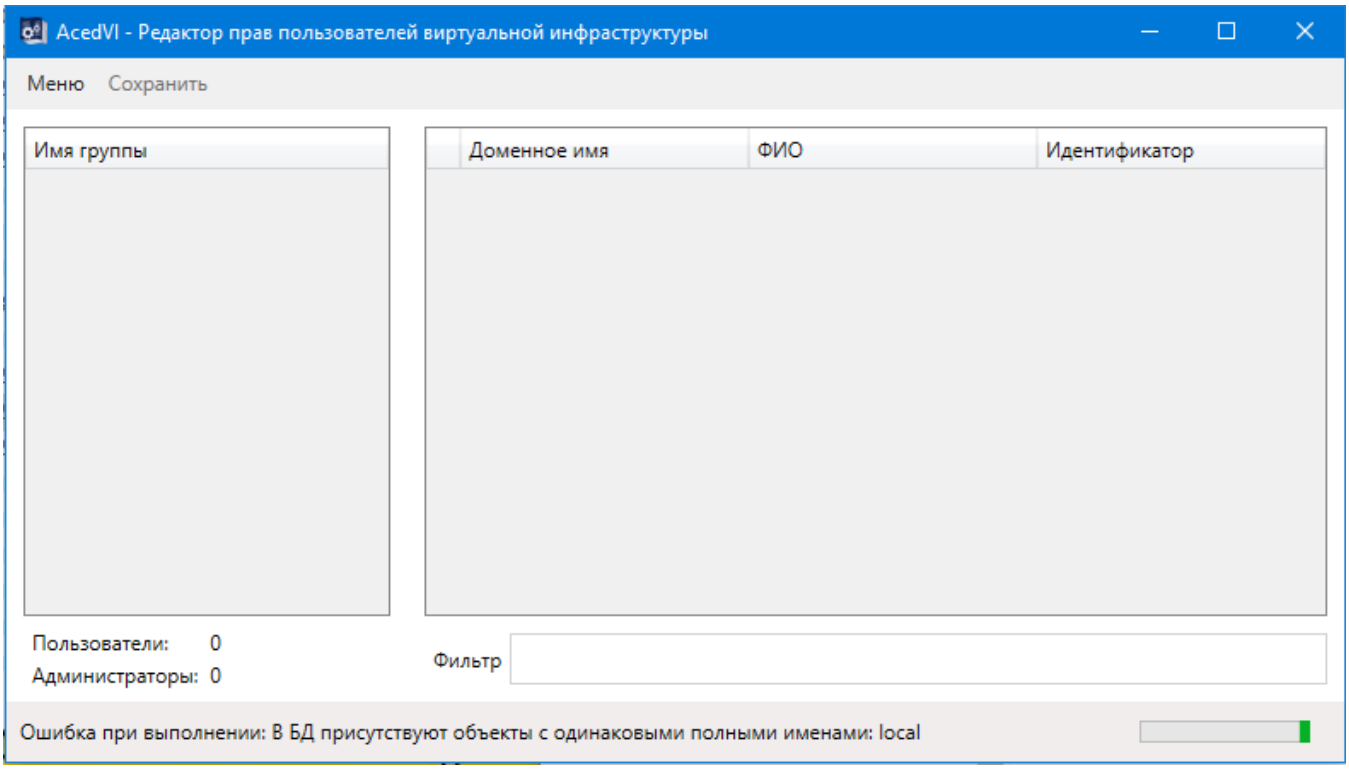



**Рисунок 28 - Ошибка при открытии БД, в которой присутствуют пользователи с одинаковыми полными именами**

[3] При переходе с использования программы Aced32 на AcedVI не рекомендуется сразу запускать программу AcedVICLI. Следует сделать первый вход через AcedVI, оценить загруженную базу с точки зрения возможных преобразований и сохранить ее. При последующих запусках AcedVICLI все стартовые изменения в БД будут регистрироваться в журнале, но в явном виде сообщения показаны не будут – только при конфликте имен при выставленном значении Abort параметра DuplicateNamesMode

Если подобная ситуация сложится при проведении импорта из .amz, появится сообщение об ошибке импорта (рисунок 29), причина ошибки также отобразится в нижней панели окна импорта.

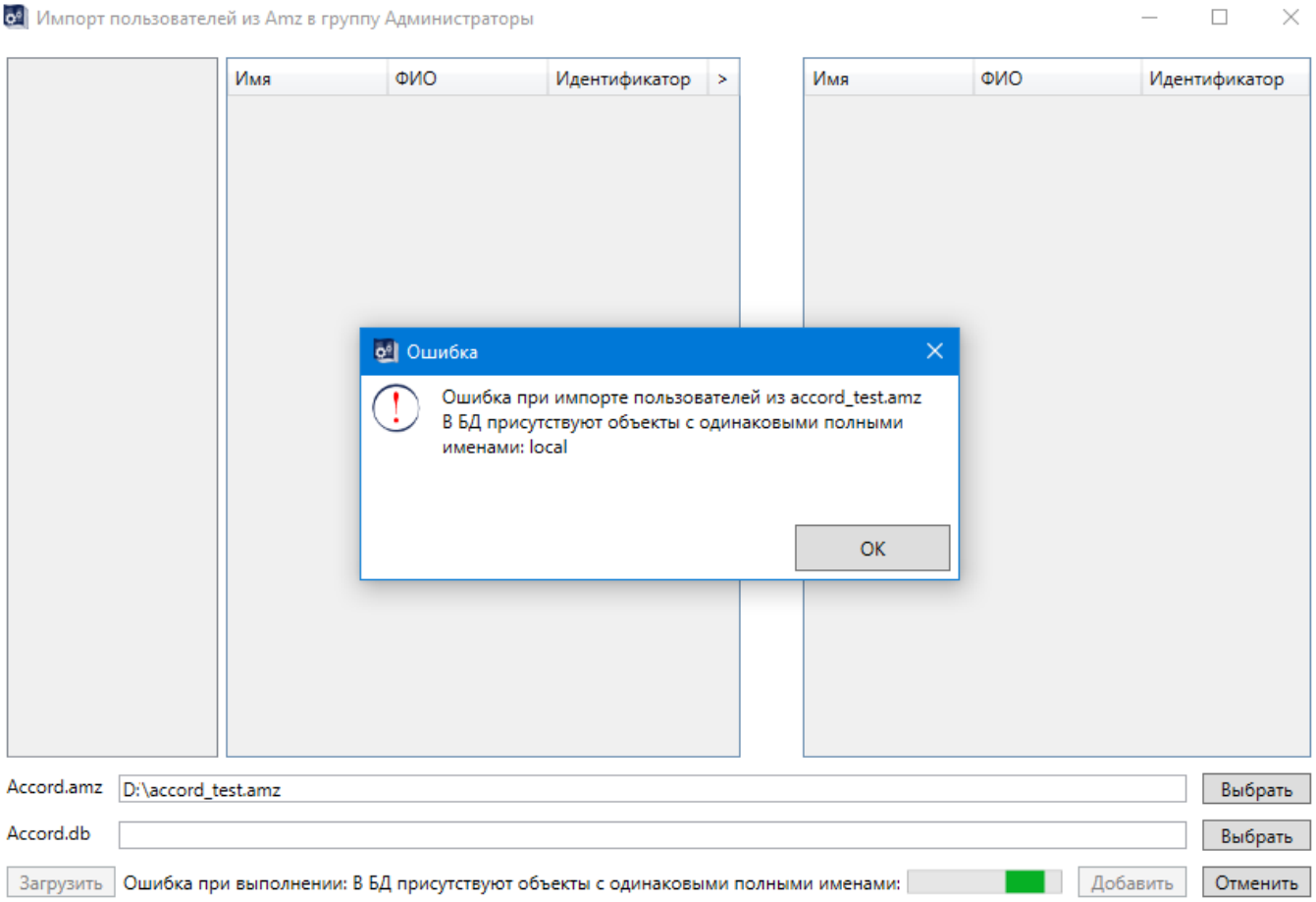



**Рисунок 29 - Сообщение о невозможности провести импорт БД**

При установке значения Remove из базы удаляются пользователи с одинаковыми доменными именами (кроме одного), а в журнал регистрации заносится информация по каждой операции удаления[4].

Значение Rename позволяет оставить в базе всех пользователей с изначально совпадающими именами, при этом произойдет их переименование: если в файле локальных настроек включен параметр LowerCasedFullNames (true), в конец имени пользователя добавится сквозная нумерация; в противном случае (false) в совпадающем имени пользователя будет изменен регистр последней буквы, а при нескольких таких пользователях у следующего будет изменен регистр предпоследней буквы, и так далее, к началу имени, после чего будет добавляться цифра (возрастающая) в конец имени.

Вышеупомянутые параметры конфигурационного файла учитывают только конфликт пользовательских имен, но он может проявиться не только между пользователями, но и между пользователем и группой, поэтому в редакторе

[4] При любых операциях с пользователями в журнал регистрации событий вносится запись формата «Создан (удален) пользователь {DisplayName} (имя в БД {UserName}, идентификатор {TmId/Не назначен})», где DisplayName - Доменное/Полное имя, TmId - идентификатор

AcedVI нельзя создавать пользователей с именами групп. Подобный конфликт возможен в случаях загрузки базы редактора Aced32.

Помимо обстоятельств совпадения полных/доменных имен пользователей преобразование имени может произойти в некоторых иных случаях. Например, если у пользователя не заполнено поле «Доменное имя», его обычное имя будет автоматически перенесено в это поле, а в качестве имени в БД останется имя, хэшированное от доменного. Исключением в этой ситуации является пользователь SUPERVISOR, у которого при работе через AcedVI может быть только пустое доменное имя, а если БД открывается после работы через Aced32, его полное имя будет очищено. В таком случае рекомендуется вручную создать дополнительного администратора с аналогичным доменным именем.

Следует учитывать, что подобное видоизменение имен происходит до анализа БД на совпадение полных/доменных имен.

Также следует обратить внимание, что в БД при ее открытии у пользователей очищаются списки ПРД и списки КЦ.

Любые преобразования БД в обязательном порядке регистрируются в журнале.

## 3.6. Импорт пользователей из *.amz

Импорт пользователей из БД комплекса «Аккорд» осуществляется аналогично импорту пользователей из AD. В окне импортирования в строке «Accord.amz» следует выбрать необходимую базу. Если в директории с этой базой будет найдена вспомогательная база Accord.db, содержащая некоторые дополнительные параметры пользователя (например, ФИО), то она автоматически отобразится в соответствующей строке, и загруженная (при нажатии кнопки <Загрузить>) база будет содержать полные пользовательские данные. В левой части окна импортирования (рисунок 30) отображаются группы выбранной базы Amz, а в центральной таблице появляется список пользователей отмеченной группы. Формирование списка для импортирования (правая таблица) осуществляется аналогично операциям импорта из AD.

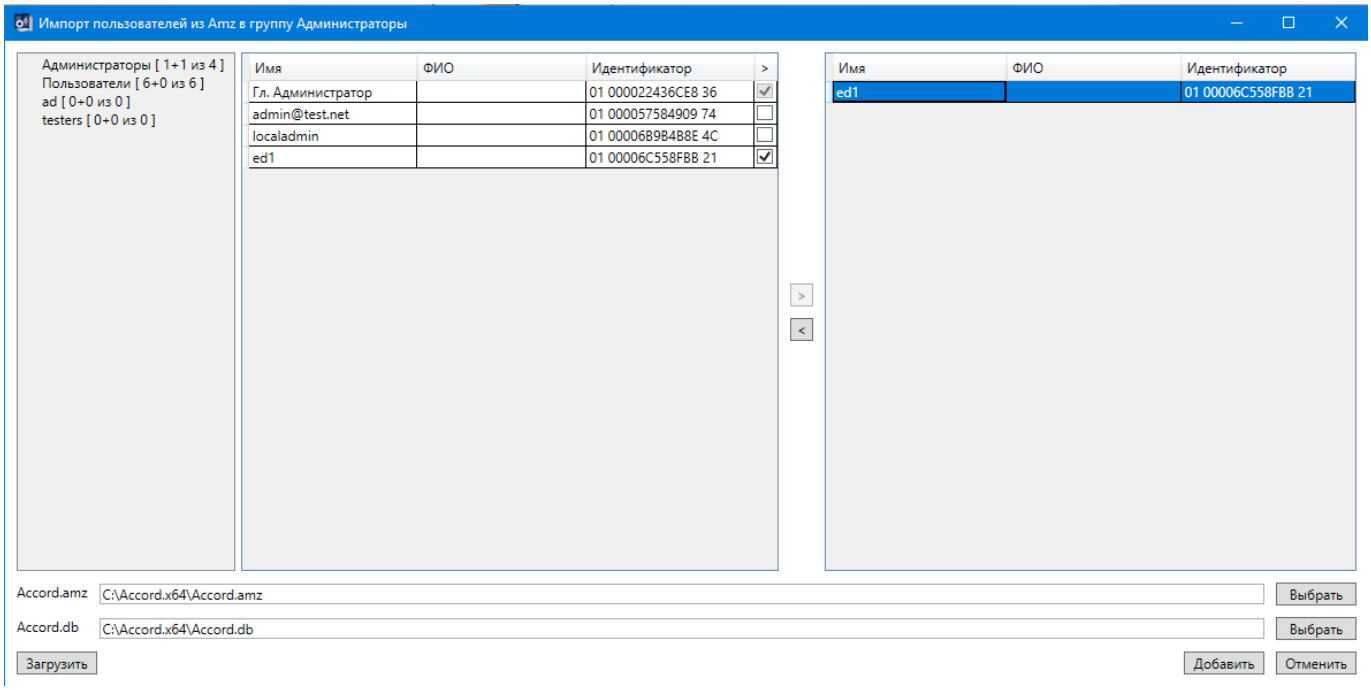



**Рисунок 30 - Отображение данных из базы Accord.amz**

Если в сформированном списке для импортирования обнаружатся пользователи, имеющие одинаковые полные имена с пользователями из текущей базы, то при импортировании (нажатии кнопки <Добавить>) этим пользователям будут заменены имена через смену регистра букв, начиная с последней, к началу имени (только для "LowerCasedFullNames": false) и далее добавлением цифры в конец имени.

## 3.7. Импорт пользователей из *.atf

При необходимости импортирования в выделенную группу информации о пользователях из файла с описанием идентификаторов *.atf следует в главном окне программы отметить нужную группу и выполнить команду контекстного меню поля со списком групп или списком пользователей «Импортировать пользователей из *.atf». Появится окно Windows для выбора файлов с фильтром *.atf. После выбора необходимого файла (допускается выбор нескольких файлов) откроется окно импортирования (рисунок 32).

Таблица в верхней части окна содержит записи (строки) со следующими данными из файлов *.atf:

- имя пользователя (параметр «Доменное имя»);
- идентификатор пользователя.

Если в разных файлах (при выборе нескольких файлов) встречаются одинаковые идентификаторы, то импорт из этих файлов не будет произведен. Появится информационное сообщение об игнорировании конкретных файлов с запросом подтверждения этого действия (рисунок 31), а если в этом окне нажать кнопку <Отменить>, остановится вся операция импорта пользователей.

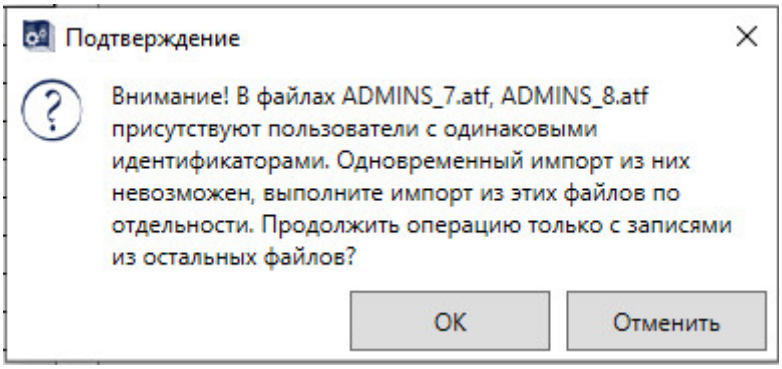



**Рисунок 31 – Сообщение при обнаружении одинаковых идентификаторов в разных файлах .atf при импорте пользователей**

Если идентификатор, указанный в файле .atf, уже существует среди назначенных в БД, в соответствующей строке таблицы появится отметка об этом, и пользователь из этой записи будет недоступен для импортирования.

Если поле идентификатора в файле .atf будет иметь нулевое значение, в одноименном столбце таблицы отобразится статус «Не назначен» (при совпадении имен в случае выбора режима перезаписи пользователя ранее назначенный ему идентификатор будет сброшен).

Импортировать можно только пользователей, записи о которых отмечены в первом столбце таблицы. Кнопкой <Полный> отмечаются все пользователи (доступные для импортирования), кнопкой <Сброс> все сделанные отметки снимаются.

На пользователя с именем OBJECTS накладывается запрет импортирования.

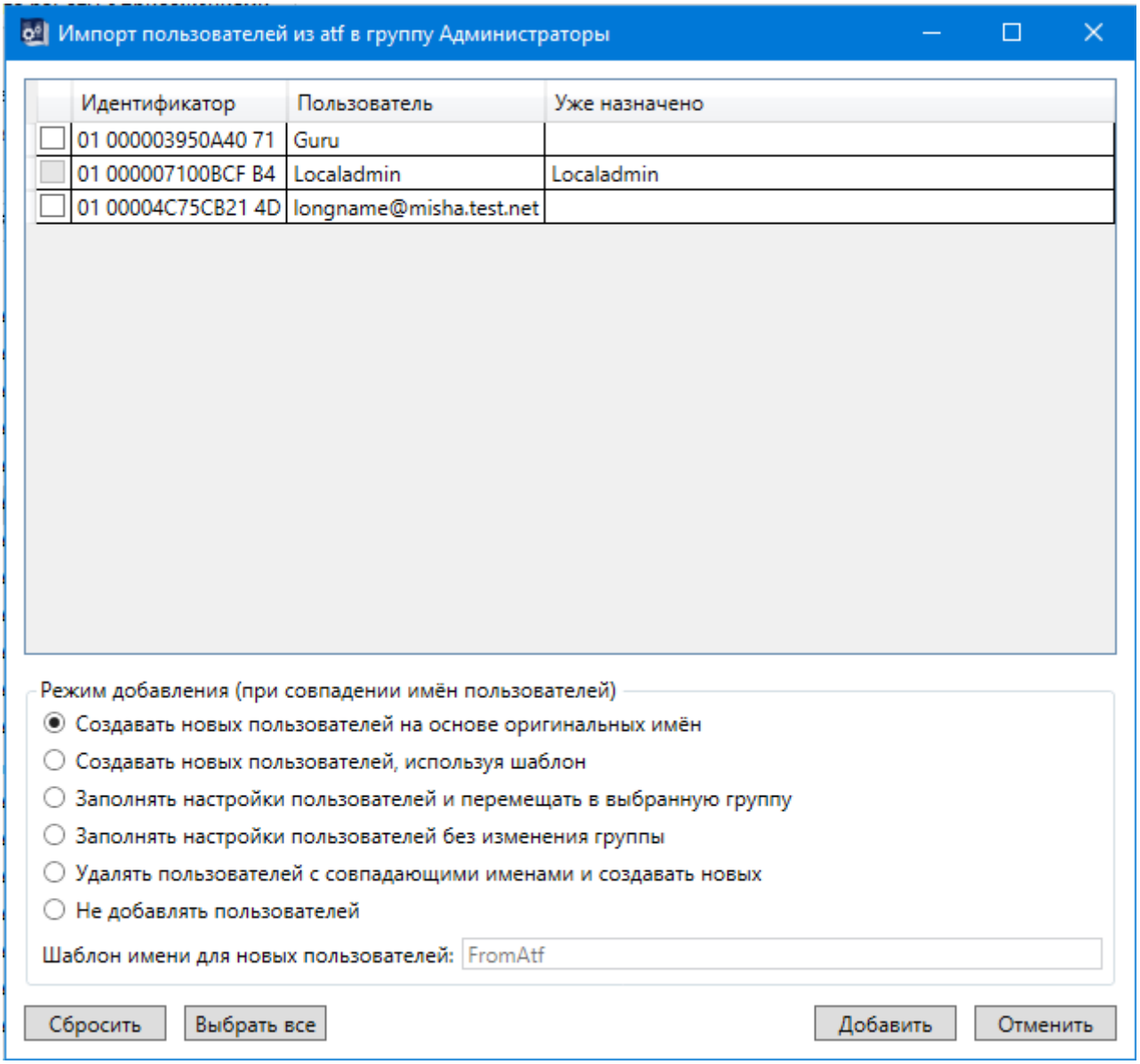



**Рисунок 32 - Окно импорта пользователей из файла *.atf в выделенную группу**

В нижней части окна импорта представлен список режимов, которые используются при совпадении имени пользователя, отмеченного для импортирования, с уже существующим в БД именем:

- «Создавать новых пользователей на основе оригинальных имен» - пользователь из БД с совпадающим именем останется без изменений, а в целевой группе будет создан пользователь с собственным именем, в котором будет изменен регистр последней буквы. Если обнаружатся несколько таких пользователей, то у следующего будет изменен регистр предпоследней буквы, и так далее, к началу имени, после чего будет добавляться цифра (возрастающая) в конец имени. Если в файле локальных настроек параметру LowerCasedFullNames установлено значение true, в конец имени создаваемого пользователя сразу будет добавлена сквозная нумерация. Все созданные в этом режиме пользователи получат настройки синхронизации от группы и идентификатор из файла .atf;

- «Создавать новых пользователей, используя шаблон» - в этом режиме пользователь из БД с совпадающим именем останется без изменений, а в целевой группе будет создан пользователь с именем FromAtf и добавлением к имени сквозной нумерации. Если среди выбранных пользователей окажутся другие с совпадающими именами, все они также получат имя FromAtf с разными номерами в конце. Имя FromAtf предлагается по умолчанию (как и режим импорта), его можно заменить на любое другое в строке «Шаблон имени для новых пользователей». Все созданные пользователи получат настройки синхронизации от группы и идентификатор из файла .atf;
- «Заполнять настройки пользователей и перемещать в выбранную группу» - новый пользователь в этом режиме не будет создан, идентификатор из файла .atf применится к пользователю из БД (с перезаписью ранее назначенного идентификатора). Если этот пользователь был не в целевой группе, он будет перемещен в нее, при этом сохранит свои персональные настройки (остальные настройки будут синхронизированы от группы);
- «Заполнять настройки пользователей без изменения группы» - в этом режиме новый пользователь не будет создан, идентификатор из файла .atf применится к пользователю из БД (с перезаписью ранее назначенного идентификатора). Пользователь не будет перемещен в другую группу и сохранит все свои настройки, кроме идентификатора и пароля;
- «Удалять пользователей с совпадающими именами и создавать новых» - пользователь из БД с совпадающим именем будет удален и создан новый пользователь с таким же именем в целевой группе. Он получит все настройки от группы и идентификатор из файла .atf;
- «Не добавлять пользователей» - в этом режиме пользователь из БД с совпадающим именем останется без изменений, новый пользователь не будет создан, идентификатор из файла .atf не будет применен.

Если имя выбранного для импортирования пользователя отсутствует в БД, то он создается в целевой группе, получает настройки от нее и идентификатор из файла .atf.

Обратите внимание, что у всех импортированных пользователей будут сброшены (не заданы) пароли.

## 3.8. Регистрация идентификатора пользователя

В столбце «Идентификатор» таблицы со списком пользователей главного окна программы отображается информация об идентификаторе активного (выделенного) пользователя. Пока пользователю не назначен идентификатор, в окне редактирования (рисунок 23) недоступны для изменения другие параметры. Для регистрации идентификатора в поле «Идентификация/Аутентификация» следует нажать на кнопку <Настроить> строки «Идентификатор». Появится окно «Операции с ключом пользователя»

(рисунок 33). В нижней строке этого окна отображается информация о типе подключенного идентификатора и его серийный номер.

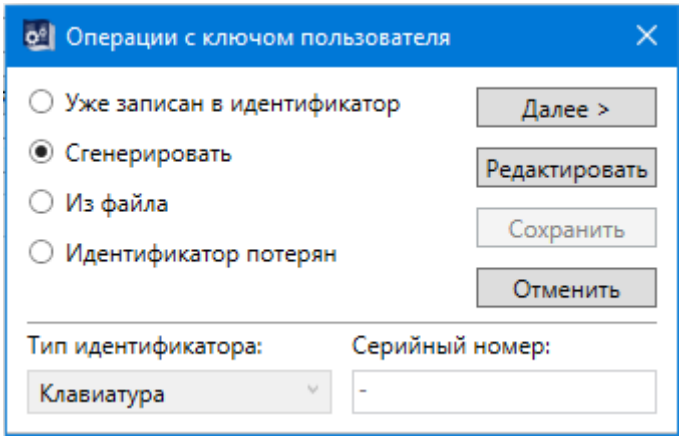



**Рисунок 33 – Окно операций с ключом пользователя**

Ключ пользователя генерируется с использованием датчика случайных чисел (ДСЧ) и записывается в энергонезависимую память идентификатора.

Идентификатор, в котором не записан ключ пользователя, считается недопустимым в СЗИ «Аккорд».

Возможны четыре варианта работы с ключом пользователя:

1) «Уже записан в Идентификатор».

Ключ может быть уже записан в идентификатор, например, при перерегистрации пользователя, который уже был зарегистрирован в составе комплекса «Аккорд» на другом СВТ, или ключ уже был сгенерирован при регистрации пользователя в контроллере «Аккорд-АМДЗ». Кнопка <Редактировать> позволяет изменить тип и серийный номер идентификатора (рисунок 34).

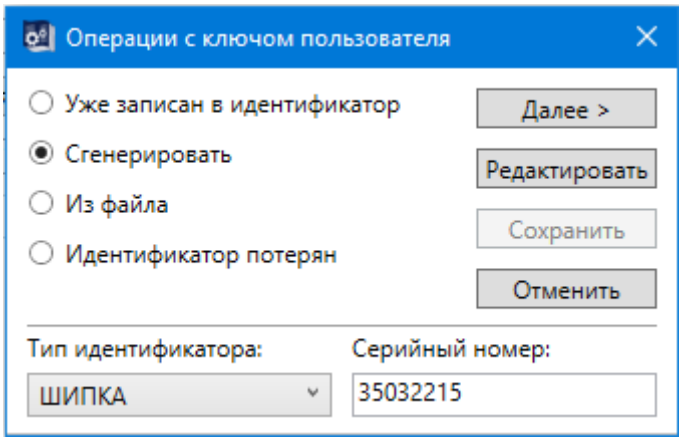



**Рисунок 34 – Режим редактирования типа и серийного номера идентификатора**

При нажатии кнопки <Далее> выдается запрос на считывание серийного номера идентификатора. При появлении запроса следует присоединить идентификатор пользователя к контактному устройству считывателя информации - происходит регистрация предъявленного идентификатора.

2) «Сгенерировать».

В этом случае при нажатии кнопки <Далее> генерируется новый ключ и выдается запрос на считывание серийного номера идентификатора. После присоединения идентификатора к контактному устройству считывателя происходит регистрация идентификатора и запись в него ключа пользователя. По окончании регистрации рекомендуется сохранить БД.

3) «Из файла».

Данная опция позволяет считать из файла (*.atf), подготовленного на другом компьютере с помощью специальной утилиты, номер идентификатора и ключ пользователя. При указании имени этого файла в окне запроса появляется окно для выбора идентификатора (рисунок 35). 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» 11443195.4012-036 98, подраздел 2.5.2).

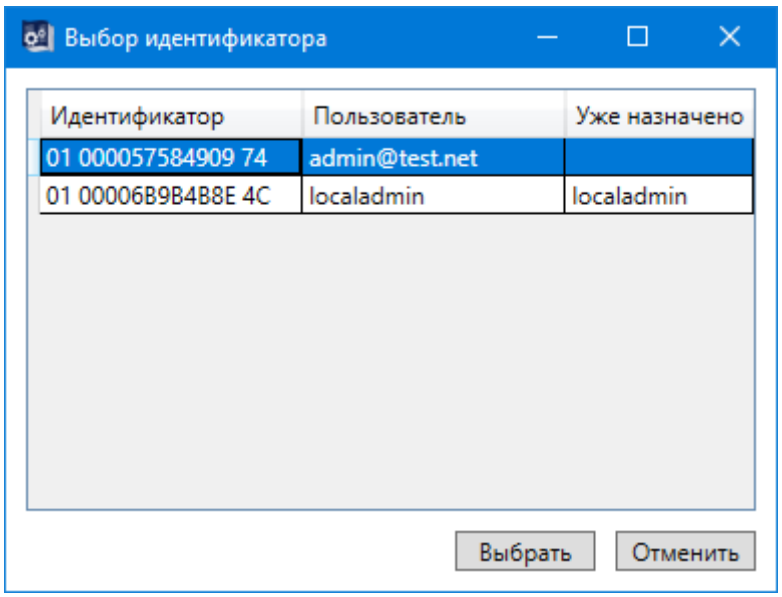



**Рисунок 35 – Считывание идентификатора и ключа пользователя из файла *.atf**

4) «Идентификатор потерян».

В этом случае при нажатии кнопки <Далее> поле «Идентификатор» данного пользователя примет значение «Не назначен». Все остальные настройки останутся неизменными. Администратор таким способом может временно отключить доступ данного пользователя на время разбора конфликтной ситуации, а потом восстановить его, назначив новый идентификатор.

## 3.9. Установка параметров пароля

Прежде чем задать пароль пользователя, следует настроить его параметры. Параметры пароля задаются в поле «Вход в систему» окна редактирования пользователя (рисунок 23) и включают в себя следующие характеристики:

- «Минимальная длина (0-63)» - диапазон значений от 0 (пароль задавать не обязательно) до 63 символов.
- «Дни действия (0-366)» - временной интервал действия пароля до смены: от 0 (нет смены пароля) до 366 дней.
- «Попыток для смены (0-5)» - количество попыток смены пароля: от 0 (бесконечное) до 5.
- «Кто может менять пароль» - установка прав на смену пароля (только Супервизор (Гл.Администратор) или Супервизор и пользователь).
- «Заглавные буквы [A-Z]», «Строчные буквы [a-z]», «Цифры» [0-9]», «Символы [`!@#$%^&*()_+|\[]{};:",<.>/?=-']» - определяют 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.
- «Только генерировать» - пароль будет генерироваться случайным образом из символов заданного алфавита при смене пароля пользователя.

Обратите внимание, что если пароль уже задан, то изменения его параметров вступят в силу только при смене пароля.

## 3.10.Задание пароля пользователя

Пароль настраивается в поле «Идентификация/Аутентификация» окна редактирования пользователя после задания его параметров. При нажатии кнопки <Настроить> в строке «Пароль» появляется окно задания пароля (рисунок 36).

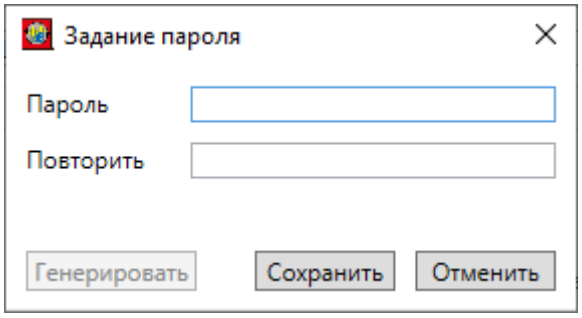



**Рисунок 36 – Окно задания пароля пользователя**

В этом окне следует ввести пароль (он должен соответствовать заданным ранее параметрам) и повторить его ввод для подтверждения. При использовании кнопки <Генерировать> полученная последовательность автоматически вводится в верхнее поле пароля (в виде символов •), а в нижней части окна в строке «Ваш новый пароль:» выводится текстовое значение пароля для возможности его повторного ввода (рисунок 37).

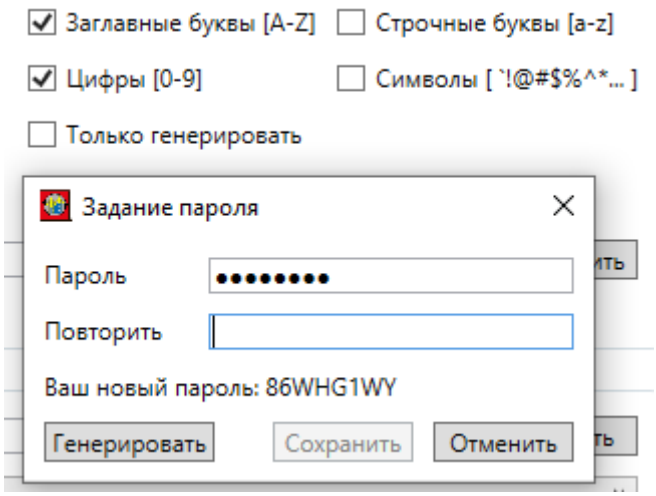



**Рисунок 37 – Окно задания пароля при его генерировании с выбранным алфавитом**

При выборе режима «Только генерировать» в окне задания пароля верхняя строка будет недоступна для изменения (рисунок 38).

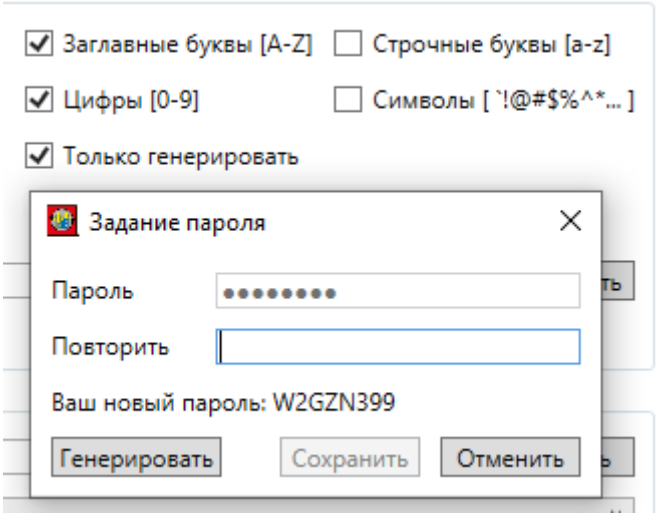



**Рисунок 38 - Окно задания пароля при его генерировании с выбранным режимом «Только генерировать»**

## 3.11.Установка детальности протокола работы

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. Значение поля «Детальность журнала» выбирается из списка, который раскрывается при щелчке мышью по кнопке, расположенной справа в одноименной строке окна редактирования пользователя (рисунок 23).

Параметр имеет следующие характеристики:

- «Отключен» - регистрация только входа/выхода из системы и событий НСД.
- «Низкий» - регистрация входа/выхода из системы, попыток несанкционированного доступа, запуска исполняемых модулей, событий СЗИ.
- «Средний» - то же, что при низкой детальности, плюс операции доступа к файлам и каталогам.
- «Высокий» - то же, что и при средней детальности, плюс все файловые операции, включая параметры команд.
- «Сбор статистики» - то же, что и при высокой детальности журнала, но помимо этого для пользователя не действуют установленные правила разграничения доступа.

## 3.12. Установка режима блокировки экрана

Блокировка экрана используется для временного отключения экрана и доступа к клавиатуре и мыши по истечении установленного интервала «неактивности» пользователя либо при нажатии комбинации горячих клавиш «Гашение» (по умолчанию <Ctrl+F12>). Вернуться в рабочий режим можно только при предъявлении идентификатора пользователя, который начал данный сеанс работы. Параметры гашения экрана редактируются по кнопке <Настроить>, расположенной в строке «Гашение экрана» поля «Программная среда» окна редактирования пользователя (группы). При ее нажатии появляется окно «Параметры Screen Saver» (рисунок 39).

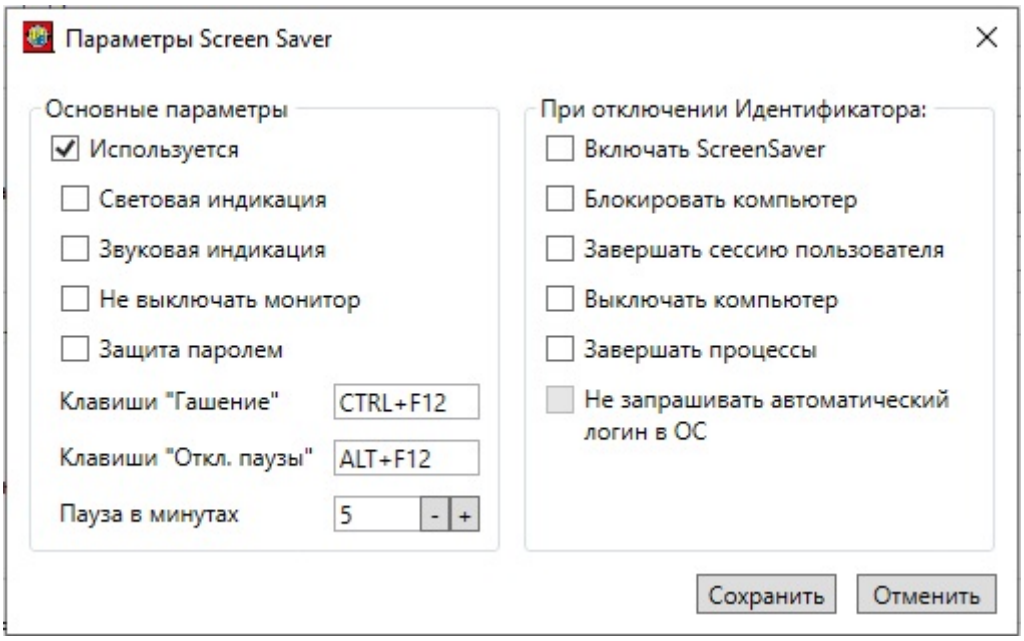



**Рисунок 39 – Окно редактирования параметров Screen Saver**

Необходимые параметры задаются с помощью мыши. Режим гашения экрана включается при установке параметра «Используется» (этот параметр имеет наиболее высокий приоритет). Затем (при необходимости) можно установить дополнительные параметры:

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

«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 блокировка мыши и клавиатуры не происходит, если же в этом поле установить значение, отличное от нуля, то блокировка происходит по истечении указанного временного интервала.

«Пауза в минутах» - временной интервал для перехода в режим гашения экрана, если клавиатура и мышь не используются (по умолчанию – 5 минут).

В поле Клавиши «Гашение» (по умолчанию <Ctrl+F12>) можно установить комбинацию клавиш принудительного включения Screen Saver.

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 установки другой комбинации клавиш «Гашение» или «Откл. паузы» необходимо перейти непосредственно в эти поля и одновременно нажать клавиши Shift, Ctrl или Alt и одну из клавиш F1-F12.

Поле «При отключении Идентификатора:» окна редактирования параметров гашения экрана определяет специальные режимы блокировки (выключения) при использовании идентификаторов, подключаемых к USB-портам компьютера – параметры этого поля позволяют задавать поведение компьютера при извлечении идентификатора из USB-порта.

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

При снятом флаге «Не запрашивать 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 с применением клавиш C-A-D «блокировать», то для выхода из режима блокировки потребуется предъявить идентификатор (если для этого пользователя используется хранитель экрана), а затем ввести пароль пользователя, включающего компьютер.

## 3.13.Установка временных ограничений

В строке «Временные ограничения» окна редактирования пользователя (группы) отображается информация о наличии временных ограничений. При

нажатии кнопки <Настроить> в этой строке появляется окно для их редактирования (рисунок 40).

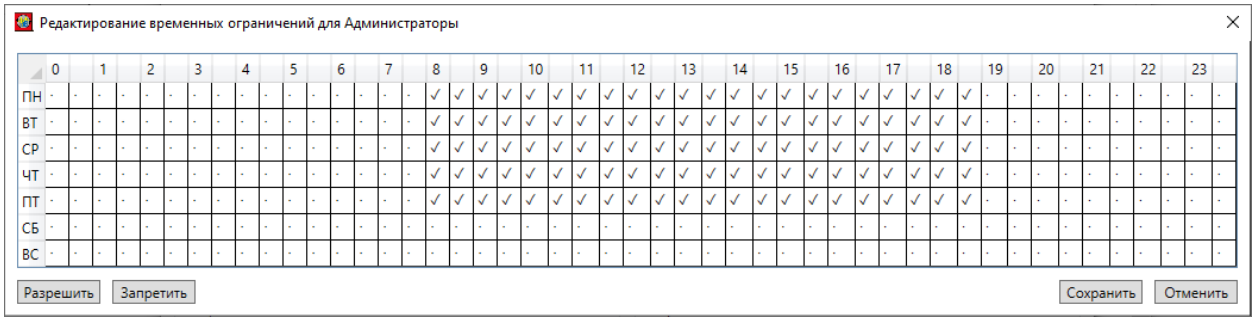



**Рисунок 40 – Окно редактирования временных ограничений**

В этом окне отображена таблица со строками, соответствующими дням недели, и столбцами, соответствующими временным промежуткам (часам). При помощи мыши можно выделить область редактирования. Для разрешения работы в выделенной области следует нажать кнопку <Разрешить>, при этом область заполнится символами √. Для запрета работы используется кнопка <Запретить>. При нажатии кнопки <Сохранить> временные ограничения устанавливаются в соответствующей строке окна редактирования пользователя (группы), как показано на рисунке 41.

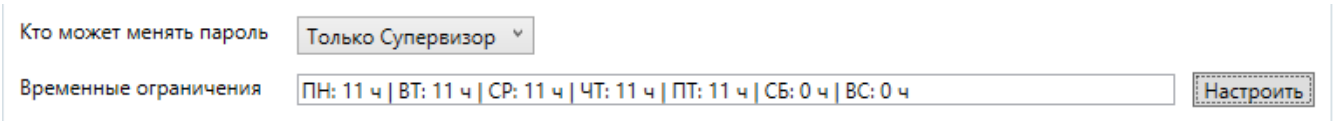



**Рисунок 41 – Установленные временные ограничения в окне редактирования группы**

В окне редактирования пользователя (рисунок 23) также отображается дата последнего входа пользователя, которую можно обнулить с помощью кнопки <Сбросить>. Если период времени, прошедший с этой даты, больше, чем заданный период неактивности (период задается в опциях программы настройки комплекса «Аккорд»), дата будет красного цвета.

## 3.14. Блокировка пользователя/группы

В поле «Вход в систему» окна редактирования пользователя (группы) находится флаг «Блокирован». При установке этого флага все параметры пользователя сохраняются в базе данных, но вход в систему и, соответственно, работа будут невозможны. Флаг можно использовать для временной блокировки. При снятии флага администратором работа пользователя восстановится с прежними настройками после перезагрузки компьютера.

## 3.15. Контроль доступа пользователя к рабочей станции

Флаг «Подконтрольный» в поле «Вход в систему» окна редактирования пользователя позволяет контролировать доступ пользователя к рабочей станции. Этот контроль осуществляет пользователь с привилегией «Контролер». Для входа в учетную запись пользователю с установленным флагом «Подконтрольный» помимо своего идентификатора и пароля

потребуется предъявление идентификатора и пароля пользователя с привилегией «Контролер».

Для включения опции «Подконтрольный» и, соответственно, запроса идентификатора Контролера при включении компьютера «с нуля» 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.

## 3.16. Коллективная работа

Для группы пользователей в окне редактирования группы можно установить флаг «Коллективная работа». Данный флаг определяет режим работы, при котором пользователи соответствующей группы могут разблокировать компьютеры друг друга. Так, если в группе с установленным флагом «Коллективная работа» состоят пользователи USER1 и USER2, а USER1 блокировал свой компьютер, то USER2 может разблокировать компьютер пользователя USER1 (пользователи должны знать пароли друг друга в ОС Windows). При этом в комплексе «Аккорд» будет начата новая сессия для USER2, а в ОС Windows сессия останется прежней.

Для корректной работы опции «Коллективная работа» необходимо, чтобы в параметре «Гашение экрана» был установлен флаг «Защита паролем».

## 3.17. Установка стартовой задачи

Стартовая задача – исполняемый файл, который запускается для пользователей группы после старта операционной системы в качестве программной оболочки. При этом пользователи могут работать только в загруженной программной среде (рабочий стол Windows, кнопка <Пуск> и панель задач на экран не выводятся). Выбрать исполняемый файл можно в поле «Программная среда» окна редактирования группы при нажатии кнопки <Выбрать> в строке «Стартовая задача». В случае, когда пользователям в рамках их 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».

### 3.17.1. Подготовка файла .act для стартовой задачи AcTskMng.exe

Для успешной работы программы AcTskMng.exe необходимо создать текстовый файл – список задач, разрешенных для запуска пользователям группы. Имя этого файла должно совпадать с именем группы, расширение файла должно быть .act.

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

```
[Group1]
GroupName=File managers
Expand=Yes
[Task1.1]
DisplayName=Notepad1
ImagePath=C:\windows\system32\notepad.exe
WaitEndTask=Yes
[Group1.1]
GroupName=File managers1
Expand=Yes
[Task1.1.1]
DisplayName=FAR Manager1
ImagePath=C:\PROGRA~1\Far.x32\Far.exe
[Task1.2]
DisplayName=Notepad1
ImagePath=C:\windows\system32\notepad.exe
WaitEndTask=Yes
[Task1.1.2]
DisplayName=Volcov Commander1
ImagePath=c:\vc\vc.com
[Task1.4]
DisplayName=Notepad4
ImagePath=C:\windows\system32\notepad.exe
WaitEndTask=Yes
[Task1.3]
DisplayName=Notepad3
ImagePath=C:\windows\system32\notepad.exe
WaitEndTask=Yes
[Group1.2]
GroupName=File managers2
Expand=Yes
[Task1.2.1]
DisplayName=FAR Manager2
ImagePath=C:\PROGRA~1\Far.x32\Far.exe
[Task1.2.2]
DisplayName=Volcov Commander2
ImagePath=c:\vc\vc.com
```

```
[Group2]
GroupName=Язык и региональные стандарты
Expand=Yes
[Task2.1]
DisplayName=Язык
ImagePath=rundll32.exe
Parameters=shell32.dll,Control_RunDLL intl.cpl
WorkDir=c:\windows\system32\
WaitEndTask=Yes
[Task2.2]
DisplayName=Язык Link
ImagePath=c:\link.lnk
WorkDir=c:\
WaitEndTask=No
```

Параметр Expand со значением Yes показывает содержимое группы в Менеджере задач, при этом обладает большим приоритетом, чем подобный параметр в файле запуска Actskmng.ini.

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 подготовки файла .act и указании в качестве стартовой задачи программы AcTskMng.exe при старте монитора разграничения доступа запустится оболочка AcTskMng со списком программ, доступных для выполнения пользователям редактируемой группы.

До выбора конкретной стартовой задачи кнопка <Запуск> в окне Менеджера задач остается неактивной.

При нажатии кнопки <Пуск> на экране появляется меню, в котором пользователю доступны кнопки завершения работы, перезагрузки и завершения сеанса, информация о программе, а также кнопка включения блокировки экрана (Screen Saver). Если AcTskMng.exe запускается в терминальной сессии пользователя, то кнопки <Завершение работы> и <Перезагрузка> будут заблокированы. 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» появляется информация о программе, а также информация о сессии пользователя (версия драйвера разграничении доступа, дата и время начала сессии пользователя, имя пользователя, дата и время завершения сессии пользователя - если для пользователя установлены временные ограничения).

Обратите внимание, что 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 и/или дискреционного механизма доступа с контролем процессов и динамического контроля целостности файлов из этого списка, как используя, так и не используя утилиту Actskmng.exe.

## 3.18. Контроль целостности

Комплекс СЗИ НСД «Аккорд-Win32» позволяет контролировать целостность файлов и параметров реестра по списку, созданному администратором для каждой группы пользователей. Предусмотрены два режима контроля:

статический - контроль целостности любых объектов, расположенных на жестком диске в момент начала сеанса пользователя и обновление контрольных сумм при завершении сеанса работы пользователя;

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

### 3.18.1. Создание списка контроля целостности в статическом режиме

Для создания списка контролируемых объектов в окне редактирования группы в поле «Контроль целостности» следует нажать кнопку <Настроить>. Появится окно редактирования контроля целостности объектов для группы (рисунок 42, рисунок 43).

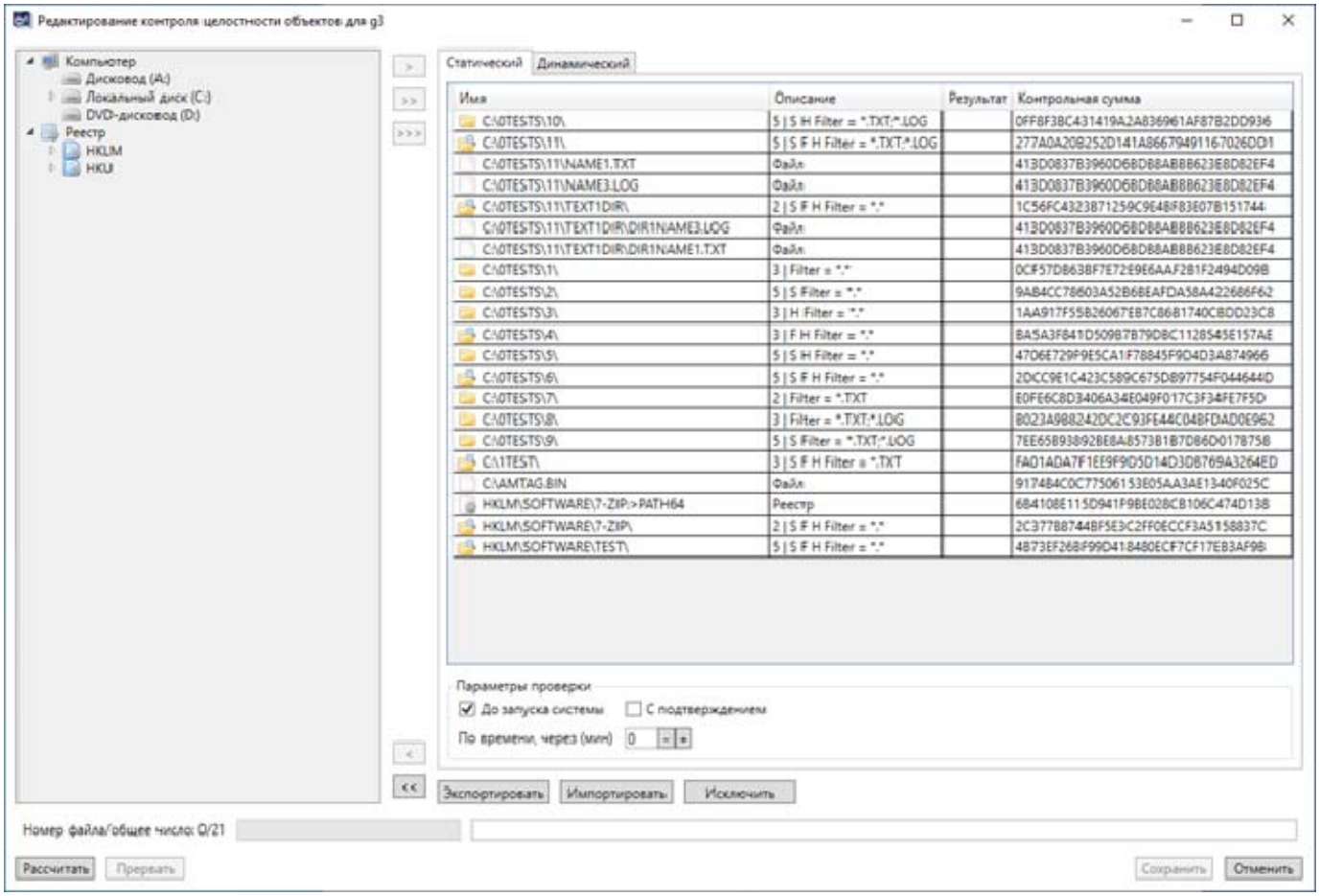



**Рисунок 42 – Окно редактирования списка контроля целостности объектов. Вкладка «Статический», выбор файлов.**

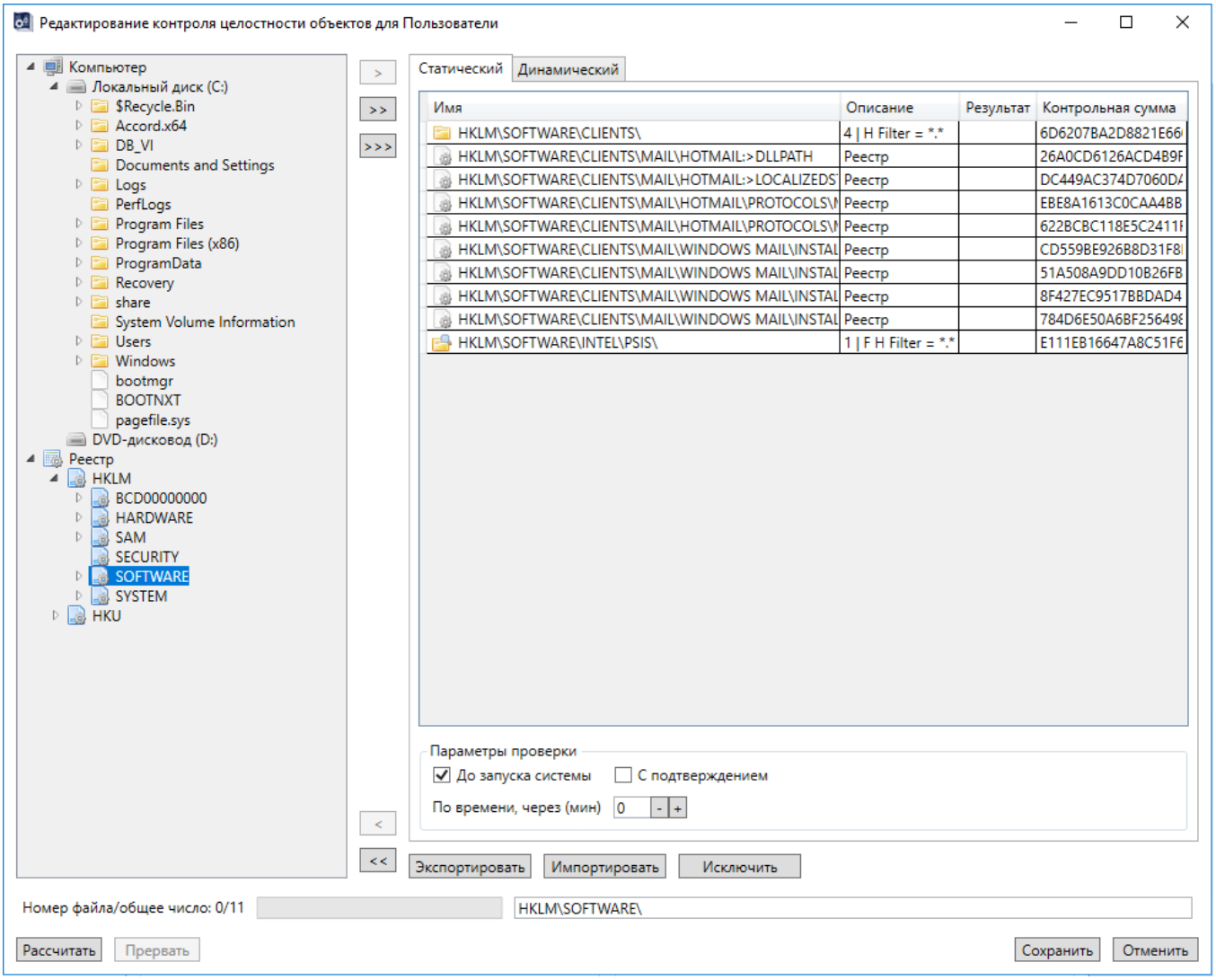



**Рисунок 43 - Окно редактирования списка контроля целостности объектов. Вкладка «Статический», выбор параметров реестра.**

На первом этапе необходимо сформировать список объектов, для которых будет рассчитана контрольная сумма (КС). Возможен выбор отдельного объекта, всех объектов выделенного каталога или самого каталога (включая подкаталоги).

В левой половине окна представлен древовидный список объектов на всех дисках компьютера. Отмеченный мышью объект переместится в правую часть окна (в список контролируемых) при двойном щелчке мыши или при нажатии на кнопку «>». При выборе каталога и нажатии на кнопку «>>» в список контролируемых переместятся все объекты данного каталога.

Список контролируемых объектов можно сформировать в виде контейнера с заданными параметрами. Для создания контейнера следует выделить объект (в качестве объекта может выступать корневой каталог логического раздела жесткого диска или отдельный каталог) и нажать кнопку «>>>». Появляется окно, в котором есть возможность задать маску по расширению файлов и выбрать следующие опции: «Включая подкаталоги», «Включая контроль содержимого объекта», «Включая полные имена файлов». (рисунок 44).

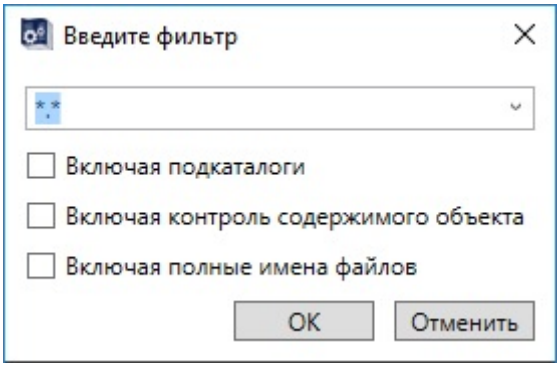



**Рисунок 44 – Задание фильтра для создания контейнера объектов**

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

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

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

При использовании режима контроля целостности контейнера объектов следует учитывать, что при установке полного контроля, например, на папку Windows время расчета хэш-функции нескольких тысяч файлов будет значительным, и пользователь вряд ли сможет нормально работать на компьютере, защищенном подобным образом, ибо операционная система при работе создает временные файлы, и при каждом новом сеансе будет выявлено нарушение целостности.

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

Очистить список контролируемых объектов можно кнопкой «<<», удалить отдельный (выделенный) объект списка - кнопкой «<».

На втором этапе осуществляется установка режимов контроля целостности.

Выбор режимов осуществляется установкой флагов в поле «Параметры проверки». Возможны следующие варианты:

- «До запуска системы» - контроль целостности до запуска операционной системы.
- «С подтверждением» - запрос подтверждения контроля целостности до запуска ОС (пользователь может отказаться от выполнения процедуры контроля).
- «По времени через, мин.» - 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, то процедура контроля целостности осуществляется по истечении интервала.

На третьем этапе производится расчет КС выбранных объектов при нажатии кнопки <Рассчитать>.

Еще раз обратите внимание на последовательность процесса создания списка контролируемых объектов, так как расчет КС будет невозможен без определения параметров режима контроля, а при попытке рассчитать контрольную сумму без установки параметров появится сообщение об ошибке.

Выход из процедуры контроля с сохранением результатов расчета осуществляется по кнопке <Сохранить> (<F2>), без сохранения – по кнопке <Отменить> (<Esc>), а по кнопке <Прервать> расчет КС останавливается, и кнопка <Сохранить> становится неактивной.

### 3.18.2. Создание списка контроля целостности в динамическом режиме

Эта операция выполняется при каждом запуске процесса (исполняемого модуля). Для создания списка контролируемых процессов в окне редактирования группы в поле «Контроль целостности» следует нажать кнопку <Настроить>. Появится окно редактирования контроля целостности объектов для группы. При щелчке мышью на закладке «Динамический» правого окна откроется список файлов для динамического контроля (рисунок 45).

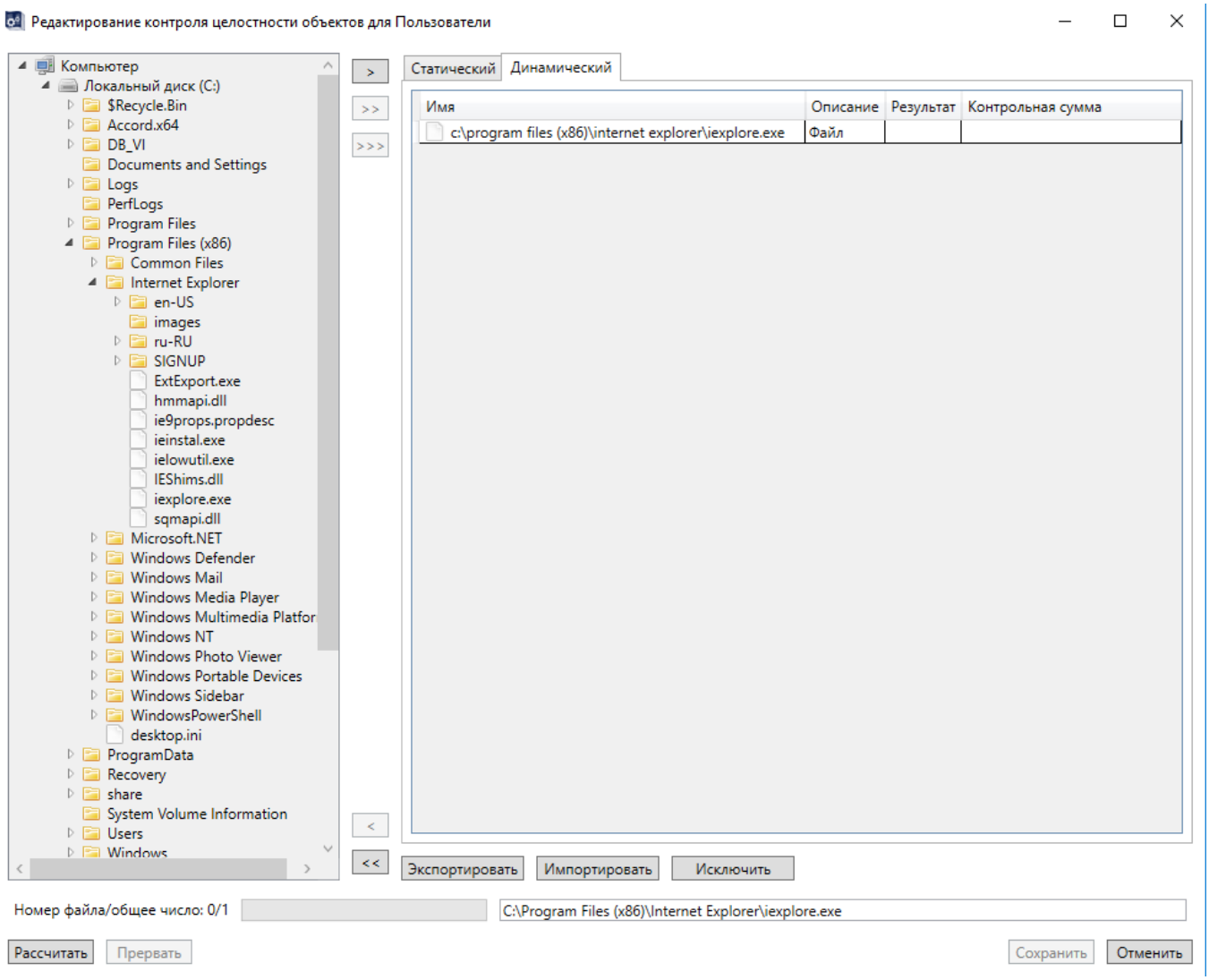



**Рисунок 45 – Окно редактирования списка контроля целостности объектов. Вкладка «Динамический»**

С этим списком можно работать так же, как и со статическим, при этом не требуется задания параметров проверки.

### 3.18.3. Экспорт и импорт списков контроля целостности

Как в статическом, так и в динамическом режиме контроля целостности есть возможность экспорта/импорта списка контролируемых файлов в виде специального файла с расширением hsh. Этот файл можно использовать на других защищаемых СВТ с идентичным составом прикладного ПО (с обязательным пересчетом контрольных сумм после импорта).

Формат содержимого файла *.hsh имеет следующий вид:

```
---Статический список----
Контрольная сумма объекта:                    Имя объекта:
[413D0837B3960D6BDB8ABBB623E8D82EF4] C:\0TESTS\11\NAME1.TXT
[413D0837B3960D6BDB8ABBB623E8D82EF4] C:\0TESTS\11\NAME3.LOG
[413D0837B3960D6BDB8ABBB623E8D82EF4] C:\0TESTS\11\TEXT1DIR\DIR1NAME3.LOG
```

[413D0837B3960D6BDB8ABBB623E8D82EF4] C:\0TESTS\11\TEXT1DIR\DIR1NAME1.TXT
[9174B4C0C77506153E05AA3AE1340F025C] C:\AMTAG.BIN
[6B4108E115D941F9BE028CB106C474D138] HKLM\SOFTWARE\7-ZIP:>PATH64
[0FF8F3BC431419A2A836961AF87B2DD936] C:\0TESTS\10\ <S H|*.TXT;*.LOG>
[277A0A20B252D141A86679491167026DD1] C:\0TESTS\11\ <SFH|*.TXT;*.LOG>
Параметры проверки
До запуска системы

В общем случае каждая строка списка содержит контрольную сумму и имя объекта. Для контейнера после имени объекта в угловых скобках перечислены его внутренние настройки. После списка указаны параметры контрольной проверки.

Для наиболее часто используемых каталогов предусмотрены следующие короткие обозначения (псевдонимы):

#W: - Windows

#S: - Windows\System32

#D: - Windows\System32\Drivers

#P: - Program Files

#A: - Accord.X32

И если при экспорте списка контролируемых файлов (кнопка <Экспортировать>, рисунок 42) согласиться с использованием псевдонимов (рисунок 46), то, например, файл c:\windows\system32\drivers\d.txt будет внесен в список с именем #D:d.txt.

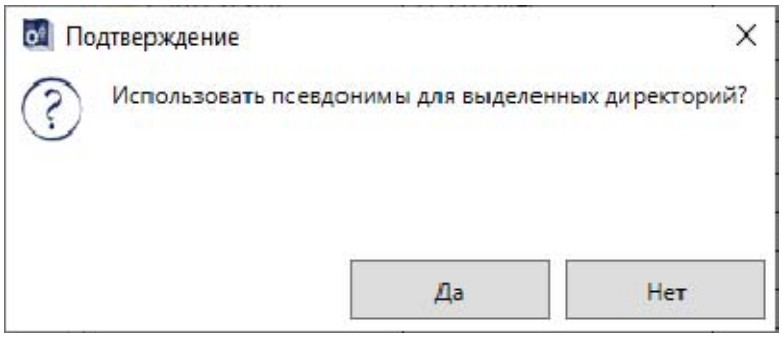



**Рисунок 46 – Предложение использовать псевдонимы при экспорте списка контролируемых файлов**

При нажатии кнопки <Импортировать> (рисунок 42) откроется окно импорта контролируемых объектов (рисунок 47). В окне отображается список объектов контроля из файлов *.hsh, с помощью которого можно отредактировать существующий список. Так, можно добавить выбранные объекты в список при выборе режима «Объединить» (при совпадении имен существующие параметры контейнеров останутся без изменений) или полностью очистить текущий список и заполнить его выбранными объектами (режим «Заменить»).

При нажатии кнопки <Исключить> (рисунок 42) можно убрать выбранные имена из имеющегося списка, если они там есть.

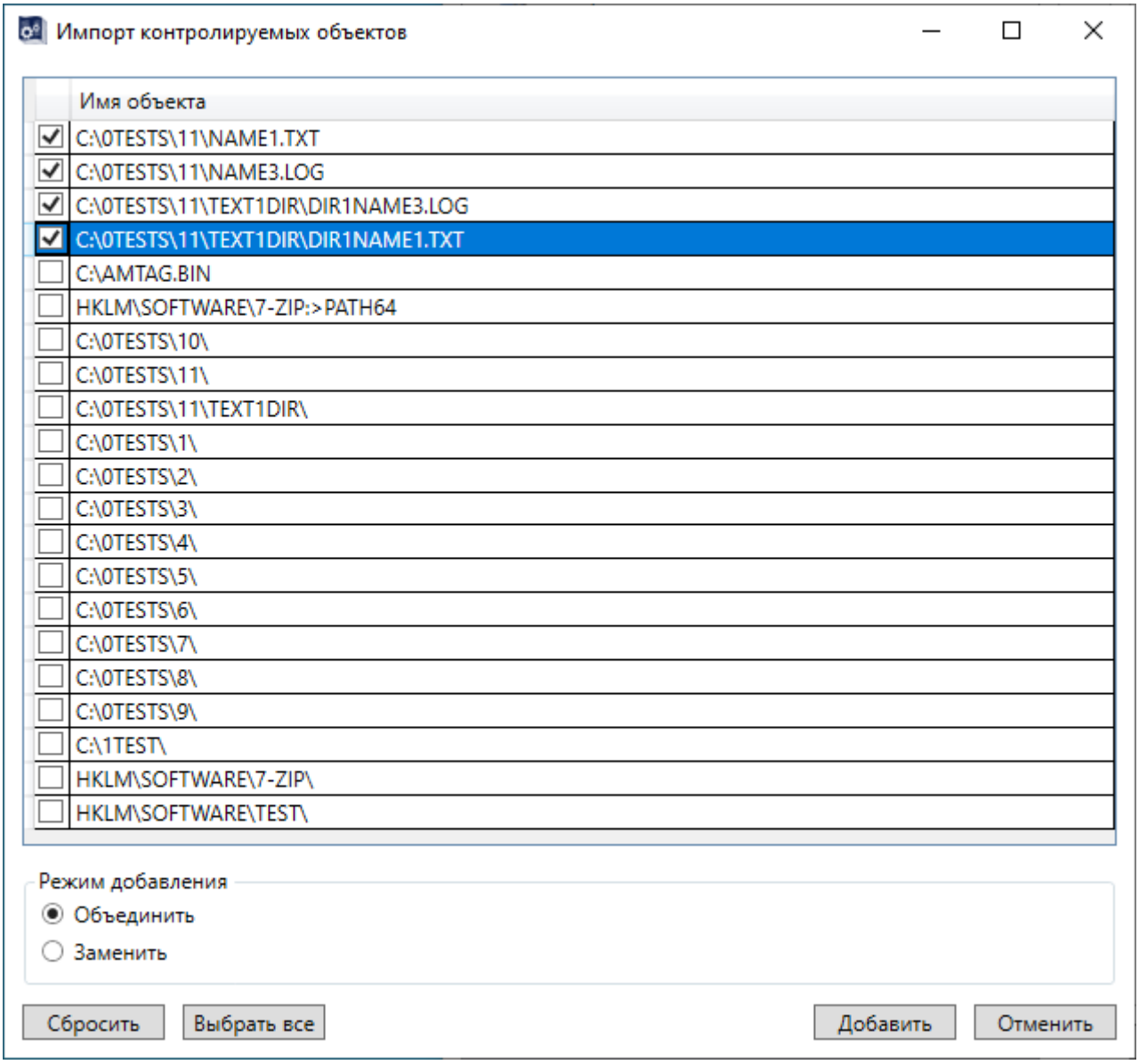



**Рисунок 47 – Окно импорта списка контролируемых файлов**

## 3.19. Установка правил разграничения доступа к объектам

СЗИ НСД «Аккорд» поддерживает два типа управления правилами разграничения доступа (ПРД):

- дискреционный механизм ПРД;
- мандатный механизм ПРД.

Система атрибутов доступа и особенности ее реализации описаны в «Руководстве администратора» (11443195.4012-036 90). Можно использовать отдельно каждый механизм управления или задать комбинированную политику безопасности с применением обоих механизмов ПРД.

Выбор механизма управления ПРД осуществляется:

- установкой соответствующих флагов («Дискреционный», «Мандатный», «Контроль процессов») в программе настройки комплекса «Аккорд» – ACSETUP.EXE, 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 1).

### 3.19.1. Установка доступа к объектам с использованием дискреционного метода ПРД

Включить дискреционный механизм задания и контроля ПРД можно в программе настройки комплекса «Аккорд» при установке в ее главном окне флага «Дискреционный».

Установка ПРД выделенной группы начинается при нажатии кнопки <Настроить> поля «Разграничение доступа» окна редактирования группы - появляется окно с правами доступа пользователей группы к ресурсам СВТ (рисунок 48). Вкладка «Процессы» в этом окне появляется при установке флага «Контроль процессов» в главном окне программы AcSetup.

По умолчанию в этом окне выведен перечень всех доступных корневых каталогов (для сетевых корневых каталогов указано полное сетевое имя). В этом окне нет деления на диски, каталоги, файлы и т. д., а ведется один общий список объектов. Для запрета доступа к логическому диску достаточно исключить корневой каталог этого диска из списка объектов, используя кнопку <Удалить>. 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.

В список объектов уже включены определенные ограничения, которые защищают от модификации программные компоненты комплекса «Аккорд». Просмотреть и отредактировать присвоенные атрибуты доступа к отдельному объекту можно по кнопке <Редактировать>. Окно редактирования этих атрибутов изображено на рисунке 49.

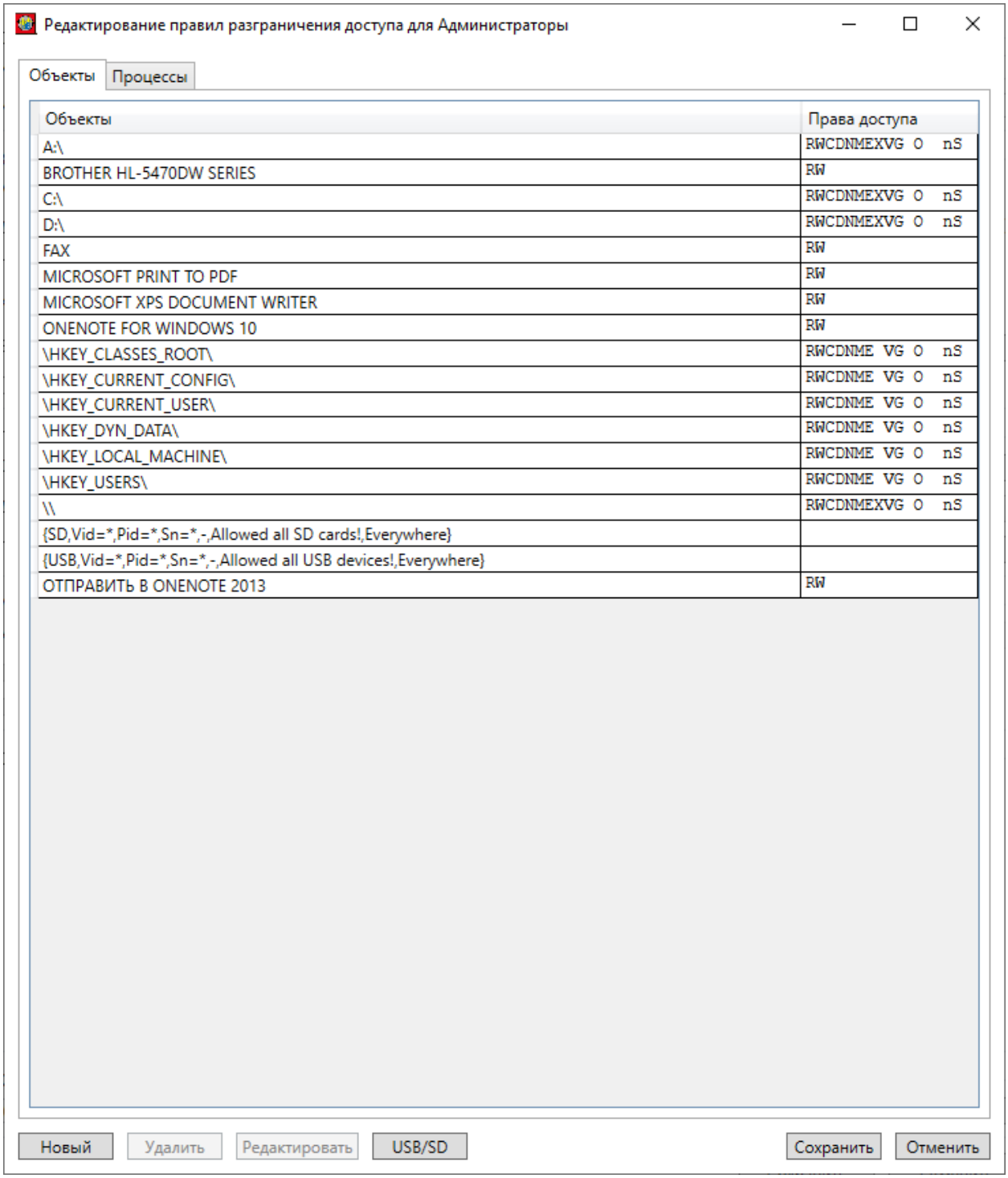



**Рисунок 48 – Окно с правами доступа к ресурсам СВТ**

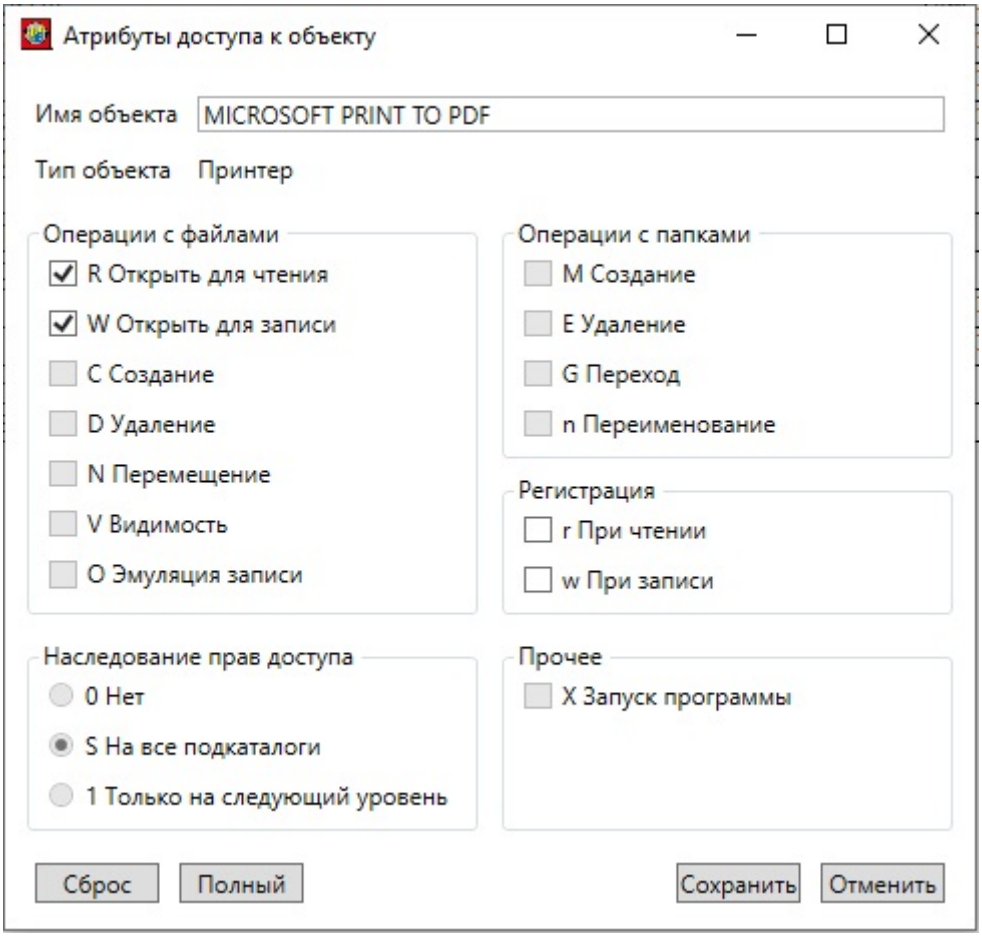



**Рисунок 49 – Окно редактирования ПРД к объекту**

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 пользователю желательно разрешить только просмотр файла.
2. Операции с папками:
   - 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, по сути, 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.

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

Параметр наследования прав доступа может принимать три значения:

- 0 - параметры доступа текущего каталога не наследуются подкаталогами;
- 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.

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 определяются 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 в окне со списком объектов (рисунок 48) необходимый объект отсутствует, при нажатии кнопки <Новый> выведется расширенное окно атрибутов доступа к объекту (рисунок 50), в котором отображен список всех объектов СВТ.

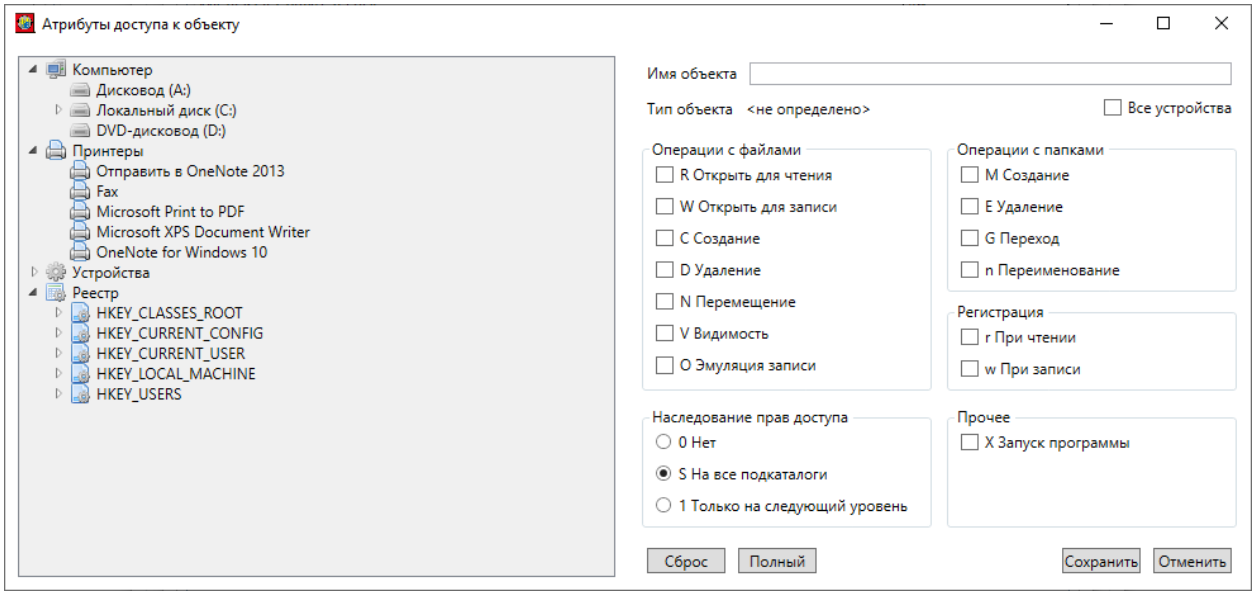



**Рисунок 50 – Окно добавления новых ПРД к объекту**

В поле «Имя объекта» можно вручную ввести имя и установить для него необходимые атрибуты. С помощью мыши также можно выбрать имя объекта в дереве объектов, и 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.

Для сохранения изменений ПРД выделенного объекта следует нажать кнопку <Сохранить>. Более подробно действие атрибутов доступа и их комбинаций описано в документе «Руководство администратора».

#### *3.19.1.1. Формирование списка разрешенных USB- и SD-устройств*

При формировании списка разрешенных съемных устройств необходимо учитывать, что после включения устройства в список следует описать правила доступа к тому логическому съемному диску, который монтируется в системе после подключения физического устройства к компьютеру. Если такую операцию не выполнить, съемный диск останется недоступным после подключения к компьютеру, т.к. все логические диски, не включенные в список ПРД, запрещены.

В список объектов редактирования ПРД (рисунок 48) по умолчанию включены записи «USB, Vid=*, Pid=*, Sn=*, -, Allowed all USB devices!, Everywhere» и «SD, Vid=*, Pid=*, Sn=*, -, Allowed all SD cards!, Everywhere». Это означает, что любое USB- и Secure Digital-устройство разрешено для доступа. Если необходимо назначить конкретные устройства, доступ к которым будет разрешен, в окне редактирования ПРД следует нажать клавишу <USB/SD>. Откроется окно редактирования списка съемных устройств (рисунок 51).

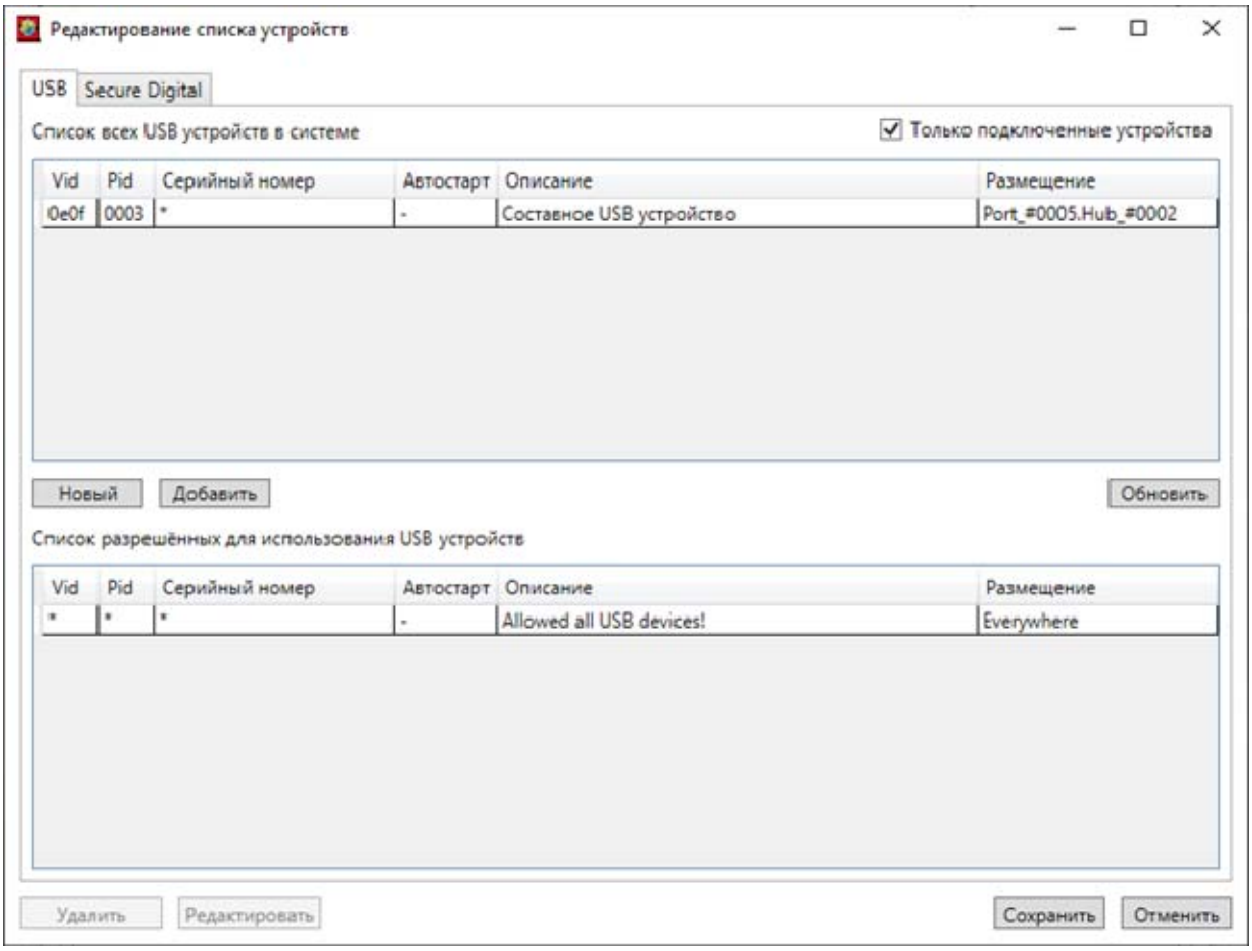



**Рисунок 51 - Окно редактирования списка USB- и SD-устройств**

В верхней части этого 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 устройств, то по кнопке <Обновить> следует выполнить поиск подключенных устройств, результатом которого станет обновленный список в верхней части окна. При установке курсора на устройство, доступ к которому должен быть разрешен для конкретного пользователя, и нажатии кнопки <Добавить> отмеченное устройство появляется в нижней половине окна в списке разрешенных для использования. Кнопка <Новый> открывает окно редактирования, изображенное на рисунке 52. При необходимости изменения отдельной позиции нижнего списка следует использовать кнопку <Редактировать>.

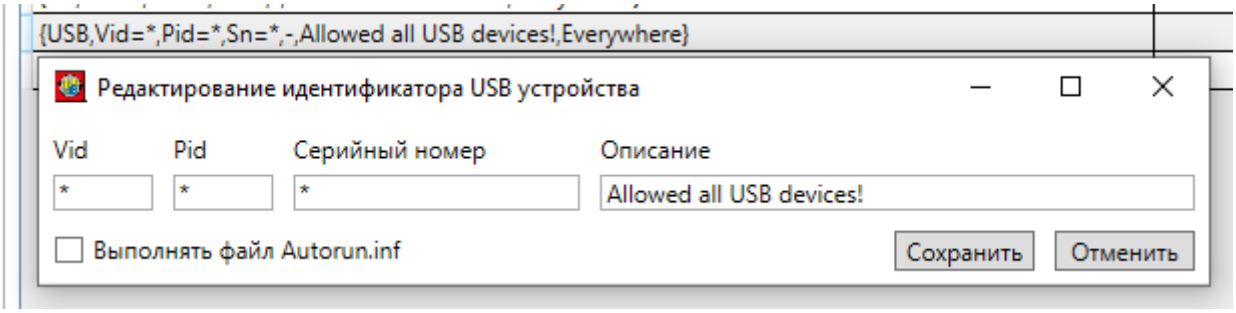



**Рисунок 52 – Окно редактирования настроек ПРД USB- и SD-устройств**

По кнопке <Сохранить> устройство появляется в списке объектов ПРД (рисунок 48).

При формировании списка разрешенных устройств можно использовать режим добавления, 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 точно известен серийный номер того устройства, доступ к которому будет разрешен.

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 порту USB, то в списке устройств в ОС отображается только одно устройство, а серийные номера карт будут недоступны. Администратор не сможет формировать список SD-карт по уникальным номерам. Поэтому в системах, в которых обрабатывается конфиденциальная и секретная информация, следует избегать подключения считывателя карт через USB.

### 3.19.2. Установка доступа к объектам с использованием механизма мандатных меток ПРД

Включить мандатный механизм задания и контроля ПРД можно в программе настройки комплекса «Аккорд» (AcSetup) при установке в ее главном окне флага «Мандатный». Редактирование мандатных политик, а также их импорт и экспорт через файлы *.prd доступны при выполнении команды «Мандатные метки» контекстного меню главного окна программы AcedVI.

Выбор опции «Редактировать» этой команды открывает окно установки меток мандатного доступа (рисунок 53). В этом окне выведен общий список объектов, в который уже включены определенные ограничения для программных компонентов комплекса «Аккорд». Просмотреть и отредактировать присвоенные атрибуты доступа отдельному объекту можно кнопкой <Редактировать> (рисунок 54), исключить объект из списка - кнопкой <Удалить>. Если необходимый объект отсутствует, при нажатии кнопки <Новый> выведется расширенное окно атрибутов доступа к объекту (рисунок 55), в котором будет отображен список всех объектов СВТ.

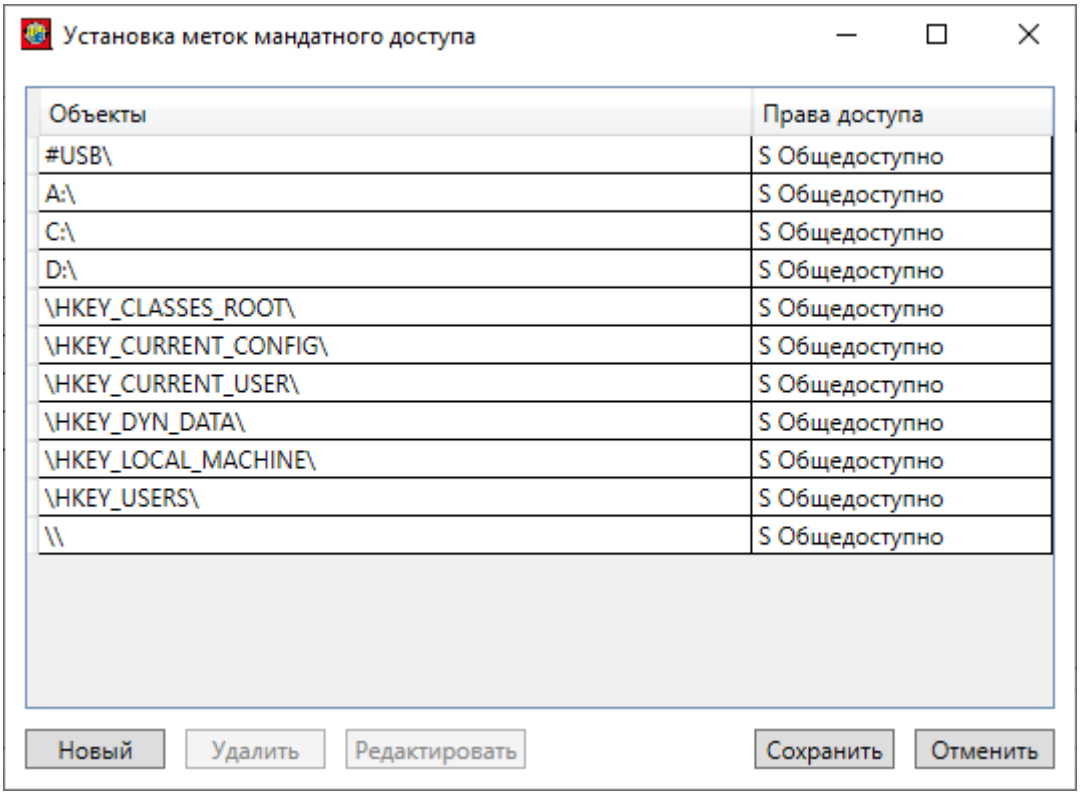



**Рисунок 53 – Окно установки меток мандатного доступа**

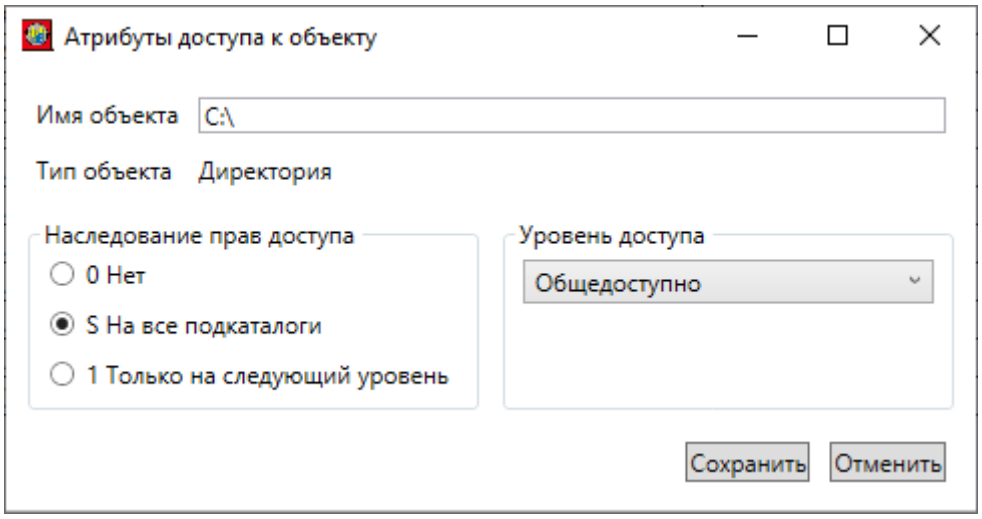



**Рисунок 54 – Редактирование отдельной мандатной метки**

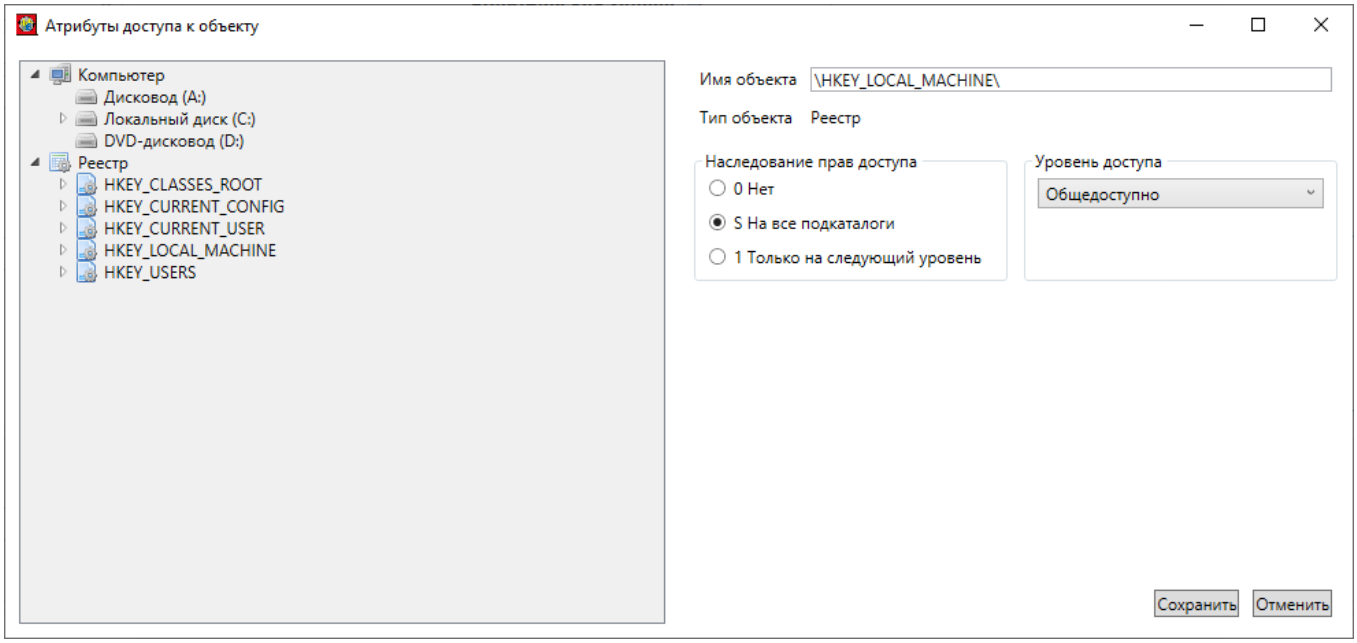



**Рисунок 55 – Установка новой метки мандатного доступа**

Для импорта/экспорта мандатных меток используется соответствующая команда меню «Мандатные метки» или команда импорта (экспорта) настроек из (в) *.prd контекстных меню списков групп/пользователей. При импортировании после выбора файла *.prd появляется окно импорта настроек (рисунок 56), в котором отмечены все параметры импортируемого файла.

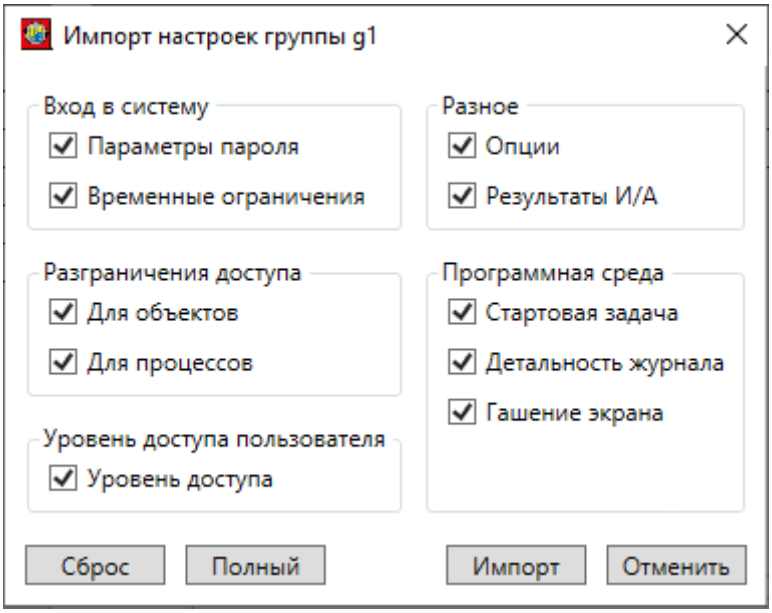



**Рисунок 56 – Окно импорта настроек ПРД в выделенную группу**

В этом окне можно выбрать необходимые для импорта параметры. При отметке в поле «Разграничение доступа» параметра «Для объектов» появится еще одно окно (рисунок 57), в котором можно выбрать конкретные объекты и режимы их импортирования.

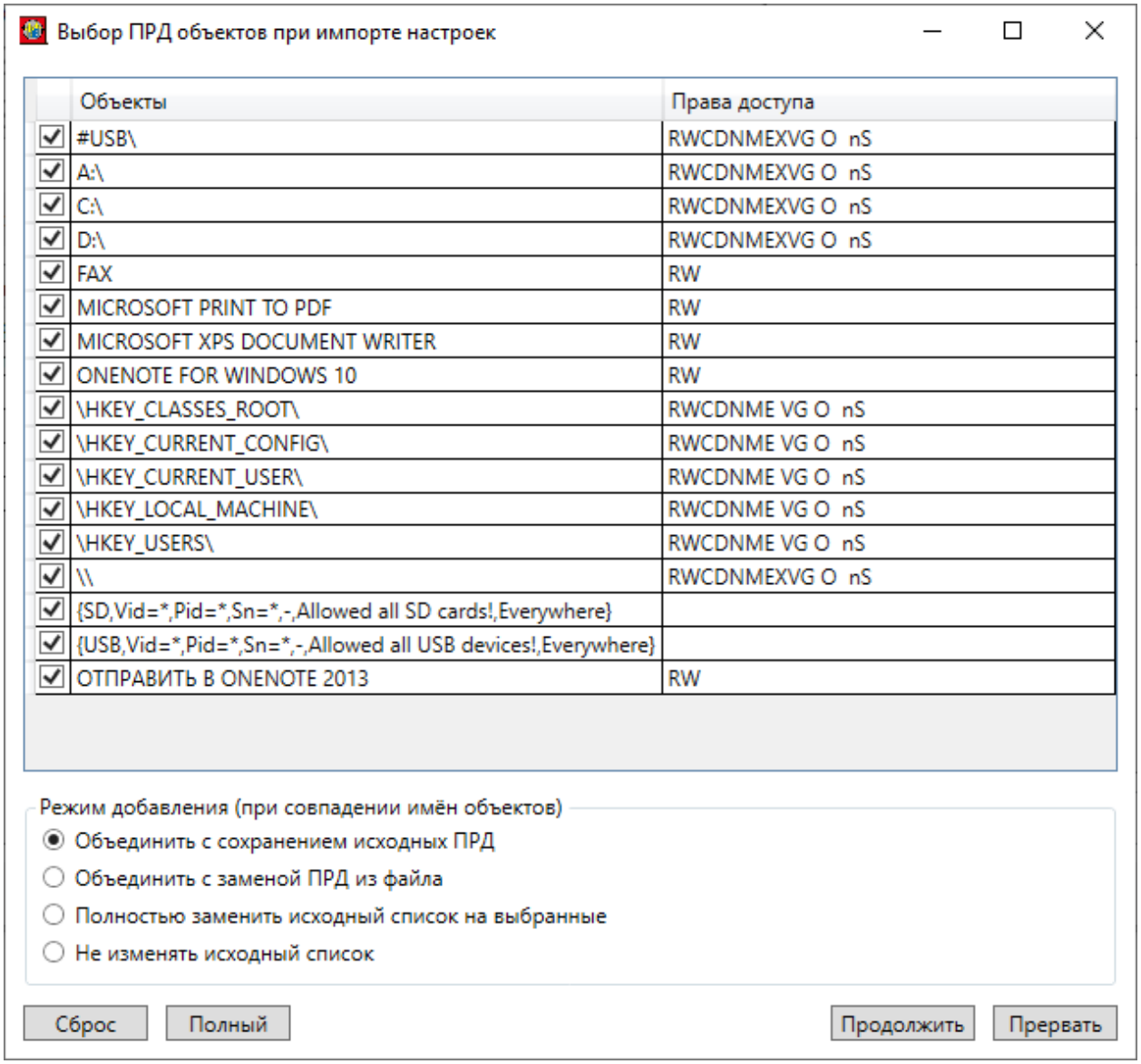



**Рисунок 57 – Окно выбора конкретных объектов для импортирования и режимов их добавления (в том числе при совпадении имен)**

Импорт может быть осуществлен в одном из четырех режимов:

1. «Объединить с сохранением исходных ПРД». Режим установлен по умолчанию. Если среди выбранных для импорта объектов нет совпадающих по имени с объектами в БД, то все настройки будут импортированы с указанными в записи ПРД. В случае совпадения имен объектов с существующими в БД настройки этих объектов изменены не будут, а все остальные объекты будут импортированы с указанными в записи ПРД настройками.
2. «Объединить с заменой ПРД из файла». Если среди выбранных для импорта объектов нет совпадающих по имени с объектами в БД, то настройки будут импортированы с указанными в записи ПРД. В случае совпадения имен объектов с существующими в БД настройки будут перезаписаны.
3. «Полностью заменить исходный список на выбранные». В этом режиме исходный список настроек будет полностью очищен и далее создан

заново из настроек ПРД выбранных записей. Если не окажется отмеченных записей, список все равно будет очищен без добавления новых записей.

4. «Не изменять исходный список». Имеющийся список не будет изменен. Все выбранные записи будут проигнорированы.

Процесс импортирования настроек выбранных (отмеченных галочками в первом столбце) объектов начинается при нажатии кнопки <Продолжить>.

По кнопке <Прервать> импорт (в том числе параметры импортируемого файла) будет полностью отменен, и в итоге настройки выделенной группы останутся без изменений.

Аналогично выбору объектов, при отметке в поле «Разграничение доступа» параметра «Для процессов» появится окно выбора конкретных процессов и режимов их добавления (рисунок 58).

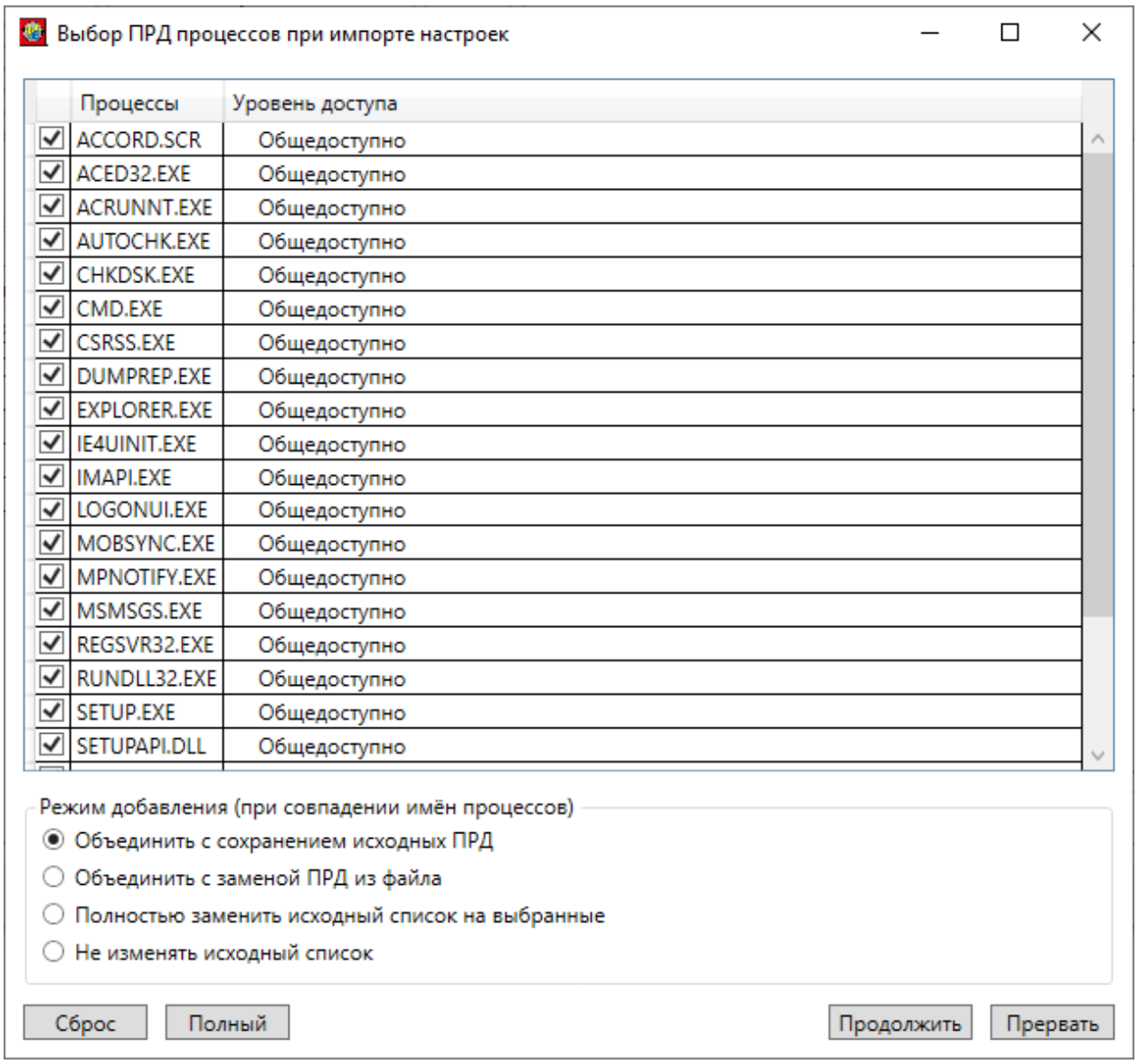



**Рисунок 58 - Окно выбора конкретных процессов для импортирования и режимов их добавления при совпадении имен**

### 3.19.3. Настройка механизма ПРД для процессов

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

1) запустить программу «Настройка комплекса «Аккорд» (исполняемый файл ACSETUP.EXE или Пуск–> Программы–> Аккорд–> Настройка комплекса Аккорд);

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

3) завершить работу приложения с сохранением изменений.

После включения в программе AcSetup механизма разграничения доступа для процессов в окне с правами доступа пользователей группы к ресурсам СВТ появляется закладка «Процессы» (рисунок 59).

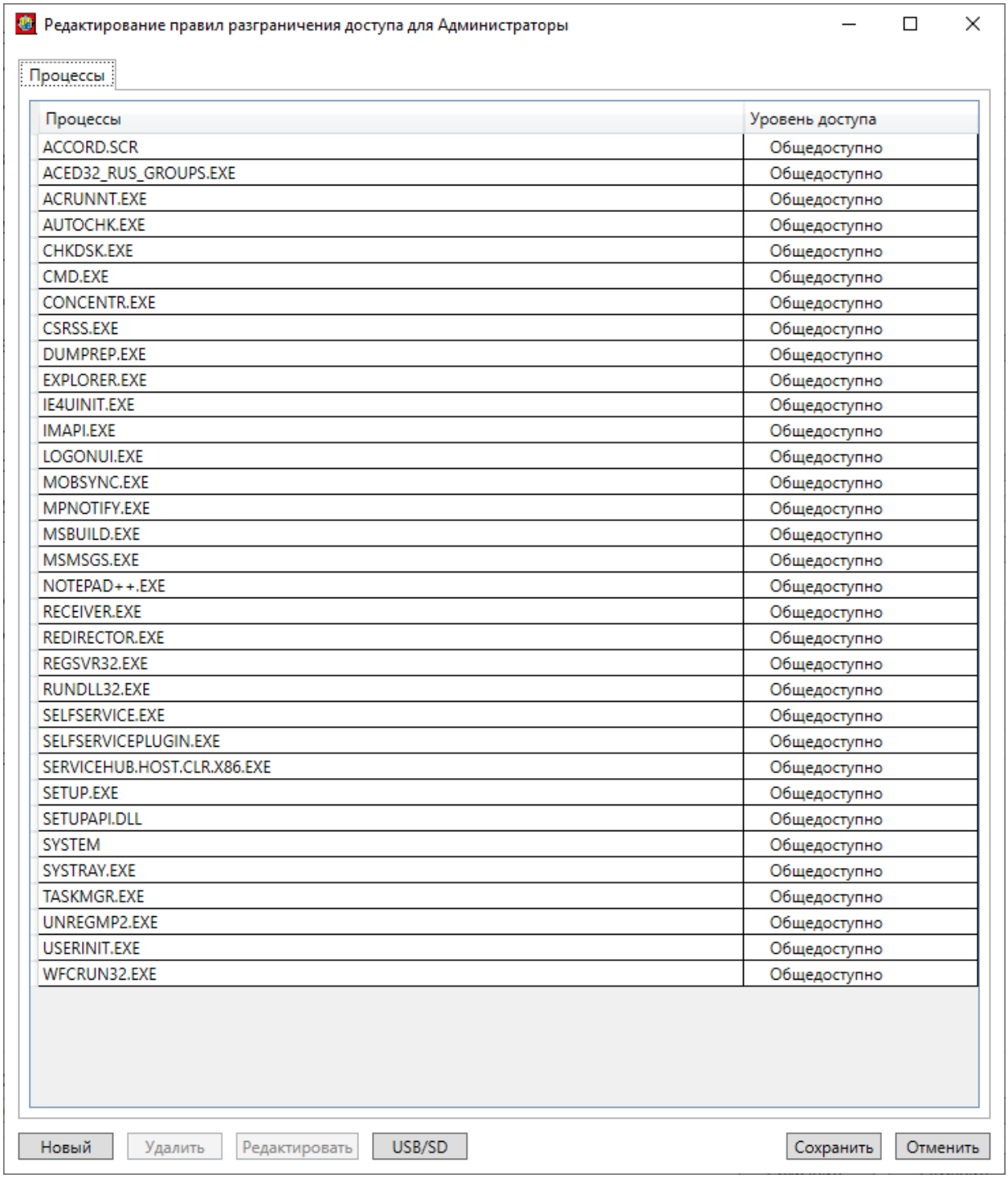



**Рисунок 59 – Закладка «Процессы» окна ПРД пользователей группы к ресурсам СВТ**

При первом запуске программы в список процессов заносятся все процессы, которые в данный момент находятся в оперативной памяти.

Для изменения уровня доступа процесса следует выбрать строку с нужным именем и нажать кнопку <Редактировать> - появится окно установки уровня доступа процесса (рисунок 60). Это же окно появляется при нажатии кнопки <Новый> и позволяет добавить в список новый процесс, отсутствующий в общем списке.

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.

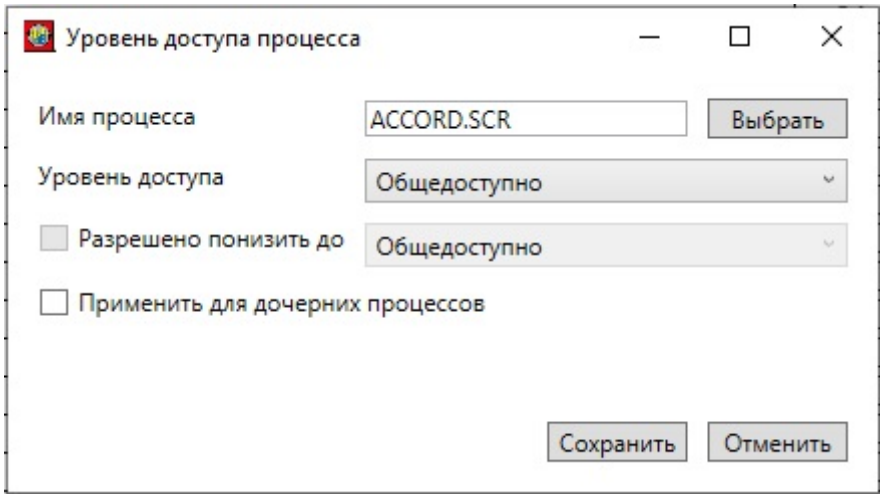



**Рисунок 60 – Окно редактирования ПРД процесса**

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[5].

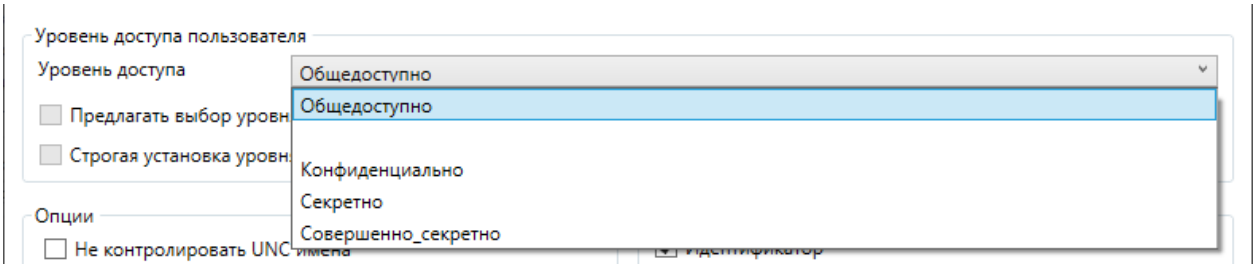
Флаг «Применить для дочерних процессов» предназначен для того, чтобы при присвоении родительскому процессу определенного уровня доступа дочерним процессам автоматически присваивался такой же уровень доступа, как и у родительского (так как присвоение одного и того же уровня доступа большому количеству 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 до». Если этот флаг установлен, то при старте такого процесса выводится окно выбора текущего уровня процесса (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.

Еще один вариант работы с разными уровнями процессов – это выбор уровня доступа сессии пользователя.

---

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




При задании уровня доступа пользователя (одноименное поле на рисунке 23) Администратор БИ может установить флаги «Предлагать выбор уровня конфиденциальности сессии» и «Принудительно устанавливать уровень сессии». Эти флаги доступны только при включенном механизме контроля процессов (при уровне доступа, отличном от значения «Общедоступно»), при этом флаг «Принудительно устанавливать уровень сессии» доступен только при установке флага «Предлагать выбор уровня конфиденциальности сессии».

Если не включен флаг «Принудительно устанавливать уровень сессии», то пользователь в процессе работы выбирает уровень отдельных программ при их запуске - фиксируется уровень процессов, для которых Администратор включил флаг «Разрешено понизить пользователю», только на уровне сессии. Для остальных процессов уровни доступа не меняются и будут соответствовать фиксированным значениям, прописанным в списке процессов редактора ПРД.

При включении флага «Принудительно устанавливать уровень сессии» 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.

## 3.20. Установка опций настройки

В поле «Опции» окна редактирования параметров пользователя/группы (рисунок 23) отображается информация о дополнительных опциях настройки системы «Аккорд» у выделенного пользователя/группы.

Поле содержит следующие опции:

- «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 параметр уточняет, разрешать ли полный доступ к файлам и папкам данного компьютера администратору безопасности информации;
- «Проверять доступ к реестру» - параметр уточняет, использовать ли разграничение доступа к разделам и ключам системного реестра.

## 3.21. Установка фиксированных сетевых имен ресурсов общего пользования

Локальные ресурсы отдельного СВТ можно выделить в общее пользование для других СВТ локальной вычислительной сети.

Для вызова этой функции следует выбрать в главном меню команду "Сетевые ресурсы" > "Редактировать" (рисунок 61). Откроется окно, представленное на рисунке 62.

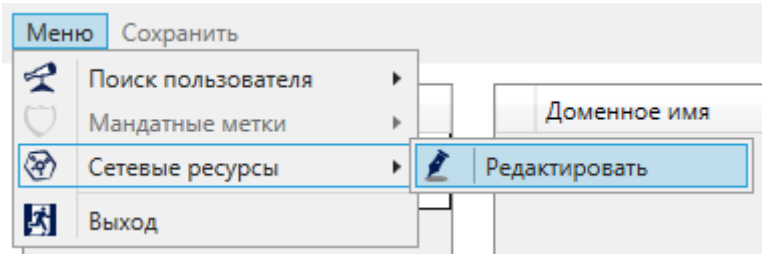



**Рисунок 61 – Запуск редактирования сетевых ресурсов**

В этом списке можно описать ресурсы (с полным именем), которые находятся на жестком диске отдельного СВТ, и задать сетевое имя, под которым ресурс будет доступен другим пользователям в сети. Сетевое имя объекта можно редактировать (кнопка <Редактировать>). Можно добавить новый ресурс в список (кнопка <Создать>) или удалить ранее введенный (кнопка <Удалить>).

При использовании этой функции 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. Фиксированное сетевое имя необходимо, поскольку в сети могут функционировать другие СВТ, на которых описан доступ к сетевым ресурсам, и в этом случае политика безопасности обеспечивается проверкой доступа к ресурсу по полному сетевому пути.

Если производится попытка предоставить общий доступ ресурсу, не указанному в списке имен общих сетевых ресурсов, то такое действие заносится в журнал регистрации событий как попытка НСД.

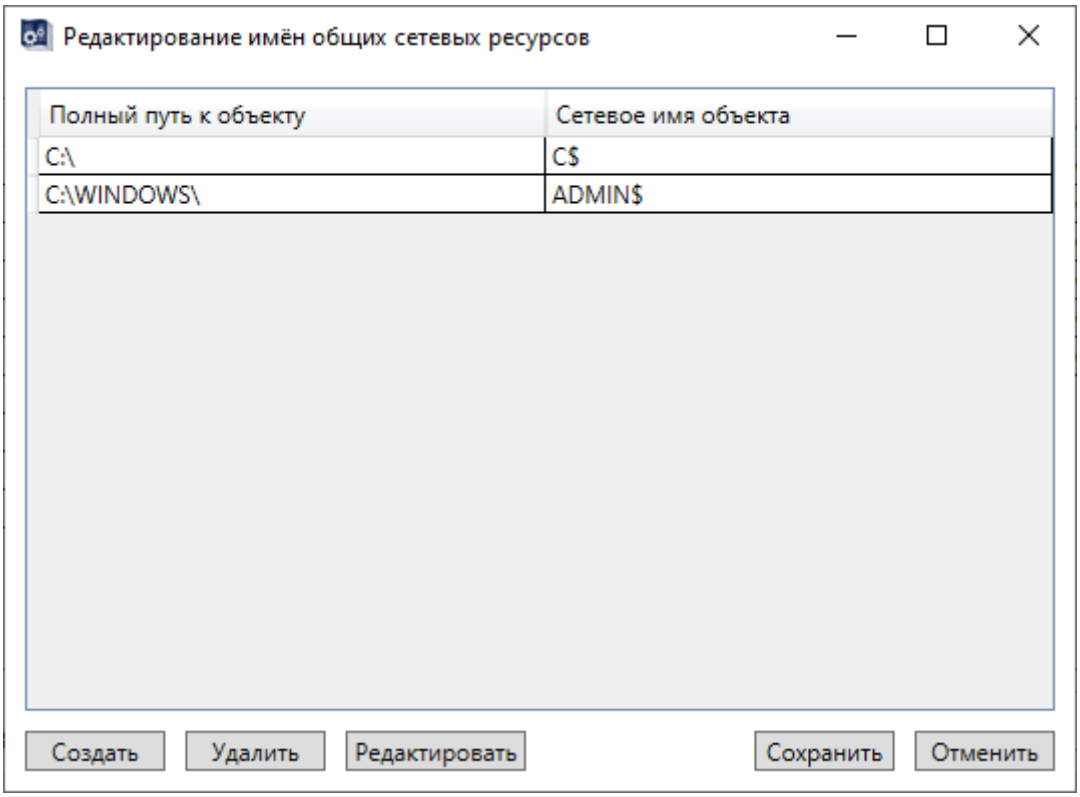



**Рисунок 62 – Окно редактирования имен общих сетевых ресурсов**

## 3.22. Результаты И/А

Поле «Результаты И/А» содержит параметры, которые включаются в информацию о пользователе, передающуюся или на терминальный сервер, или в контроллер комплекса «Аккорд-АМДЗ» (например, при включенном режиме «Автоматический логин в ОС»).

Если пользователь успешно провел процедуру идентификации/аутентификации, то по результатам проверки переданной информации для него открывается сессия с тем набором ПРД, который установил администратор безопасности.

## 3.23. Журнал регистрации событий AcedVI

С момента запуска AcedVI и до выхода из нее все события регистрируются в журнале утилиты. Журналы сохраняются в формате .log в каталоге Logs. Его расположение определяется в программе настройки комплекса «Аккорд» AcSetup.exe в поле «Вести журналы в:» (вкладка «Режим сессии» окна «Дополнительные опции»).

Файл конфигурации журнала LocalConfig.json находится в директории C:\Accord.x32. В этом файле в строке «LogLevel» можно задать уровень детальности журнала. Предлагаются следующие уровни:

INFO - отражает основные действия – создание, удаление пользователя (группы), изменение параметров;

DEBUG - показывает внутренние процессы одного действия (считан идентификатор, считан пароль, проведена проверка параметров аутентификации и т.п.);

TRACE – делает запись при входе и выходе в каждую функцию главных элементов программы.

Каждая запись в журнале регистрации описывает определенное действие пользователя или процесса, вызванного его действием, и содержит метку времени и метку уровня, т.е. при установке уровня DEBUG журнал будет содержать также строки уровня INFO.

Модифицировать/удалять файлы *.log имеет право только Администратор с привилегией «Управление журналом».

## 4. Заключение

Программа AcedVI является лишь редактором параметров доступа пользователя к объектам виртуальной инфраструктуры. А собственно разграничение доступа пользователей реализует драйвер ACRUN.SYS, который использует матрицу доступа, подготовленную с помощью редактора AcedVI. Подробно процесс настройки и запуска монитора безопасности ACRUN.SYS описан в «Руководстве по установке» (11443195.4012-036 98).

## Приложение 1.
## 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.

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.

EnableUserDuration=No – параметр определяет режим установки временного периода неактивности пользователя.

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.

InactiveDays=0 - устанавливает значение временного периода неактивности (в днях), по истечении которого учетная запись пользователя блокируется (параметр «Блокировать учетную запись при неактивности» программы настройки комплекса «Аккорд»).

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-Win32».

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).

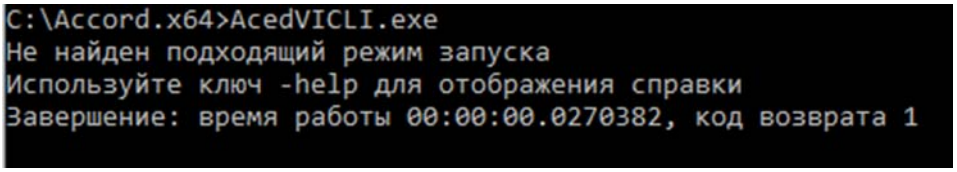
Параметры, задаваемые в файле accord.ini, изменяются программой настройки комплекса. Не рекомендуется менять их значение вручную без четкого понимания последствий вносимых изменений. Исключение – параметры UseLogicalDisksNames, WriteNsdOnFind, WriteWarningToLog, и NoConvertNetPath, они корректируются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

Обратите внимание, что после изменения значения параметра WriteNsdOnFind в файле Accord.ini требуется перезагрузка СВТ.

# Приложение 2.
# Работа с командной строкой.
# Описание ключей программы AcedVICLI

## Запуск программы AcedVICLI

Программа AcedVICLI позволяет выполнить ряд операций с использованием командной строки. Запуск программы осуществляется при наличии флага, определяющего режим дальнейшей работы. Основные флаги следующие: -help, -atf, -db, -kc, -lst. Если ни один из них не добавлен к команде запуска, то появится сообщение о невозможности запуска:




С добавлением любого флага произойдет запуск программы, при этом до момента включения ее функциональности будет проведен анализ БД Accord.amz, результатом которого могут стать стартовые преобразования в ней. При запуске режима, не предполагающего внесение исправлений в БД, эти преобразования будут учитываться только на время работы режима и не будут сохранены при выходе из него. Если режим предполагает изменение БД, она будет сохранена при выходе. Подробнее модификация пользовательских данных при запуске AcedVICLI описана в п.3.5 настоящего документа.

При добавлении флага –help будет показана справка по поддерживаемым режимам и их параметрам (ключам). Можно вывести справку отдельно по режиму atf или lst (AcedVICLI.exe –help –atf или -lst). Флаг –atf запускает режим работы (импорт, экспорт) с файлами БД пользователей *.atf. Флаг –db определяет режим модификации БД (добавление/удаление пользователей/групп). Флаг –kc позволяет рассчитать контрольные суммы объектов СКЦ. Флаг –lst определяет печать настроек одного или нескольких пользователей в файл *.lst.

При задании параметров командной строки необходимо учитывать следующую особенность: значения, передаваемые с ключом, должны идти вплотную к нему, определяя один параметр командной строки. Если в значении параметра необходимо использовать пробел, следует поставить кавычки, которые и определят единство параметра.

## Описание проведения процедуры импорта пользователей из файла *.atf в файл Accord.amz

Режим импорта пользователей запускается при указании ключей -atf -i

Далее в исходной директории (имя указывается дополнительным параметром к ключу -f) производится поиск необходимых для импорта файлов .atf. Каждый найденный файл следует прочитать, и каждого из находящихся в

нем пользователей создать в отмеченной группе (-g), после чего переложить в результирующую директорию (-t).

В процессе импорта будет выполнена проверка имени пользователя на идентичность уже существующим именам. При обнаружении в БД пользователя с идентичным доменным именем (с учетом регистра) будет создан пользователь с именем, в котором будет изменен регистр последней буквы. Если обнаружатся несколько таких пользователей, то у следующего будет изменен регистр предпоследней буквы, и так далее, к началу имени, после чего будет добавляться цифра (возрастающая) в конец имени. Если при импорте указать флаг –U, то идентификатор пользователя в БД с идентичным именем будет заменен на идентификатор из файла .atf, а пароль будет сброшен. В подобной ситуации администратору комплекса «Аккорд» после сохранения обновленной БД **необходимо назначить новый пароль пользователю с измененным идентификатором**.

Следует учитывать, что при наличии в файле .atf пользователей с идентичными именами базы данных SUPERVISOR и ASM_ACCOUNT и при указании флага –U они не будут добавлены в файл Accord.amz. Также не будут добавлены пользователи из файла .atf, если их идентификаторы окажутся уже назначенными пользователям редактируемой базы. При возникновении одной из этих ситуаций произойдет появление ошибки и завершение импорта, или же процесс импорта не прервется (-s), а в итоговом сообщении будет указано общее количество найденных пользователей и количество добавленных (импортированных).

В конце работы программы база данных автоматически сохраняется в результирующей директории.

Все операции по изменению БД в AcedVICLI заносятся в журнал регистрации событий.

### Описание проведения процедуры экспорта пользователей из файла Accord.amz в файлы *.atf

Режим экспорта пользователей запускается при указании ключей -atf -e

Каждый пользователь экспортируется в отдельный файл .atf. Эти файлы создаются в результирующей директории (-t). Имя пользователя в файле .atf формируется из параметра полное/доменное имя, или SUPERVISOR (для Гл. Администратора). Имя самого файла .atf будет зависеть от использования ключа –w.

Если указать ключ –w, то имя файла будет содержать полное/доменное имя пользователя и его идентификатор. При отсутствии ключа –w имя файла будет содержать только часть полного/доменного имени до @.

В процессе экспорта будет выполнена проверка имени файла на идентичность уже существующим именам, и при необходимости к имени файла .atf будет добавлена часть _# (# - числовое значение).

Ключи –g, -u, -k, -m выбирают пользователей для экспорта, все выбранные пользователи экспортируются в отдельные файлы.

Если указать ключ -g, для экспортирования будут выбраны пользователи указанной группы, при указании ключа -u будет выбран пользователь с указанным именем, при использовании ключа -k будет выбран пользователь с указанным идентификатором, а при использовании ключа –m будут выбраны пользователи, в именах которых будет указанная в параметре строка (для –m регистр не важен).

Ключи -u, -k, -m можно указывать многократно, при этом будут выбраны такие пользователи, которые подходят хотя бы под один из этих параметров.

Могут быть указаны или один ключ -g или любая комбинация ключей -u, -k, -m или ни одного (тогда будут выбраны все пользователи).

## Описание проведения процедуры удаления пользователей и групп из файлов Accord.amz и Accord.db

Удалить пользователя из БД можно при указании его имени или идентификатора.

Режим удаления пользователя по его имени запускается с помощью ключей -db –d –u, имя пользователя указывается после флага -u. Режим удаления пользователя по идентификатору запускается ключами -db –d –k, идентификатор пользователя указывается после флага -k. Перед запуском процесса удаления пользователя будут проверены наличие данного пользователя в базе (и что его имя не SUPERVISOR) и наличие прав на удаление у текущего администратора. Пустые значения имени или идентификатора не допускаются.

Режим удаления всех пользователей в группе запускается ключами -db –d –g –a, имя группы указывается после флага -g. Перед удалением всех пользователей в группе проверяется соответствие следующим условиям:

наличие данной группы в базе,

группа не пуста,

наличие прав на удаление у текущего администратора,

текущий администратор не оператор УЗ, если указанная группа - группа ADMINS.

Пустое значение имени группы не допускается.

Режим удаления группы запускается ключами -db –d –g, имя группы указывается после флага -g. Перед удалением группы проверяется соответствие следующим условиям:

наличие данной группы в базе,

группа пуста,

наличие прав на удаление у текущего администратора,

имя группы не ADMINS или EVERYONE.

Пустое значение имени группы не допускается.

## Описание проведения процедуры создания пользователей и групп в файлах Accord.amz и Accord.db

Режим создания группы запускается с помощью ключей -db –c –g, имя группы указывается после флага -g. Перед созданием группы проверяется, что пользователя или группы с указанным именем еще нет в базе, и наличие прав на создание у текущего администратора. Пустое значение имени группы не допускается.

Режим создания пользователя в группе запускается ключами -db –c –g -u, имя группы указывается после флага -g, имя пользователя указывается после флага -u. Перед созданием пользователя в группе проверяется соответствие следующим условиям:

наличие данной группы в базе,

пользователь или группа с указанным именем отсутствует в базе,

имя пользователя не SUPERVISOR,

наличие прав на создание у текущего администратора.

Если имя группы пустое, пользователь добавляется в группу EVERYONE. Пустое значение имени пользователя не допускается.

## Описание проведения перерасчета контрольных сумм объектов из списка КЦ группы

Режим перерасчета контрольных сумм (КС) проводится для списков статического и динамического контроля. Запускается режим при указании ключей -kc -r.

Расчет КС можно организовать или по отдельно указанной группе - для этого используется флаг –g (например, -gADMINS) - или (при отсутствии флага –g) поочередно по всем группам. Для расчета КС файлов БД и пароля используются стандартные флаги -z, -b и -p.

Если файл (контейнер), присутствующий в списке, не будет обнаружен в системе, возникнет ошибка с кодами 113 - 116 (отсутствие объекта), при этом если расчет ведется поочередно по всем спискам, то проведенные до этой ошибки расчеты сохранятся, а начиная с группы с отсутствующим объектом расчет остановится. Чтобы в подобной ситуации обеспечить возможность проведения расчета КС путем игнорирования отсутствующих объектов, следует добавить флаг -F, и тогда при появлении ошибок 113 – 116 перерасчет будет произведен только по оставшимся объектам после удаления отсутствующих. При этом появится информационное сообщение с перечислением отсутствующих элементов списка и сообщение "Всего не найдено X объектов. Они удалены из списков КЦ".

При расчете КС контейнера следует учитывать, что отсутствие объекта внутри контейнера не вызовет ошибку, так как при этом список КЦ остается неизменным, а изменения затрагивают только внутреннее состояние контейнера.

## Описание режима печати настроек пользователей в файл *.lst

Режим печати настроек пользователей в файл запускается при указании ключа –lst. При этом необходимо выбрать общие параметры печати: все пользователи из всех групп (не указаны ключи -g, -u, -k, -m), все пользователи из одной группы (-g), один пользователь, указанный по имени (-u) или идентификатору (-k), или список мандатных меток (-m). Также выбирается набор отображаемых параметров (-c), которые указывают на часть настроек каждого пользователя, записываемую в файл *.lst. Настройки берутся только у конкретных пользователей, настройки групп не используются (только имя группы). В режиме записи мандатных меток (-m) выбор настроек игнорируется, и отображается только список разграничений доступа.

Имя результирующего .lst-файла имеет следующий формат (в зависимости от выбора источника -g, -u, -k, -m):

Источник не указан (все пользователи): allusers[X].lst

где X – число пользователей, например, allusers[12].lst

-g: полное имя группы, например, ADMINS.lst

-u, -k: Полное/доменное имя пользователя, например, testuser@testdomain.lst

-m: OBJECTS.lst

Если файл с этим именем уже существует, будет добавлена приписка _# (# - числовое значение для избегания конфликтов), например, ADMINS_1.lst

Если ключи заданы корректно, то в начале работы программы выводится список значений для входных параметров.

В таблице 1 приведены основные ключи программы AcedVICLI и указаны особенности их использования.

**Таблица 1**

| Ключ | Описание | Примечание |
|---|---|---|
| -help | Отображение справочной информации по ключам программы | При указании вместе с –atf, -db, -kc, -lst выводит информацию по этим режимам, при их отсутствии – справку по всем доступным режимам.<br>Остальные ключи игнорируются |
| -atf | Указание на использование режима работы с файлами .atf | Не имеет дополнительного значения параметра |
| -db | Указание на использование режима работы с базой данных | |
| -kc | Указание на режим расчета контрольных сумм объектов из списка КЦ | |
| -lst | Указание на использование режима печати в файл .lst | Не имеет дополнительного значения параметра |
| -i | Указание на режим импорта из набора файлов .atf | Не имеет дополнительного значения параметра. Обязательно указание одного из режимов: –i или -e |

| | | | |
|---|---|---|---|
| -e | Указание на режим экспорта из базы данных в файлы .atf | | Не имеет дополнительного значения параметра. Обязательно указание одного из режимов: –i или -e |
| -d | Указание на режим удаления из базы данных | | |
| -r | Указание на перерасчет КС для существующих списков КЦ групп | | |
| -f | Указание директории, в которой будут искаться файлы .atf для импорта | | Дополнительный параметр. При отсутствии поиск будет производиться в текущей директории |
| -U | Проверка имени пользователя на идентичность уже существующим в БД именам с целью замены данному пользователю идентификатора | | Не имеет дополнительного значения параметра. Используется в режиме импорта |
| -t | Режим импорта | Указание директории, в которую будут перемещены файлы .atf | Дополнительный параметр. При отсутствии будет использовано значение по умолчанию atf_out |
| | Режим экспорта | Указание директории, в которой будут созданы файлы .atf | |
| | Режим печати в файл .lst | Указание директории и (или) имени файла .lst | Дополнительный параметр. При отсутствии файл с текущим именем будет создан в директории lst_out. При указании имени можно использовать полный и относительный путь. Если указано только имя (строка заканчивается не на "\"), файл будет создан в директории lst_out. Если не указано расширение файла, будет добавлено .lst |
| -z | Указание на расположение основного файла БД (Accord.amz) | | Дополнительный параметр. При отсутствии будет использовано значение Accord.amz из текущей директории |
| -b | Указание на расположение вспомогательного файла БД (Accord.db) | | Дополнительный параметр. При отсутствии будет использовано значение Accord.db из текущей директории. Если параметр отсутствует, но -z указан, то Accord.db будет искаться в той же директории, где расположен Accord.amz |
| -g | Режим импорта | Указание имени группы, в которую будут добавлены новые пользователи из файлов .atf | Дополнительный параметр. Будет использовано дефолтное значение EVERYONE (основная группа пользователей) |
| | Режим экспорта | Указание имени группы, пользователи которой будут экспортированы | Дополнительный параметр.<br>Может быть указан или один ключ -g или любая комбинация ключей -u, -k, -m или ни одного (тогда будут выбраны все пользователи) |
| | Режим перерасчета КС | Указание имени группы для проведения расчета | Дополнительный параметр. Можно указать только одну группу |

| | | | |
|---|---|---|---|
| | Режим печати в файл .lst | Указание имени группы, из которой следует брать настройки пользователей | Дополнительный параметр. Может быть указан только один из ключей: -g, -u, -k, или -m. Если все ключи отсутствуют – будут взяты все пользователи из всех групп |
| | Режим удаления | Указание имени удаляемой группы или группы, из которой будут удалены все пользователи | Дополнительный параметр |
| | Режим создания | Указание имени создаваемой группы | Дополнительный параметр |
| -s | Указание на пропуск пользователя с идентификатором, уже назначенным другому пользователю редактируемой базы, или пользователя с недопустимыми символами в имени | | Дополнительный параметр. Используется при импорте. Позволяет не импортировать (пропускать) пользователя с назначенным ранее другому идентификатором или с недопустимыми символами в имени, не прерывая при этом процесса импорта. |
| -p | Пароль для аутентификации в Accord.amz (пароль того из администраторов в БД, которым будет проводиться аутентификация) | | Дополнительный параметр. При отсутствии будет запрос пароля в командной строке |
| -u | Режим экспорта | Указание имени (полного/доменного) экспортируемого пользователя | Дополнительный параметр.<br><br>Может быть указан или один ключ –g, или любая комбинация ключей -u, -k, -m, или ни одного (тогда будут выбраны все пользователи) |
| | Режим печати в файл .lst | Указание имени пользователя (полного/доменного) для печати его настроек | Дополнительный параметр. Может быть указан только один из ключей: -g, -u, -k, или -m. Если все ключи отсутствуют – будут взяты все пользователи из всех групп |
| | Режим удаления | Указание имени (полного/доменного) удаляемого пользователя | Дополнительный параметр |
| | Режим создания | Указание имени (полного/доменного) создаваемого пользователя | Дополнительный параметр |
| -k | Режим экспорта | Назначенный идентификатор экспортируемого пользователя | Дополнительный параметр.<br>Может быть указан или один ключ –g, или любая комбинация ключей -u, -k, -m, или ни одного (тогда будут выбраны все пользователи)<br>Для этого параметра важен формат значения – при его указании возможны пробелы, и, следовательно, необходимо использование кавычек |

| | | | |
|---|---|---|---|
| | Режим удаления | Назначенный идентификатор удаляемого пользователя | Дополнительный параметр.<br>Для этого параметра важен формат значения – при его указании возможны пробелы, и, следовательно, необходимо использование кавычек |
| | Режим печати в файл .lst | Назначенный идентификатор пользователя для печати | Дополнительный параметр.<br>Может быть указан только один из ключей: -g, -u, -k, или -m. Если все ключи отсутствуют – будут взяты все пользователи из всех групп.<br>Для этого параметра важен формат значения – при его указании возможны пробелы, и, следовательно, необходимо использование кавычек |
| -m | Режим экспорта | Часть Полного/Доменного имени выбираемого для экспорта пользователя | Дополнительный параметр.<br>Может быть указан или один ключ –g, или любая комбинация ключей -u, -k, -m, или ни одного (тогда будут выбраны все пользователи)<br>Для данного параметра не важен регистр. |
| | Режим печати в файл .lst | Указание на подрежим вывода мандатных меток | Не имеет дополнительного значения параметра |
| -c | Режим печати в файл .lst | Выбор блока настроек, необходимых для добавления в результирующий файл .lst | Имеет набор фиксированных дополнительных значений и может многократно быть указан в команде с этими значениями - все они станут выбранными для записи (подробнее в таблице 2) |
| | Режим создания | Указание на создание объектов при работе с базой данных | Не имеет дополнительного значения |
| -a | Выбор режима удаления всех пользователей в группе | | |
| -F | Выбор опции режима перерасчета КС, которая удаляет из списка КЦ отсутствующие объекты и проводит расчет оставшихся элементов списка | | |
| -w | Формат имени atf-файла для режима экспорта | | При наличии данного ключа имена файлов будут иметь формат:<br><ПолноеИмяПользователя>_<идетификатор>.atf<br>Например, user@domain_01 020304050607 D2.atf.<br>При отсутствии данного ключа имена файлов будут иметь формат:<br><ИмяПользователя>.atf<br>Например, user.atf.<br>Если файл с этим именем уже существует, будет добавлена приписка _# (# - числовое значение для избегания конфликтов) |

В таблице 2 приведены дополнительные значения ключа –c для режима печати настроек.

**Таблица 2**

| **Дополнительное значение ключа -c** | **Название добавляемого в файл *.lst блока настроек** |
|---|---|
| Options | Опции |
| Password | Настройки пароля |
| EnterTime | Временные ограничения |
| StartTask | Стартовая задача |
| LogLevel | Детальность журнала |
| SSaver | Гашение экрана |
| PrdObjects | ПРД объектов |
| PrdProcesses | ПРД процессов |
| ResultIa | Результаты И/А |
| UserLevel | Уровень доступа |
| IControl | Контроль целостности |
| All | Не имеет названия. Добавление -cAll эквивалентно указанию всех значений ключа -c по отдельности: -cOptions -cPassword …-cIControl |

В таблице 3 приведены коды возврата команд, соответствующие им текстовые сообщения, а также даны описания и предлагаемые действия при их появлении.

**Таблица 3**

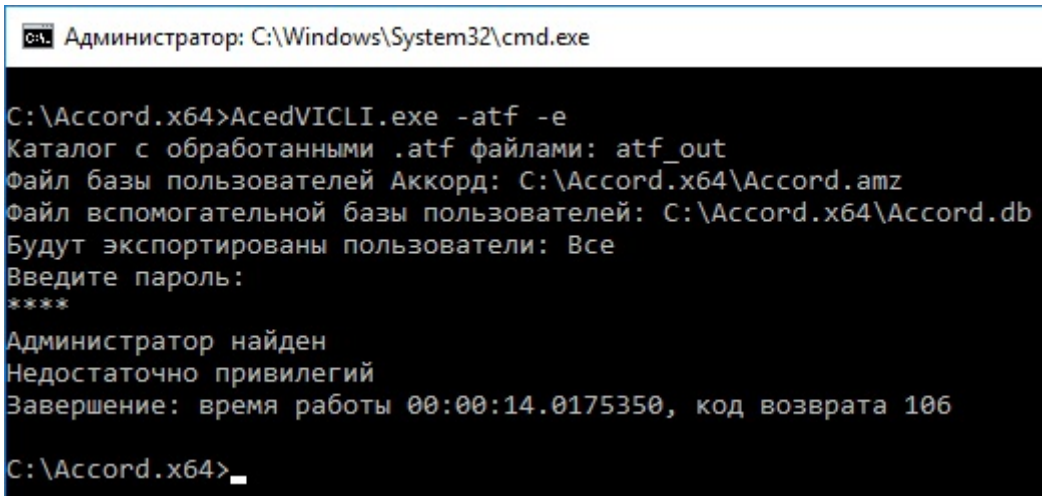
| **Код возврата** | **Текстовое сообщение** | **Комментарий** | **Действия при появлении кода** |
|---|---|---|---|
| 0 | | Возвращается, если работа программы прошла успешно, и не возникла ни одна из указанных ниже ошибок | |
| 1 | «Неизвестный параметр»<br>«Не выбран режим работы с atf файлами»<br>«Попытка запуска нескольких режимов одновременно»<br>«Попытка экспорта из нескольких источников»<br>«Не найден подходящий режим запуска. Используйте ключ -help для отображения справки»<br>«Неизвестная настройка для отображения»<br>«Попытка получения настроек из нескольких источников»<br>«Не выбраны настройки для записи» | Указан несуществующий ключ<br>Одновременное указание ключей –help и –atf<br>Указано неизвестное дополнительное значение для ключа –c<br>Указан более чем один ключ из -g, -u, -k, -m<br>Не указан ни один ключ -c (с правильным значением из доступных) | При импорте/экспорте обязательно следует указывать ключ –atf<br>При экспорте следует указывать только один из ключей: -g, -u, -k |

| | | | |
|---|---|---|---|
| 10 | «Ошибка при распознавании параметров» | | |
| 11 | «Ошибка при чтении базы» | Возникает при чтении и распаковке .amz файла | |
| 12 | «Ошибка при поиске .atf файлов» | | |
| 13 | «Ошибка при аутентификации» | | |
| 14 | «Ошибка при поиске группы» | На этом этапе при импорте создается группа (при необходимости) | |
| 15 | «Ошибка при распознавании .atf файла» | Возникает при чтении .atf файла | |
| 16 | «Ошибка при добавлении пользователей» | | |
| 17 | «Ошибка при записи базы» | | |
| 18 | «Ошибка при поиске пользователей» | | |
| 19 | «Ошибка при создании .atf файла» | | |
| 20 | «Ошибка при сборе информации о настройках» | | |
| 21 | «Ошибка при создании .lst файла» | | |
| 100 | «Исходный каталог не найден» | Каталог, указанный для импорта, отсутствует | |
| 101 | «Исходный каталог пуст» | В указанном для импорта каталоге не найдены .atf файлы | |
| 102 | «Не найден .amz файл» | | |
| 103 | | Появляется, если идентификатор не был предъявлен, например, по истечении тайм-аута | При предъявлении идентификатора следует учитывать, что время для этой процедуры устанавливается таймером |
| 104 | «Администратор не найден» | В группе «Администраторы» не найден пользователь, которому назначен предъявленный идентификатор | Проводить импорт/экспорт может только пользователь из группы «Администраторы» |
| 105 | «Аутентификация не пройдена» | Был введен неправильный пароль или не подошел открытый ключ (вычисленный на основе закрытого, записанного в предъявленный идентификатор) | |

| | | | |
|---|---|---|---|
| 106 | «Недостаточно привилегий» | Проверка привилегий подключившегося администратора после успешного ввода пароля.<br>При импорте должен быть установлен флаг «Редактирование пользователей».<br>Если установлен флаг «Оператор УЗ», то:<br>1) для импорта необходимо, чтобы группа была уже создана на момент импорта и чтобы это не была группа «Администраторы»;<br>2) для экспорта должен быть выбран дополнительный параметр, и если этот параметр –g, то группа не должна быть Администраторы»<br>3) для режима печати в файл .lst должен быть выбран один дополнительный параметр из -g, -u, -k, -m, и если этот параметр –g, то группа не должна быть Администраторы» | |
| 107 | «Идентификатор XXX уже назначен другому пользователю» | Появляется, если идентификатор импортируемого пользователя уже присутствует в БД.<br>При появлении ошибки ранее добавленные пользователи сохраняются в БД, но работа программы прерывается, а atf файл с пользователем, у которого возникла ошибка, не переносится в отработанные.<br>Эту ошибку можно проигнорировать (не добавив этого пользователя) и производить импорт дальше, если использовать ключ –s | Рекомендуется использовать при импорте ключ –s.<br>Это позволит избежать прерывания процесса импорта и дальнейшего его повторного запуска |
| 108 | «Указанная группа не найдена» | Появляется при экспорте для режима одной группы (-g) | |
| 109 | «Пользователь с указанными параметрами не найден»<br>«Найдено 0 пользователей» | Появляется:<br>1) при экспорте для режимов –m, -u и -k.<br>Если подключившийся администратор имеет привилегию «Оператор УЗ», то группа «Администраторы» пропускается, и поиск в ней не производится;<br>2) если для экспорта не нашлось ни одного пользователя | Если администратор имеет привилегию «Оператор УЗ», поиск в группе «Администраторы» ему не доступен. |
| 113 | «Не найден файл» | Появляется в режиме расчета КС списка КЦ групп при фактическом отсутствии в | При использовании флага -F расчет будет |

| | | | |
|---|---|---|---|
| | | системе отдельного файла из списка КЦ | произведен только по оставшимся объектам после удаления отсутствующих |
| 114 | «Не найдена директория» | Появляется в режиме расчета КС списка КЦ групп при фактическом отсутствии в системе директории из списка КЦ | При использовании флага -F расчет будет произведен только по оставшимся объектам после удаления отсутствующих |
| 115 | «Не найден параметр реестра» | Появляется в режиме расчета КС списка КЦ групп при фактическом отсутствии в системе параметра реестра из списка КЦ | При использовании флага -F расчет будет произведен только по оставшимся объектам после удаления отсутствующих |
| 116 | «Не найден ключ реестра» | Появляется в режиме расчета КС списка КЦ групп при фактическом отсутствии в системе ключа реестра (для контейнеров реестра) из списка КЦ | При использовании флага -F расчет будет произведен только по оставшимся объектам после удаления отсутствующих |
| 117 | «Имя пользователя содержит недопустимые символы" | Появляется в режиме импорта при попытке импортировать пользователя с недопустимыми символами в имени | В имени пользователя должны применяться только буквы латинского алфавита и символы @ _ . - |

## Примеры использования командной строки при проведении процедур импорта/экспорта БД и печати в файл *.lst




**Попытка администратора произвести экспорт, не имея на это полномочий**

```
C:\Accord.x64>AcedVICLI.exe -atf -e -gADMINS
Каталог с обработанными .atf файлами: atf_out
Файл базы пользователей Аккорд: C:\Accord.x64\Accord.amz
Файл вспомогательной базы пользователей: C:\Accord.x64\Accord.db
Будут экспортированы пользователи: из группы ADMINS
Введите пароль:
****
Администратор найден
Найдено 2 пользователей
Записано 2 файлов
Завершение: время работы 00:00:09.0060897, код возврата 0

C:\Accord.x64>
```

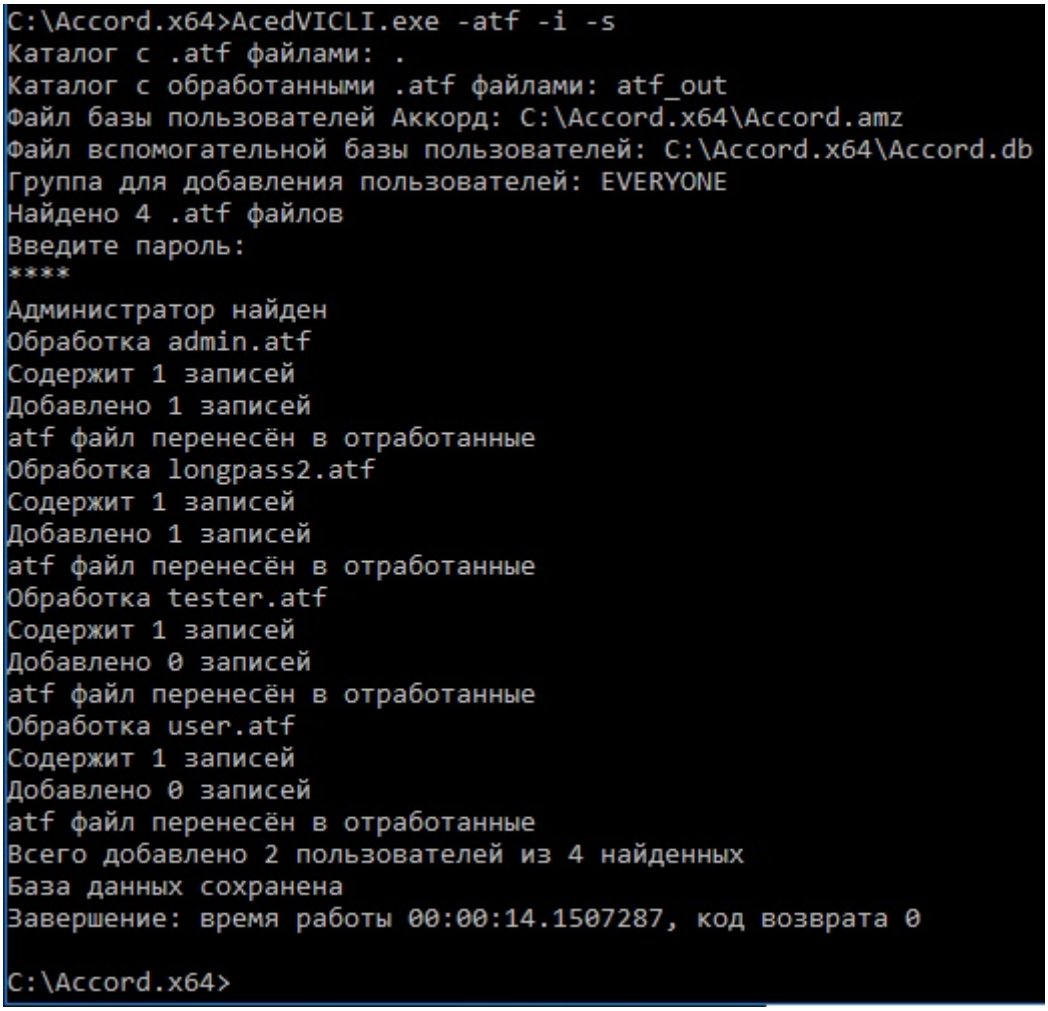
**Успешный экспорт пользователей группы ADMINS**

```
C:\Accord.x64>AcedVICLI.exe -atf -e -p1q2w
Каталог с обработанными .atf файлами: atf_out
Файл базы пользователей Аккорд: C:\Accord.x64\Accord.amz
Файл вспомогательной базы пользователей: C:\Accord.x64\Accord.db
Будут экспортированы пользователи: Все
Администратор найден
Найдено 5 пользователей
Записано 5 файлов
Завершение: время работы 00:00:05.0793144, код возврата 0

C:\Accord.x64>_
```

**Использование ключа -p**

```
C:\Accord.x64>AcedVICLI.exe -atf -e "-k01 00002FD9DC92 C4"
Каталог с обработанными .atf файлами: atf_out
Файл базы пользователей Аккорд: C:\Accord.x64\Accord.amz
Файл вспомогательной базы пользователей: C:\Accord.x64\Accord.db
Будут экспортированы пользователи: с идентификатором 01 00002FD9DC92 C4
Введите пароль:
****
Администратор найден
Найдено 1 пользователей
Записано 1 файлов
Завершение: время работы 00:00:08.2056413, код возврата 0

C:\Accord.x64>_
```

**Использование ключа –k**




**Использование ключа –s**

```
Не найден .amz файл
Завершение: время работы 00:00:00.0588639, код возврата 102

C:\Accord.x64>AcedVICLI.exe -atf -i -zC:\amz\Accord.amz -bC:\db\Accord.db -fC:\atf -tC:\out
Каталог с .atf файлами: C:\atf
Каталог с обработанными .atf файлами: C:\out
Файл базы пользователей Аккорд: C:\amz\Accord.amz
Файл вспомогательной базы пользователей: C:\db\Accord.db
Группа для добавления пользователей: EVERYONE
Найдено 3 .atf файлов
Введите пароль:
****
Администратор найден
Обработка admin.atf
Содержит 1 записей
Добавлено 1 записей
atf файл перенесён в отработанные
Обработка tester.atf
Содержит 1 записей
Добавлено 1 записей
atf файл перенесён в отработанные
Обработка user.atf
Содержит 1 записей
Добавлено 1 записей
atf файл перенесён в отработанные
Всего добавлено 3 пользователей
База данных сохранена
Завершение: время работы 00:00:12.8341666, код возврата 0

C:\Accord.x64>
```

**Использование ключей –z –b –f –t**

```
C:\Accord.x64>AcedVICLI.exe -lst -cAll -gADMINS -zC:\Accord.x64\Accord.amz -tC:\Accord.x64\lst_out
Каталог с созданным .lst файлом: C:\Accord.x64\lst_out
Файл базы пользователей Аккорд: C:\Accord.x64\Accord.amz
Файл вспомогательной базы пользователей: C:\Accord.x64\Accord.db
Будут записаны настройки пользователей: из группы ADMINS
Выбраны настройки[11]:
  Опции
  Настройки пароля
  Временные ограничения
  Стартовая задача
  Детальность журнала
  Гашение экрана
  ПРД объектов
  ПРД процессов
  Результаты И/А
  Уровень доступа
  Контроль целостности
Введите пароль:
********
Администратор найден
Настройки собраны
Файл ADMINS_1.lst успешно создан
Завершение: время работы 00:00:12.6568381, код возврата 0

C:\Accord.x64>_
```

**Использование команды -lst**